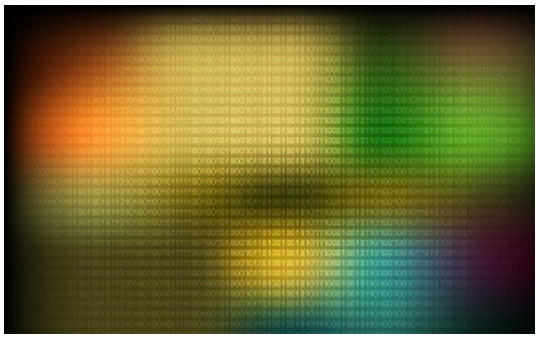
Tractica


RESEARCH REPORT

Blockchain for Enterprise Applications

Distributed Ledger Technology for Payments, Processing & Settlement, Microtransactions, Asset Management, Identity & Access Management, Automated Compliance, and Prediction Markets: Global Market Analysis and Forecasts

Published 4Q 2016

JESSICA GROOPMAN
Principal Analyst

ADITYA KAUL
Research Director

SECTION 1
EXECUTIVE SUMMARY

1.1 INTRODUCTION

There has been much ado about blockchain: a distributed data-verification technology wherein financial and operational transactions are recorded and validated across a network, rather than through a central authority. What some relegate to being a Pandora's Box, others deem the greatest revolution in technology since the Internet itself. Amid all of the hyperbole, two certainties underlie the blockchain market today.

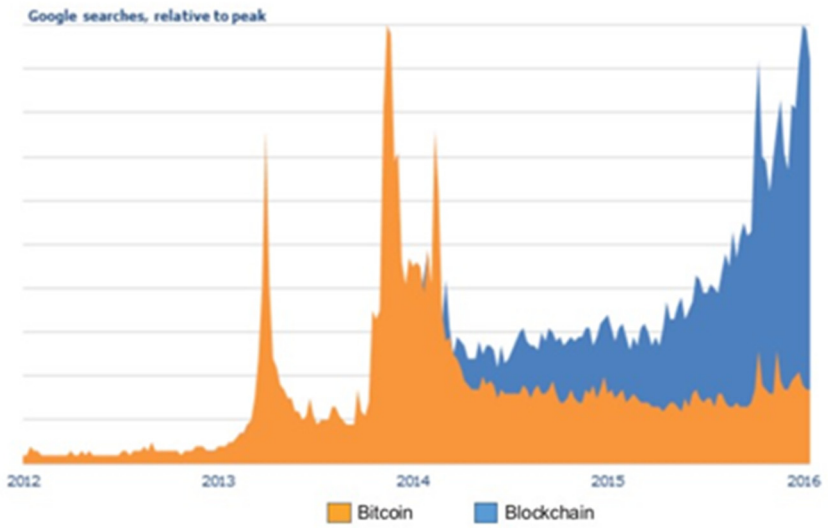
First, we are in the primordial days of blockchain. This is a market of extreme nascence and fragmentation; a notable void of in-production or at-scale implementations; and a lack of regulatory, legal, governance, collaborative, economic, digital, and even cultural precedent. Industry-wide, blockchain remains in the proof-of-concept (POC) stage of development, in which proofs are experimental, highly limited in size and scope, and primarily designed to build stakeholder understanding. This, coupled with high investments associated with current efforts, has some expecting blockchain to tumble into the "trough of disillusionment" in the coming months.

Second, blockchain is intriguing bait for the many global actors in a gold rush for the next transformative technology. Blockchain technology teases a radical new approach for enterprise *and* individual engagement, transaction, and collaboration, thus posing both an opportunity and threat to all. In the last year alone, over a hundred financial institutions, more than two dozen governments, and countless technology corporations have invested in blockchain. Venture capitalists alone have sunk more than $1 billion into blockchain startups. Blockchain startups make up some 20% of the largest crowdfunding projects of all time.

Blockchain is not just capturing wallet share, it is capturing the imaginations of individuals, entrepreneurs, innovators, academics, legislative bodies, and institutions of all types, worldwide. In a market synonymous with decentralization, the race to own the rights to blockchain is also underway. More than 2,500 patents have been filed on distributed ledger technology (DLT) since 2013. Bank of America alone has already filed 20 blockchain patent submissions; JP Morgan, MasterCard, Wells Fargo, Visa, American Express, and Western Union have all followed suit.

Many have argued that Bitcoin was blockchain's first "killer app," just as email was to the Internet. But what began with Bitcoin is now blossoming beyond cryptocurrency and the transfer of money, to an architecture that can support many types of transactions, from logging an event, to signing a document, to allocating energy between parties, and far beyond.

Figure 1.1 Google Searches for Bitcoin versus Blockchain between 2014 and 2016



(Source: Google Trends)

This research report addresses the applicability of blockchain across industries and large-scale business processes, including, but also beyond financial services and cryptocurrency. What are the use cases for which current processes can be replaced with a blockchain-based approach because it is more efficient, secure, lightweight, cheaper, or better than the current model?

Tractica's research into this emerging technology unearthed more than 30 use case categories for which blockchain, sometimes called "distributed ledger" architectures, could drive significant efficiencies. Based on our research and forecasting, Tractica believes the opportunity for blockchain expands across a wide range of industries and geographies and is particularly disruptive in highly regulated markets with numerous counterparties. Blockchain faces a number of fundamental and significant hurdles to adoption, which will be outlined in this report. It also introduces a framework for significant improvements in efficiency, security, authenticity, and most importantly, trust.

1.2 MARKET DRIVERS

The primary driver behind the application of blockchain technology is trust, or more commonly, the lack thereof. Today, in most areas of economic and business processes, *transaction,* the exchange of value, is disassociated from *operational execution*, or the interaction between products, services, and people. In the absence of trust (and in the presence of abuse), millions of people worldwide are employed to document, verify, audit, and secure these exchanges. This fosters distrust, errors, inefficiencies, and abuse.

Through **digitizing** previously analog or disparate interactions, distributing the verification of those events across a **decentralized** network in a way that is both **secure** and **immutable**, the very architecture of blockchain drives a range of efficiencies in areas where trust falters. Encoding access, permissions, smart contracts, and security rules into the ledger helps enable trust, as more code (and fewer people), becomes the intermediary in settling transactions.

Protocol-based trust distributed across a network offers significant potential to drive greater visibility, efficiencies, security, and cost savings in processes, infrastructure, and reduction of corruption. At scale, the conceivable benefits of blockchain are many:

- Decreasing the time required for settlement and reconciliation of transactions
- Enabling devices to negotiate and transact themselves
- More easily detecting and preventing fraud and anti-counterfeit
- Automating compliance adherence
- Enhancing security
- Providing increased identity controls, integrity, and protections

These are but a snapshot of the range of benefits a distributed database architecture could enable. Furthermore, these efficiencies cut across numerous industries, compounding cost savings related to infrastructure, headcount, systems maintenance, integration, compliance, and greater liquidity.

While it may be entirely too early to predict the long-term future for blockchain deployment, we can be sure its *potential* for disruption is massive.

1.3 MARKET BARRIERS

Despite growing awareness and a wide range of benefits blockchain *could* enable, the technology faces numerous barriers to achieve widespread or enterprise-scale adoption. First, any sober assessment of this market must stress *just how early we are* in our collective understanding, exploration, and application of blockchain technology.

The reality today is the space desperately needs definition, standardization, and deep collaboration if it stands to ever come to fruition. Developing a decentralized architecture to handle billions (one day, trillions) of transactions securely requires unprecedented cooperation and collaborative infrastructure development across counterparties. Unclear monetary regulations or shared (cross-border) policies are significant barriers to achieving anything close to a critical mass of adoption, and these are only the beginning. For most enterprise applications, a wide range of regulatory hurdles and a lack of shared liability frameworks and governance structures hinder blockchain adoption.

Blockchain also presents a number of challenges to current economic structures and concepts. For many companies, disassociating business assets, processes, and control from a “centralized” way of thinking is an enormous strategic and cultural hurdle. Many orthodoxies foundational to current business models could face extinction. Furthermore, blockchain presents a structure for digitizing “identity” in a far more unified manner than currently possible. This has manifold implications, not just for business models that rely on mining user and machine data, but for the very notions of identity, privacy, autonomy, and control.

In these early days, the diversity of those interested in the blockchain market – from anarchists to academia to investors and enterprises – is directly influencing its development trajectory, creating numerous tensions, which exacerbate or contort many of the aforementioned dynamics.

1.4 TECHNOLOGY ISSUES

This report provides a high-level examination of blockchain architecture and discusses the range of public and private blockchain structures. Within these structures, Tractica explores a number of technical questions that have yet to be fully resolved:

- Defining what a blockchain is (and is not)
- Appropriateness of blockchain application
- Blockchain as a bundle versus à la carte
- Blockchain software versus firmware
- Security and privacy implications

Blockchain is not a panacea or a solution to all information technology (IT) inefficiencies, but rather a series of modules that businesses must evaluate against current solutions and the needs and risks associated with integration. Interoperability remains a massive challenge for blockchain, not just with other chains, but with devices, existing data sets, and incumbent systems. Although a central objective of numerous consortia and development activities, standardization is lacking at most layers of the stack, not to mention at the process level or across sectors or geographies. Requirements for customization can further fragment the technology's ability to function harmoniously with other counterparties and architectures.

These problems are augmented by a host of other uncertainties around security, privacy, identity, and perhaps most notably, blockchain's ability to scale. Data storage, bandwidth, and energy waste remain massive questions to the long-term scalability of blockchain. As a result, such constraints influence today's architectural development.

1.5 ENTERPRISE USE CASES FOR BLOCKCHAIN

Although financial services have sponsored the majority of investment in blockchain, the applicability of DLTs touches a wide range of industries and use cases. Tractica's research finds use cases for blockchain roll up into six parent categories, which can be segmented into more than 30 distinct use cases.

- Payments, Transaction Processing, & Settlement
- Microtransactions
- Asset Management
- Identity & Access Management
- Automated Compliance
- Prediction Markets

Within each of the use cases Tractica identified, we see countless sector-specific variations. As with most technological innovations, different industries will adopt pieces of this technology at varying paces. But unlike other recent technological advancements, the network effect compounds blockchain's potency, utility, and efficiency; the more institutions that adopt blockchain simultaneously, the faster its impact.

Tractica's analysis also surfaces at least seven distinct criteria for blockchain adoption and prioritization.

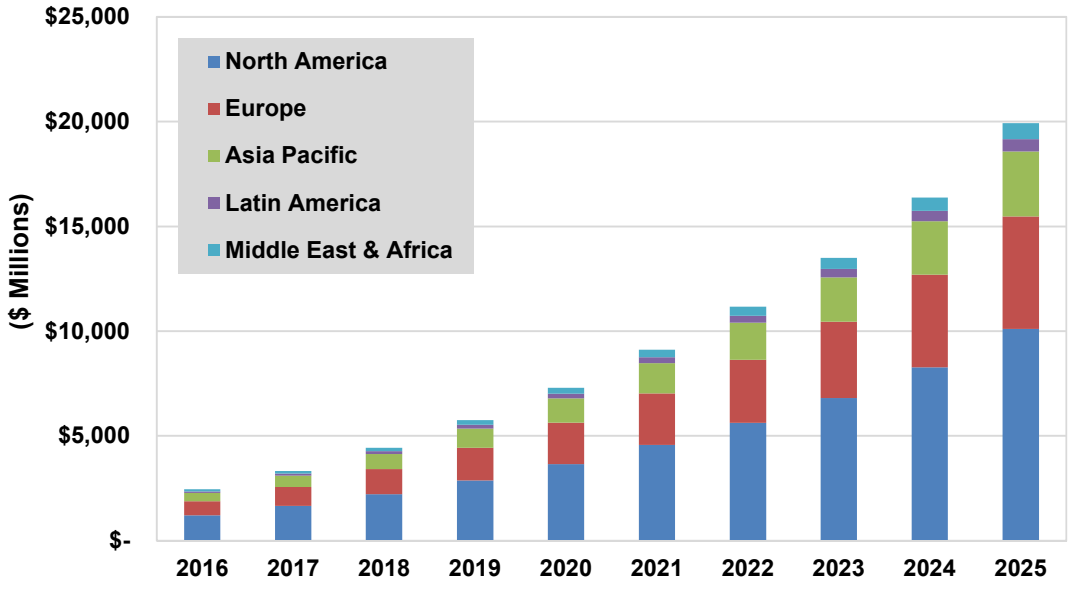
1.6 MARKET FORECAST

Tractica forecasts that annual revenue for enterprise applications of blockchain will increase from roughly $2.5 billion worldwide in 2016 to $19.9 billion in 2025, representing a compound annual growth rate (CAGR) of 26.2%. While a relatively lower CAGR than other emerging technology markets, Tractica forecasts the blockchain market's growth will remain conservative for some time. Although the blockchain market has seen significant investment over the last 18 months, areas of growth will remain fragmented and contingent upon numerous macro forces far beyond the control of any single country, government, enterprise, or technology.

The forecast developed for this research segments the market by five world regions, 19 different industry verticals, and approximately 29 unique use case categories. Use cases in the forecast have been identified as priority use cases, as they represent the greatest potential for cost savings and/or business model disruption and opportunity. Readers of this report will also find additional use cases and sub-categories in the qualitative assessment in Section 4.1. Some of these use cases include the Internet of Things (IoT)/machine-to-machine (M2M) communications & device interactions, digital advertising management, online gaming, and patient records management, among many others. Tractica's forecast model also assesses the revenue opportunity for blockchain across implementation categories such as software, database, hardware, maintenance, consulting, and more. Finally, Tractica forecasts the opportunity for cost savings versus blockchain services (net new) revenue. Detailed market sizing, segmentation, and forecasting tables are included in the Excel databook that accompanies this report.

Alongside the market forecast, this research presents a comprehensive exploration and analysis of the market drivers, obstacles, technologies, vendors, businesses, and societal implications essential to assessing the market opportunity and challenges for enterprise blockchain deployment.

Chart 1.1 Blockchain Revenue by Region, World Markets: 2016-2025



(Source: Tractica)

SECTION 2
MARKET ISSUES

2.1 BLOCKCHAIN DEFINITION AND OVERVIEW

A blockchain is a technology that offers a new model of digital transaction in which financial transactions and operational execution are integrated. Tractica defines a blockchain as a decentralized, distributed ledger wherein financial and operational transactions are recorded across, and verified by the network rather than a single central authority.

Blockchain networks are unique because of their *decentralized consensus mechanism*. This is a new mechanism to transfer *any kind of asset* as well as *the legacy or history of value and interaction* associated with that asset, neither of which requires a centralized intermediary.

Blockchain is about using technology to create trust and eliminate corruption through immutable records. Some have called it a technological and mathematical breakthrough because it is the first time in history humans have developed a system to reliably coordinate action among many parties without having any central authority.

Blockchain can also be viewed as a "meta technology" as it is made up of numerous technologies, including computers, devices, networks, algorithms, and software, all of which are built on top of the Internet and work together to reach consensus on mutual information transactions.

A deeper technological explanation for blockchain can be found below in Section 3.1.

It is worth noting that the term "blockchain" itself often carries different connotations, nuances, and even preferred synonyms based on the person or agenda using it. Although blockchain is used more frequently than (but often synonymously with) DLT, blockchains are but one type of distributed consensus data structure. This report will use blockchain and DLT synonymously, but acknowledges the lack of global consensus in nomenclature.

2.2 MARKET DRIVERS

The primary driver behind the application of blockchain technology is trust, or more commonly, the lack thereof. In this market, areas ripe for blockchain are those where trust among contributing actors is low, and the need for records security and integrity (to prevent corruption and streamline transaction) is high. In business and economic environments where trust is limited, this technology offers a means to integrate financial and operational execution while fostering far increased visibility, accountability, efficiency, security, and cost savings compared to current approaches.

2.2.1 THE INTEGRATION OF FINANCIAL TRANSACTION AND OPERATIONAL EXECUTION

Today, in most areas of economic and business processes, transaction, the exchange of value, is disassociated from operational execution, or the interaction between products, services, and people. Within this gap lie massive and diverse inefficiencies and loss; from analog reconciliation and settlement processes to more nefarious tampering or fraud. The fundamental value proposition of blockchain technology is its ability to integrate, or at least significantly shorten the gap, between transaction and operational execution.

Conceptualizing the scope of opportunities and use cases blockchain presents requires a survey of the context for what makes it valuable in the first place. Blockchain's underlying architecture has four essential characteristics supporting its value proposition:

- **Digitization:** The ability to store coded representations or references for digital and physical assets, documents, events, identities, etc. to digitize all consumption of products and services.

  Value: Improves auditability, transparency, access, provenance tracking, and authenticity.

- **Decentralization:** The requirement to distribute control, computing processes, processing power, security, vulnerability, etc. across multiple nodes.

  Value: Eliminates the need for central approving authority over value exchange; lowers risk of tampering, human error, singular attack point vulnerability; and streamlines settlement, latency, and cost reductions.

- **Immutability:** Transaction blocks created through digital transactions are irreversible and immutable, thus auditable; and serve as "truth" for all future transaction validations.

  Value: Increases transparency, access, records integrity, compliance adherence, efficiency; lowers risks of fraud.

- **Security:** Distributed architecture, cryptographic signatures occurring at the block-level, plus sophisticated smart contract and identity authentications, permissions, public, and private keys strengthen security and reduce opportunity for tampering or fraud.

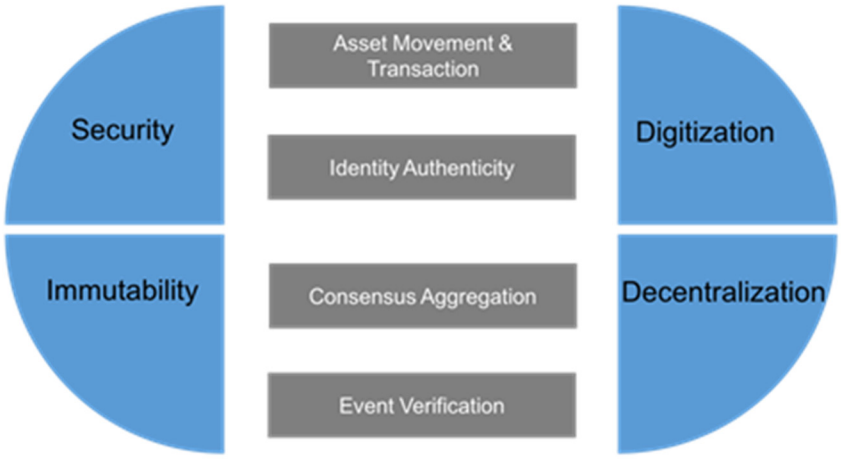
  Value: Increased security integrity across broader threat surface means large-scale attacks are more difficult and costly; immutability helps identify events or points of attack.

Through **digitizing** previously analog or disparate interactions, distributing the verification of those events across a **decentralized** network in a way that is both **secure** and **immutable**, enables the very architecture of blockchain to drive efficiency in areas where trust falters. Assets and actors can interact with each other to exchange both value and activity integrated together, securely, immutably, and in real time.

But what will drive market development in this space is not the technology per se, rather the *outcomes* and *efficiencies* the components enable at scale. Integration of financial and operational execution is made possible because of how this technology supports the following processes:

- **Identity Authenticity:** The ability to tie unique individual data, attributes, documents to a person, group, machine, or other individual actor within the network.
- **Event Verification:** The ability to know and notarize precisely when a piece of data or evidence came into existence.
- **Consensus Aggregation:** The ability for a shared database, wherein no single user or entity can control, manipulate, add, or delete data without consensus approval.
- **Asset Movement & Transaction:** The ability to automate transactions (i.e., payment, settlement, or other manner of the transfer of products or services) between persons or objects through pre-defined rules.

Figure 2.1 The Value Proposition of Blockchain Technology



(Source: Tractica)

The technological characteristics of blockchain and the outcomes made possible spell the potential for wide-sweeping impact and value creation when applied to existing processes involving numerous stakeholders, complex transaction chains, high regulation, and a requirement for trust.

2.2.2 Blockchain Enables Visibility in the Absence of Trust

Trust is perhaps the most important currency in any exchange—economic, social, or otherwise. That this technology may forge new immutable ways to establish and make "truth" accessible, particularly as it exists in real time, is a significant step in the digitization of human life.

A number of macro effects set the stage for the development and reception of blockchain. Societies across the world are seeing increasing disparities in wealth and power; a rapidly globalizing and ever-connected world grants access to more information across a broader range of people. The knowledge of this disparity juxtaposed against painful economic realities for billions of individuals, plus a list of corporate and government transgressions, has eroded trust. Financial services is the least trusted industry in the world, according to Edelman's Trust Barometer. As an institution, governments score even lower.

The issue of trust set the backdrop for the birth of blockchain; an anonymous person going under the pseudonym Satoshi Nakamoto published the source code and original white paper in October, 2008, just one month after the stock market crash, which was spurred by failure on the part of global financial institutions. The 2008 financial crisis exposed deep weaknesses in the balance sheets of numerous financial institutions, as well as risky lending practices and questionable accountability. As the world continues to recover (and learn) from the ensuing recession, leveraging technology to institutionalize trust and prevent corporate abuse and corruption is a central driver of the ongoing development of blockchain. Transparency, accountability, and security are intrinsic to its makeup.

"For everyone involved, blockchain is about building for trust and an upside that outweighs the risk," observes Jonathan Vaux, executive director of new digital payments and strategy with Visa Europe. "This technology is boundary agnostic. Blockchain shines a light on that and will force companies to restructure incentives for trust."

Figure 2.2 Blockchain Trust Equation

(Source: Tractica)

Value in blockchain is about visibility and speed. Digital transactions are executed via network consensus; once verified, they are irreversible, immutable, traceable, and thus auditable. The automatic and secure execution of "smart contracts" and transaction processing reduces costly settlement and reconciliation inefficiencies for all parties. With a single "truth" stored in a distributed shared ledger, the methodologies enabling trust today suddenly appear inadequate, impractical, and obsolete.

2.2.3 Increased Efficiencies Emerge When Code Mediates Transactions

It may seem counterintuitive that a distributed computing architecture would engender greater efficiencies than one centralized to a single actor or database. But in fact, shared and distributed architecture leads to process and operational simplification.

On a blockchain, transactions can be registered from any permissioned device, event, or user; input data can be immediately processed in blocks, verified across a network of nodes, and via smart contracts can trigger additional services. These automated functions facilitate a host of process and operational efficiencies that have enterprises worldwide paying attention. A few examples are listed below.

- **Clearing and Settlement Time Reduction:** Entire industries exist today whose sole purpose is to verify transactions and validate settlement, often over the course of days or even weeks. For transactions involving numerous counterparties, asset types, documents, systems, geographies, and regulatory requirements, tremendous inefficiencies and frequent disagreements prolong reconciliation. DLT can automatically handle many aspects of identity, credit, or document verification, review, transfer of funds or titles, and many other reconciliatory processes in a fraction of the time. Account activities are updated simultaneously. All participants in the chain can see where documents are in sequenced approval processes, who is reviewing them, and over what time period. Disagreements and mistakes are reduced as authorizations are transparent across counterparties. Fewer errors and disputes translate to less frozen capital, and greater availability for new trades.
- **M2M Microtransactions:** Although M2M connectivity has been around for decades, blockchain technology helps bridge systems and process efficiencies that take M2M from connectivity to transactions and services made possible through connectivity and the resulting flow of data. For example, a leaky pipeline's sensors could not only communicate the issue, but through smart contracts, process the transaction documentation necessary to automatically and securely trigger operational queues and communications, automatically submit and verify insurance claims, solicit repair services, and even allocate payment across counterparties. Not only does this reduce risks associated with malfunction (which can be dangerous or even deadly), it saves headcount, time, and costs related to identifying and resolving the problem, as well as reconciling information and transactions for those involved.

- **Counterfeit Resiliency and Fraud Mitigation:** Adding authenticated transactions, contracts, events, identities, and other "truth states" onto a shared ledger makes counterfeit, tampering, and fraud far more challenging and costly for perpetrators. Fraud, forgery, and counterfeit costs run in the billions each year, and span numerous use cases, from product provenance to financial transactions to academic certifications. Registering an item digitally "at source" on a distributed ledger creates an immutable, digital representation of the item, which makes forgery much more difficult.

  Efficiencies include reductions of revenue loss due to fraud, as well as reductions in time and costs associated with investigating and processing fraud, as well as the headcount required to monitor and train accordingly. Other benefits of fraud mitigation have broader impacts—false identities, documentation, and certifications underlie much of the world's organized crime, such as human trafficking, money laundering, terrorist financing, financial fraud, and so on.

- **Ownership or Access Transfer Automation:** When it comes to high-value assets, trust (or a lack thereof) underlies the transfer of both ownership and access. Transferring the title of a home or estate is a process requiring numerous counterparties, many phases and document verifications, and typically involving lots of money. If not transferring ownership, authenticating access to assets (e.g., cars or apartments in a shared economy context) can also a cumbersome process, around which an entire industry of "trusted platforms"—middlemen—has emerged.

  Whether transferring large assets such as real estate or streamlining secure, permissioned, and legal access to shared services, DLT helps automate traditionally cumbersome, costly, and time-intensive legal processes and documentation. DLT helps reduce actuarial risk, which reduces the number of insurance claims as well. In the context of real estate, significant efficiencies result from streamlining document validation, certification, inspection, and the headcount and fees associated with each.

- **Regulatory Compliance Automation:** Regulatory compliance is a cumbersome and costly exchange for both the regulated and the regulators, but required for safe, secure, and sustainable business operations. Regulations change over time and vary widely across industries, products, geographies, and institutions. Many regulations require extensive verification and multiple parties to enact, review, and verify, with violations resulting in legal punishment and fines.

  Instead of a retroactive review of events or processes each requiring their own audit, DLT enables companies to program compliance into transactions so that compliance is encoded into operation and transaction. Another major efficiency blockchain offers regulatory compliance is the ability for real-time monitoring of activities, as regulators can access the ledger to view all transactions and assess compliance.

- **Multi-Party Risk Reduction:** Blockchain is best suited for instances and transactions that involve multiple parties. Of course, when money, high-value assets, and risk are part of the picture, trust erodes, or is precarious at best. Instead of relying on semi or unknown counterparties to comply and fulfill agreements, many contractual obligations can be encoded into transaction execution, and recorded immutably on a blockchain.

- **Distributed Fiat and Liquidity:** If central banks approved digital fiat currency within distributed financial infrastructure, users would have better transparency and liquidity of assets. This efficiency also applies to numerous specific processes within trade and investment, such as asset hypothecation, repurchase agreements, equity post-trades, and others.

- **Security:** Blockchain architecture holds great potential for enhancing systems and data security. Advancements in cryptography and the distributed nature of blockchain platforms render hacking far more difficult and costly than that of hacking into a single database. Not only does blockchain hold the promise of security improvements at the structural level, but it could also lower costs associated with security management, as multiple participants require fewer proprietary systems and could conceivably share responsibilities for IT security management. (A deeper outline of security efficiencies can be found in Section 2.2.4.)

Protocol-based trust distributed across a network offers significant potential to drive simplicity and efficiency in processes, infrastructure, and reduction of corruption. These efficiencies cut across numerous industries, and in many cases, beget greater efficiencies indirectly by, for instance, empowering employees with real-time analytics or simplifying processes and eliminating fees for consumers. (Reference the use cases in Section 4.1 for more vertical-specific examples.)

2.2.4 ENHANCED SECURITY

Another driver of the blockchain space is its potential to significantly enhance security. Operationally and culturally, security advancements enabled by blockchain foster trust, but such advancements have IT and architectural benefits as well.

While acknowledging blockchain's nascence, Tractica's analysis finds it reasonable to assert that blockchain is a true breakthrough in security technology because the architecture allows users to trust the result that the network provides, even if some of the participants in the network are malicious actors. The notion that in a world of constant and increasingly sophisticated cybercrime, we can have a reliable and resilient network infrastructure, even if some of the players are corrupt, is a revolution in trust enabled by technology.

In the more than 7 years since Bitcoin's blockchain's birth, the blockchain itself has never been successfully hacked. Even during the recent fall of the Decentralized Autonomous Organization (DAO) (see Section 3.1.6), the Ethereum blockchain itself was not hacked; the penetration was a result of poor governance of the contracts and bugs in the code. Even in other hacks, such as the recent $72 million in stolen Bitcoins from Bitfinex, the breach took place on the blockchain exchange, not the platform.

A *distributed* ledger system means there is no central environment that is the source of all trust or control. Instead, all work and records are distributed across all participants. Not only is work distributed, but nodes must agree on the existence and validity of each transaction. Once processed, the ledger is not only shared, but immutable, relying on the integrity of past transactions, and foundational to the validation of future transactions.

These characteristics foster an environment that is incredibly secure *because the cost of compromising the system outweighs the benefit.* It would be very difficult to compromise the ledger, because it is not just about penetrating one database, but would require editing many (thousands or even millions) databases. "The distributed nature of the network that verifies the integrity of the transactions and associated account balances makes a successful attack mathematically impossible," says Judd Bagley, Director of Communications at Overstock.com.

Control by the network helps prevent user, device, account, and transaction fraud; counterfeit assets; and automates anti-corruption compliance. Blockchain technology inherently makes fraudulent behavior and cheating the system much more difficult because tampering with a transaction messes up all of the calculations thereafter, thus exposing the cheater, or at least the presence of an attack. It represents a way to ensure consensus-

based trust between parties that may not inherently trust each other. Each of the following technologies help augment security in distributed ledger environments:

- **Smart Contracts:** Smart contracts are the first line of defense in that they provide the opportunity to write security rules into the execution of the transaction by placing logic (pre-determined protocols and programs) directly into the blockchain code.
- **Identity Verification:** The concept of using blockchain to underlie tamper-proof identities is gaining significant traction in security and privacy circles. Data about the transaction must be encrypted, use digital signatures, be cryptographically secured, and accessed only by those in need of immediate read or write access authenticity and enforcement.
- **Data Management Protection:** Companies use external data feeds to augment their own proprietary data sets. Although this makes for richer data and efficiencies, it introduces significant security risks because it is involving third parties, each with a host of unknowns. Oracles are an example of a technology that simplifies the connectivity between a smart contract or cryptocurrency and external data feeds.
- **Multi-Party Computation (MPC):** An emerging practice of using joint peer-to-peer (P2P) networks to run computations on data while maintaining complete privacy of the data. The process uses an external blockchain to manage access control, identity, and tamper-proof logging. (See more on MPC below in Section 3.1.4.)

Numerous sophisticated (and ever-evolving) security features can diminish the likelihood of breach. Microsoft recently developed Cryptlets, a set of services that can be written in any programming language serving as a sort of gateway to allow companies to bring in only trusted data from outside the blockchain system without breaking the security of that system.

Another emerging security lever is placing certain data off the chain entirely. For data meant to be publicly visible, transparency is an enabler of security and trust. But for many business or governmental applications, many data are extremely sensitive, meaning they become targets for bad actors. Payment data, confidential contract information, medical or genomic data, trade securities data, among a host of other examples, are maybe best kept off the network. “An effective mechanism for greater security and privacy protection on distributed ledgers,” explains Sergey Nazarov, CEO of Smart Contract, “is putting the minimal amount of data on the network, which keeps contextual data about the contract off the network.” Using off-chain oracles can allow the same or better computation to happen for the smart contract’s use without revealing its potentially sensitive nature.

Careful configurations of the above (and no doubt new developments in security beyond the scope of this report) offer advancement opportunities in mitigating the current risk levels within most IT security departments today. Indeed, humans will remain a tremendous weakness in any system, given the prevalence of simple phishing attacks, poor password protection, lack of security training and governance, and good old-fashioned human error. Moreover, blockchain technology cannot play the inevitable role of arbiter in the event of dispute. Acquiring the skillsets to address security across the entire lifecycle of blockchain development and management is essential. Each component used in security logic relies on architects and security experts to build business rules that prevent malicious behavior, complete thorough end-to-end testing and verification of all code. (Reference Section 3.1.3 for a deeper discussion on the technological security considerations of blockchain.)

2.2.5 Cost Reductions and Business Model Impacts

Tractica’s research finds significant cost savings potential in this technology. It is important to recognize that the savings we have identified are not actual today, but rather would

logically result if/when key counterparties adopt DLTs. Although each use case and industry's financial, technological, and regulatory requisites and opportunities vary, cost reductions associated with blockchain architecture tend to fall into the following categories:

Reduced Risks | Fewer People | Fewer Systems | Less Infrastructure | Reduced Costs

- Reduced latency and increased liquidity through automation of transactions (e.g., transfer of energy, data, documentation, money, etc.)
- Reduction in costs and fees associated processing, investigating, and reconciling errors, issues, claims, fraud, unmet compliance
- Reduction in labor required for processing, investigating, and reconciling errors, issues, claims, fraud, unmet compliance (e.g., "middlemen" industries)
- Reduction in costs associated with regulatory penalties
- Reduction in IT systems costs due to fewer systems; users could share costs of maintenance and security
- Reduced impact of infrastructure malfunction, waste, fraud, etc.
- Reduction in costs associated with piloting or integrating systems across partnerships
- Increased visibility
- Increased liquidity means more capital available for new trades

Suppliers of blockchain technology—private blockchain platforms and applications—typically monetize through a subscription model, a transaction-based fee model, or a combination of both. Some vendors are also licensing their platforms to third-party developers.

Given the early days of the market and the imperative for deep technological *and* business context required to develop effective DLT solutions, many vendors are building out robust consulting services in order to educate, guide, prototype solutions with clients, and translate best practices across their portfolios.

For vendors supporting asset provenance, other services that can supplement this include but are not limited to:

- Automated asset tracking via sensors/IoT technology (e.g., radio frequency identification (RFID), barcodes, etc.)
- Monetization of services made possible through data collected across participants (e.g., weather data via distributed energy platform is collecting sensor readings in aggregate)
- Monetization of data transparency and certification of assets
- Charging and settlement for asset-based insurance and financial products (via smart contracts)

For adopters of the technology, new business models and net new revenue streams made possible by blockchain are far less predictable than its cost reductions. As a primarily back-office architecture, blockchain's operational benefits will be easier to digest (and justify investment) than its impact on front-office processes. Once blockchain technology is implemented, enterprises are likely to discover new ways to use data to generate new forms of value. Tractica's research finds that early signals of net new revenue associated with blockchain emerge when blockchain underlies or streamlines other emerging business

technologies, namely the IoT/M2M applications, artificial intelligence (AI), and other enablers of micro-transactions.

"Revenue enhancement kicks in when companies use blockchain to create programs that were either impossible before, or that they couldn't have created without huge investment," explains Ron Quaranta, COO of loyyal, a blockchain-enabled platform for multi-brand coalitions in the loyalty space.

Organizations like SolarCoin are getting users to buy into solar energy for rewards in SolarCoins, which can be cashed in. They are also beginning to look at ways of monetizing this data, effectively registering temperature data collected via the sensors from solar panels to supplement applications such as weather modeling to drive new revenue streams.

2.3 MARKET BARRIERS

Despite the array of benefits blockchain *could* enable, the technology faces numerous significant barriers to achieving widespread or enterprise-scale adoption, causing some to question its fate altogether.

Those most involved in blockchain development tend to have the most sober point of view; every constituency Tractica interviewed stressed *just how early we are* in our collective understanding, exploration, and application of blockchain technology. **These are early, even infantile, perhaps even primordial days for blockchain.**

2.3.1 REPUTATION HURDLES IN A NASCENT MARKET

This nascence introduces a host of existential tensions in and unto itself. Such an infantile market desperately needs definition, standardization, and deep collaboration to come to fruition at any kind of scale. Below is an outline of the variety of dynamics characterizing the current state, momentum, and development environment in the blockchain market.

- **Shifting Lexicon:** Like the space itself, the terminology used to describe it remains highly fragmented: blockchain, DLT, shared ledgers, mutual ledgers, open ledgers, distributed concurrence ledgers, Blockchain 2.0, automated consensus, protocol-based trust systems. For Tractica's purposes, and for the purposes of this report, we use blockchain and DLT as generally synonymous. Readers should understand that blockchain often refers to public/permissionless blockchains (à la the Internet), while DLTs often refer to private or hybrid blockchains (à la intra-nets or IT systems).
- **Flurries of Investment:** According to CoinDesk, investment in blockchain (versus Bitcoin startups) increased from 2% to 84% of venture capital (VC) investment between 4Q 2015 and 1Q 2016. Approximately 80% of banks are expected to have invested in blockchain by 2017, according to the World Economic Forum. A recent IBM study reports that approximately 15% of banks will be using blockchain technology by the end of 2017, although it is worth noting IBM itself is a major player in the space and funded the study.
- **A Proliferation of POCs:** The blockchain space can be characterized by rapid experimentation; Barclay's bank, for example, planned approximately 45 experimentations for 2016. From financial services to healthcare, governance, manufacturing, agriculture, retail, and beyond, companies are experimenting with blockchain, yet Tractica finds very few (if any) fully scaled, reliable, in-production blockchain applications beyond Bitcoin blockchain.
- **Associations with Cybercrime:** Part of the move from Bitcoin to blockchain (in investment, language, and market organization) has to do with disassociating the

technology (and its potential) from Bitcoin—a technology with a turbulent history of volatile market fluctuations, cybercrime, and the Silk Road, and often associated with underground hackers and individual agents (not multi-national corporations or highly regulated industries).

- **Opposing Philosophies:** The ongoing debate, fragmentation, and investment trends between public versus private blockchains underscores the bifurcation between: 1) individuals motivated by decentralized transactions and disintermediating large institutions—the impetus for the Bitcoin blockchain; and 2) those institutions protecting centralized, highly permissioned transactions. Each represents distinctly opposing philosophies, and both are driving the development of the technology. This philosophical difference underscores an ongoing debate over the very definition of blockchain; purists of the original open and permissionless blockchain community dispute that private systems with permissioned actors (by a central authority) should not be considered blockchains at all.
- **Another Day, Another Press Release:** Calling attention to the extensive hype in the blockchain space, many stakeholders Tractica interviewed point to the endless stream of press releases coming out of corporations hiring blockchain-related talent, partnering with consortia, or conducting experiments. “People sneeze and say blockchain and it gets a press release,” Adam Ludwin, CEO of Chain, said recently. Handshakes and other “single-day” affairs do not constitute innovation, (even if they signal an innovative spirit), and those approaching the space must parse headlines from real application.
- **Bandwagon Effect:** In the technology space, buzz goes a long way. Investment driven by paranoia of disruption or loss of market share; marketing to drive SEO in buzz-worthy areas; and the ensuing network effect of Internet echo chambers foster a bandwagon effect. Having seen the Internet, social media, and other recent disruptions destroy slow-moving brands, many companies are jumping on the blockchain bandwagon without a clear sense of precisely where, when, and why to focus.

These dynamics make for a frenetic market environment, one in which a wide range of constituencies must collaborate.

2.3.2 THE NETWORK EFFECT

One of the unique barriers to blockchain deployment is the difference in value the technology delivers when it is deployed at scale versus with few participants. The “network effect” (and imperative) basically refers to the fact that, in a distributed ledger architecture, the broader the set of constituencies that participate, the more valuable the system becomes. Deploying blockchain-enabled transaction architectures requires multiple constituencies align, coordinate, and encode shared processes, governance, and adherence before any single one can succeed. Unlike many other emerging technologies, which can be piloted and even deployed by a single organization, achieving critical mass for blockchain deployment is a significant challenge. That just about every use case for this technology involves the exchange of value (e.g., money, energy, products, etc.) requires that the following must be solidified before deployment at scale:

- Clear monetary regulations and policy
- Governance frameworks (at operational and technical level)
- Regulatory measures, compliance, and liability frameworks
- Integration with current systems
- Security, privacy, permissions testing

- Collaboration and buy-in across required counterparties
- Communications plans

Unlike deploying a private cloud or setting up a corporate Twitter account, this technology requires *extensive* time, multi-disciplinary collaboration, and often unprecedented testing before deployment. Yet without any at-scale enterprise deployments to observe, many corporations remain highly skeptical. This reticence also underlies the corporate impulse to limit the number of participants in network as much as possible—a tendency some assert defeats the very point of blockchain technology.

"Corporations looking at this will eventually realize the power is not in un-distributing a distributed ledger, and rather it's the broad system that allows for maximum privacy and transparency at the same time," offered an executive interviewed who wished to remain anonymous.

As the technology matures, this issue will dissolve, but it will be a signature challenge for the entire market to get off the ground on the enterprise side.

2.3.3 Significant Collaboration and Infrastructural Development Required

The level of collaboration required for the successful and sustainable deployment of DLT is significant and will, in many instances, be entirely unprecedented. This theme surfaced across nearly all of Tractica's research interviews. New technological innovations often require intimate interactions between hitherto "strange bedfellows." Blockchain will not just require that estranged participants come together, but also demands multi-disciplinary integration to define new laws, rules, liability frameworks, standards, processes, ontologies, and definitions.

One of the most important areas for collaboration is in the development of logic and templates that translate the nuance of existing processes, laws, and frameworks to smart contract execution. Fostering an environment for this type of collaboration is a central role and enabler of consortia such as R3, the Hyperledger Project, or the International Blockchain Real Estate Association.

"There is a deep need for integrated development environments," says Nell Watson, associate faculty with Singularity University. "Most programmers are not lawyers and vice versa. Smart contracts are an incredibly powerful technology because they are disruptive to all sorts of frictions that get in the way of getting things done. The challenge comes in creating contracts that can be easily understood by both machines and humans, understood and built from both a programmatic and legal perspective."

2.3.4 The Need for Governance and Stakeholder Alignment in Decentralized Structures

We live in a world where centralized systems are the de-facto standard for our understanding of societal structures. The ability to process transactions directly between parties *without* a trusted intermediary—whose role is typically to reduce counterparty risk— is not just a significant cognitive and cultural hurdle for enterprises (and many consumers) to overcome, but a strategic one as well.

"It's very different to reckon decentralized solutions with centralized thinking" explains Arno Laeven, an independent blockchain consultant formally leading blockchain research with Philips. The question often comes back to "OK, but who is responsible then?"

Because smart contracts are essential mechanisms for building both automation and compliance into blockchains, they must reflect the "if-then" discrepancies and triage entrusted in human discernment. In complex multi-stakeholder processes, writing business logic into a blockchain application must be a result of consensus-based decision-making. By the accounts of many Tractica interviewed, considerations for governance and stakeholder alignment are the *essential* first step to blockchain development.

Key questions surfaced during research center around the following areas:

- **Objectives:** What is the central function and scope of the shared ledger? What are the criteria for its expansion or contraction?
- **Data Access:** Who can access what data, when, and to what extent? How will we manage and secure permissioning and authentication?
- **Intervention:** What are the mechanisms for governance in a decentralized computing architecture, and how does context determine fair intervention?
- **Accountability & Liability:** Should the system or users of the system experience compromise, who is responsible, how, and under what specific scenarios?
- **User/Consumer Benefit:** How do users benefit and what do they gain in return? How will we communicate and deliver on this?
- **Social Impacts:** Machines do not understand intent, nor can they grasp cultural nuances such as ethics, fair use, or disenfranchisement. How can we program discernment for what is sensitive and when into smart contract execution?
- **Decentralized Decision-Making:** How will decisions be made across stakeholders throughout the deployment and rollout of the technology? How will stakeholders learn from failures and share best practices?

Many point to the DAO as a cautionary tale for what can happen when proper governance is not established. (Reference Section 3.1.6 for more information.) It is also a reminder that much of this discourse should take place at the societal level, not solely among financial institutions and their consortia.

"Building a blockchain-enabled world begins with governance," says Jesse McWaters, Financial Innovation Lead with the World Economic Forum. "This isn't just about creating guiding principles for what the system should do and to whom the system reveals which attributes and when, but asking fundamental questions about what kind of world we want to live in and how we can build for that."

2.3.4.1 POLICY, LEGAL, AND REGULATORY PRECEDENTS REQUIRE OVERHAUL

To achieve commercial blockchain deployments, many significant policy and regulatory issues must be addressed. This may be the single greatest roadblock facing commercial blockchain deployments. Legal and policy questions swirling around blockchain are diverse. In some cases, such structures have precedents that are hundreds of years old, while others are new legal territory, all but entirely unchartered.

Tractica's research surfaced the following critical areas that a majority of enterprise-grade blockchain deployments will face:

- **Monetary Policy and Central Banks:** The most foundational regulatory challenge facing blockchain is obtaining governmental validation and leadership to validate central bank digital currency. This question forces a re-evaluation of the very definition of money, its

creation, its variations, and its provision. Governments could operate digital currency networks themselves, issue digital assets, manage those assets, and create products and services to run on such networks, or they could simply observe the networks. Several of the world's central banks, including the Bank of England, the People's Bank of China, the Bank of Canada, and the Federal Reserve, are exploring the idea of issuing their own digital currency. Given the trillions and trillions flowing across a vast global financial ecosystem today and the risk of added instability to markets, these questions will not be solved overnight.

- **Smart Contracts:** To integrate financial and operational transaction execution requires contract law to be encoded onto the blockchain. This task is easier said than done and requires significant collaboration between lawyers, regulators, business practitioners, and developers. Once coded, regulators would still need to determine if legislation were sufficient, or if they would need to regulate distributed ledger code itself. Moreover, enforcement itself requires re-assessment; if an issue is identified in the code, who is responsible and how are penalties defined? What about in the case of entirely decentralized autonomous (read: unincorporated) organizations? Of course, encoding smart contracts has inevitable limits and would not eliminate disputes. Thus, court systems, lawyers, and regulators themselves would need to become highly familiar with smart contracts and their development, as well as evidentiary rules and record-keeping requirements that determine data access.
- **Digital Identity:** Across both government and financial services, identity verification is essential for engaging in economic transactions and conducting affairs and accessing state services. Know your customer (KYC)/anti-money laundering (AML) compliance is one example of a regulatory requirement in which banks must verify clients' identities, but there are countless other identity-related regulations and region-specific variables that require attention in order to "transfer" identity to a blockchain. Many of these regulations must be re-written or developed in the first place to incorporate risks, accountabilities, and considerations for digitizing our very selves.
- **Dematerialized Environments:** In securities trading, among many other industries, physical paper certificates are still the standard form of documentation and accepted credit. Such documents must not only be digitized to enjoy the speed and fraud controls offered by blockchain, but the laws that govern these environments must be updated or created to articulate their acceptance.
- **Human versus Machine-Registered Audit Trails:** Blockchains can be used as registries for records of ownership in a real estate context and as proof-of-process compliance in a supply chain context, thus regulations must also reflect the validity of code-executed information. These audit trails are critical for compliance, but today they still rely on humans to verify registration.
- **Cross-Border Standards:** Networked technology confuses and often defies the "clear lines" of jurisdiction. Blockchain's distributed architecture only amplifies this because its architecture consists of multiple nodes, many of which will exist across borders. Rules governing securities law, aid to criminal conspiracies, and consumer protections could be violated inadvertently by blockchain applications. Prediction markets relying on inputs from anonymous sources, for instance, could violate U.S. gambling laws. Standards would need to be negotiated and created not just domestically, but as they apply internationally as well.
- **Anti-Trust:** In private blockchain deployments, it is not far-fetched that arguments of monopolistic activity might emerge in the event of disputes. Could algorithms be set up or edited in a way that produces anti-competitive results? How would regulators detect

these, particularly when results may not be readily accessible without private key access?

The regulatory challenge for blockchain creates a "chicken and egg" problem, in which all parties (i.e., governments, regulators, enterprises, intermediaries, etc.) are uncertain and hesitant to act; yet parties must act together to achieve the greatest and most rapid benefit. Without the incentive created by network adoption, parties will continue to stick to the system that works. The costs of unknown risk outweigh the costs of known risk.

Another notable dynamic at play is that regulators potentially have a double-sided benefit in the DLT. First, compliance measures could literally be encoded up front; that is, written into the code of smart contracts dictating the execution of the transaction. After all, the great benefit to regulators is the practical immutability of information on the blockchain. Once data is saved into the chain, it cannot be changed or deleted. Time, costs, and labor required for reporting and the need to prove compliance are reduced because transactions simply would not go through otherwise. Costs and damages would also be reduced for customers. Secondly, regulators would be granted permissioned access to monitor compliance in real time through blockchain-integrated dashboards. This would save regulators tremendous costs associated with auditing, investigations, validation, recordkeeping, and crime prevention.

"Regulators today are very interested in understanding how blockchain works," says Kari Larsen, Counsel at Reed Smith LLP and former GC and COO of LedgerX. "But rarely are regulators themselves technology experts. The trend we see today is regulators want a regulatory sandbox for testing. They want to observe where benefits and risks are for customers, but don't want to crush innovation."

In many ways, technology is not the challenge of blockchain deployment. It is the challenge of standardization that separates society of today and the decentralized, autonomous, and efficient revolution envisioned for tomorrow.

2.3.5 Blockchain Calls for Redefining Identity and Data Ownership

Identity on the blockchain exists dually as the user identification (ID) mechanism on a blockchain and more broadly as the concept for who or what defines the participant in a transaction. Identity on blockchain is interwoven with just about every other critical concept defining governance in a decentralized economic architecture—access, authentication, accountability, privacy, and verification. The sheer scope of this concept in blockchain renders it a profound opportunity and risk at once.

Identity traditionally accounts for specific societal identifiers, such as name, address, Social Security number, birth certificate, estate, etc., and is therefore central to streamlining blockchain use cases such as those involving government, real estate, and finance. Moreover, identity on blockchain may digitize identity in ways that are not formally digitized today, but are essential for accumulating trust in a decentralized system—for example, reputation. One's digital identity might incorporate numerous levers for trust, each applicable in different areas, but centralized to a single, and maybe user-controlled, digital identity access management solution.

- Resident ID (state-issued documentation, registration, address, etc.)
- Banking ID (account, asset, equity, credit, financial history, etc.)
- Biological ID (biometrics, medical history, genetic history, etc.)
- Employment ID (employer, role, accounts, security clearance, etc.)

- Trade/Certification ID (Trade, education, certification, etc.)
- Loyalty (company-issued loyalty programs, memberships, etc.)
- Reputation (an individual's standing within any business or social interaction)
- Device History (past and present login history across devices)
- Other ID (lifestyle, hobbies, general ID authentication, etc.)

Perhaps what is more disruptive than formalizing the digital organization of our selves is the notion that users (those generating the data), not companies (those collecting the data), control their own data. Identity in blockchain-based systems could be owned and operated by the user, unable to be manipulated, confiscated, sold as commodity, or censored by any central service provider. This is the fundamental and profound difference from the digital identity with which we are familiar today on centralized platforms such as Facebook or Google.

"Identity is very cultural; people have strong, engrained preferences for whom they entrust their identities that are culturally and historically determined," observes Jesse McWaters, Financial Innovation Lead with the World Economic Forum, "a model with multiple identity validators working with multiple users, characterized by an architecture that is either federated or distributed gives people the choice."

Blockchain and digital identity have a complementary relationship. Blockchain can be an underpinning to digital identity, but digital identity enables blockchain use cases. Identity fits all of the characteristics of ideal use cases for blockchain: multiple counterparties, a need for shared access, security, highly permissioned control of interactions and transactions, and a mechanism that is terribly inefficient in its current structure.

Figure 2.3 "On the Blockchain, Nobody Knows You're a Fridge"

(Source: Teespring.com)

Identity access on the blockchain also includes the notion of devices themselves being "actors" on the chain. Like other actors, identity would be obscured in many transactions. In a shared economy example, an autonomous car taxi service would no doubt require the car itself to act, authenticate, negotiate, conduct transactions, and secure itself (autonomously) and in ways traceable to that specific vehicle. As blockchain consortium R3's CTO Richard G. Brown is famous for saying, "on the blockchain, nobody knows you're a fridge."

There is an enormous need to take today's identity protocols, which are largely insecure, siloed, complicated, and fundamentally not centered around the user, and revolutionize those where identity is more controlled by the user, but the handling of identity is a much

more streamlined process. (See Section 4.1.4 for an expanded discussion on identity mechanisms as a use case for blockchain.)

2.3.6 THE EVOLVING QUESTION OF PRIVACY ON THE BLOCKCHAIN

Privacy is an evolving debate in the blockchain community. While the definition of privacy has fundamentally changed in the digital world, our research finds that blockchain may offer advancements in protections for our "digital selves" compared to traditional siloed database architectures. On its face, the inherently transparent, shared, and immutable nature of public blockchain architecture undermines the notion of highly sensitive, potentially exploitable information about individuals. But we all have an interest in privacy preservation, whether individuals developing public blockchain architecture or enterprises interested in private blockchain architecture. Adoption for both depends on trust.

Public blockchain ideology deeply values anonymity and individuals' protection. Weaving these concepts in with transparency and accountability was the whole point of the original Bitcoin blockchain, which handles security through verification in which participants can individually and autonomously validate transactions. That said, even the ability to encrypt the body of the text does not necessarily obscure details that can be deduced and analyzed from the header. Despite pseudonymous addresses, many Bitcoin experts say it is still technically possible to re-associate individuals with their addresses. Thus, it is possible that security may be somewhat offset by a reduced level of secrecy; even if the "jewels" of the transaction remain secure.

The context of privacy incentives for companies is more complex, and evolving. Today, the organizations *collecting* data from users *own and control* that data—not the users generating that data. While many users remain unaware of this, highly detailed profiles of our digital behaviors, likes, clicks, social graphs, and so on are now available to marketers and employers, and brokered by an entire industry of companies that buy and sell consumer data as a commodity. Moreover, most companies have complex data management chains in which they outsource or sub-contract some part of the management or processing of their data to drive greater efficiencies. This has the simultaneous effect, however, of widening the landscape of security threats, as companies are supposed to ensure that such third parties protect and safeguard their data against attacks. Companies that are data controllers of massive amounts of personal data, such as Google, as well as financial institutions, face significant regulatory obligations regarding IT outsourcing. In just a few years (2018), the European Union's (EU) General Data Protection Regulation (GDPR) will require far more stringent adherence to data security and privacy. Regular audits and steep penalties in the event of data breaches will cost businesses millions or tens of millions of Euros.

As enterprises' livelihoods depend more and more on harnessing ever-growing volumes of data, businesses have no choice but to evolve their data security strategies. Blockchain could play a very interesting role in this evolution.

The many institutions investing in private and hybrid blockchain development are not just prioritizing privacy to be ethical, they have a business interest in preserving it. In order to achieve the efficiencies businesses seek in blockchain, private blockchains must satisfy certain compliance requirements related to privacy. In fact, much of the activity and piloting by financial services institutions in capital markets use cases are centrally focused on how to achieve speed, scale, and reliability, while also preserving privacy and confidentiality. Must building for privacy and confidentiality compromise transparency (or vice versa)?

Technological configurations supporting privacy on a blockchain take many forms and are one of the central areas of blockchain research and development across both public and

private blockchain communities. Emerging technological mechanisms for cryptography, encryption, and authentication offer new tools for protection, and may alter the narrative around privacy in the digital age. (See Section 3.1.4 for an outline of the critical emerging technologies for privacy protection in DLTs.)

2.3.7 A Need for Simplicity

While the functional advancement of blockchain may simply be a shared, immutable database, it is a complicated concept to grasp structurally and economically. Its architecture is highly complex, and it is difficult to explain succinctly to most people. The extent to which this is a barrier to adoption is yet unclear. What is clear is that all "killer apps" must be simple and intuitive and efficiencies easy to leverage and understand.

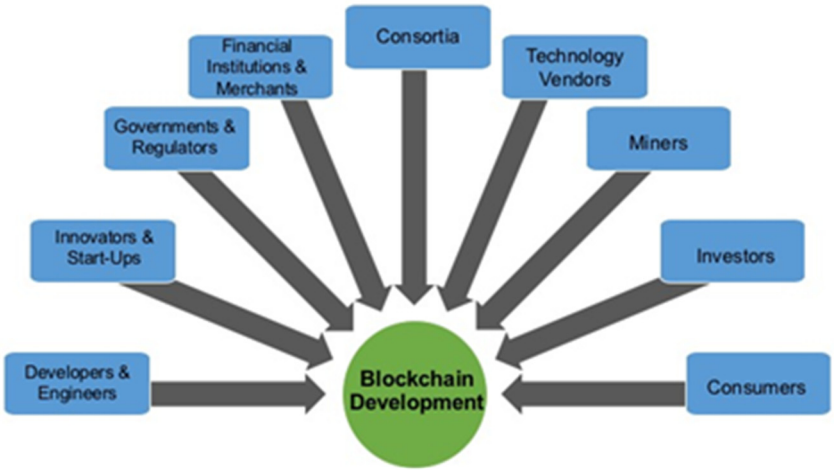
Beyond technological and regulatory hurdles, classic sociological forces may dictate blockchain's eventual role in the transfer, control, and economic management of personal data. A consumer's will to engage and entrust some sort of "mother" database with their information requires that centralized entities foster trust, simplicity, and deliver convenience.

2.3.8 A Wide Range of Constituencies Influence Blockchain Development

The primary market trend from 2014 to 2016 in this space was characterized by a shift in emphasis (i.e., investment, publication, research, google searches, etc.) from Bitcoin and cryptocurrency-centric applications, to blockchain and DLT, including non-currency-centric applications. This shift has impacted the composition of those interested in the market, and more importantly, contributed to its development.

Constituencies interested in blockchain development are diverse. Interests range from complete political and economic decentralization on one end, to lucrative opportunities to drive business efficiencies and increase the bottom line on the other end.

Figure 2.4 A Wide Range of Market Constituencies Influence Blockchain Development



(Source: Tractica)

2.3.8.1 Developers and Engineers

Blockchain as a concept was born in, incubated, and remains a central focus in the developer community. Worldwide, there are already thousands and thousands of developers and miner groups. Even among developers employed in enterprise environments, open online

communities, Slack groups, GitHub, and real-life developer environments serve as forums for ideation, sandboxing, and collaboration.

Meanwhile, more and more developers are flocking to the space. According to Coursera, approximately 35,000 people have completed the introductory "Bitcoin & Cryptocurrencies Technologies" since 2015. A recent session in September 2016 had more than 45,000 students enrolled. As of mid-September, 2016, a search on job listing site Indeed.com for "blockchain" returned more than 265 listings.

2.3.8.2 STARTUPS AND INNOVATORS

Financial technology or "fintech" startups have been impacting the operational and economic narrative for banks for years now, but the realization that there may be many millions, potentially billions to be made with blockchain has inspired a groundswell of activity by startups. A number of these startups are brainchildren of the more entrepreneurial ilk of Bitcoin enthusiasts, who bring experience in related technologies, such as sensors/IoT, automation, or cybersecurity. Perhaps unsurprisingly, Tractica also found that a number of leadership figures in the blockchain startup world are veterans of large banking corporations. By our estimates, there are already more than 400 startups across various parts of the blockchain stack, including both cryptocurrency and smart contracts. As startups are cropping up across the blockchain application space, many of the world's largest corporations are also making waves in the blockchain story.

2.3.8.3 FINANCIAL INSTITUTIONS AND MERCHANTS

Today, more than 90 banks worldwide and dozens of governments are investigating and investing in blockchain and distributed ledger initiatives. The increasing role of these powerful corporations in funding, acquiring, or partnering with those startups now dominates the lion's share of activity in the blockchain market. The World Economic Forum predicts that approximately 80% of banks worldwide will initiate DLT projects by 2017.

The development of blockchain has split from its original public, permissionless vision, to one driven by corporations that see financial benefit in fostering trust, but are incentivized by blockchain's other benefits. Beyond philosophies and intentions, enterprise adoption impacts blockchain's and has redefined blockchain's architecture from fully and openly distributed, to somewhat distributed, or distributed only across other parties. For example, the Bitcoin blockchain has thousands and thousands (soon millions) of miners and users, whereas some financial institutions are piloting DLT concepts among just six (similar) institutions. While critics argue that such activity is altering the very point of blockchain, it is hardly surprising that such risk-averse companies are already dipping their proverbial, and somewhat paranoid, toes in with the utmost caution. Financial markets have a lot at stake after all.

The vast majority of enterprises making moves in this market are financial institutions, although automotive original equipment manufacturer (OEM) Toyota and e-retailer Overstock.com are conducting finance-related experiments. Global device manufacturer Philips has also been investigating the technology for healthcare applications.

Notable Actors: Santander, Deutsche Bank, HSBC, Barclays, Depository Trust & Clearing Corporation (DTCC)

2.3.8.4 WORLD GOVERNMENTS AND REGULATORS

Like financial institutions, governments and regulators are leaning into the blockchain space with increasing spending as they begin to understand the potential for security and efficiency

gains, cost reductions, impacts on identity, and the opportunity for disintermediation of their own orbits of middlemen. Regulators themselves stand to gain significant efficiencies and protections through automating compliance using DLT, both in the reduction of inadvertent non-compliance, as well as their ability to play a proactive (not reactive) role in monitoring and auditing. (See Section 4.1.5 for more information on this use case.) Today, this technology is on the radar of more than 100 central banks, and more than 25 countries around the world are investing in DLT efforts.

Given modern society's reliance on centralized bodies, the adoption of, not to mention the transition to decentralized structures, raises many issues around governance. So much uncertainty around the technology and the concept of encoded legal contracts will lead many to look to governments and regulators for answers. Who is responsible if things go wrong? What will the central banks acknowledge? How can we safeguard global markets when computer automation plays *the central role?*

Notable Actors: Estonia, United Kingdom, United States, Germany, Australia, China, Russia

2.3.8.5 CONSORTIA

Numerous industry consortia are emerging in the blockchain space as industry competitors, which happen to be among the most highly regulated and least trusted companies in the world. They have a vested stake in creating shared standards, unifying processes and supply chains. Meanwhile, many banks fear competitive usurp and consortia provide relatively lightweight buy-in to "quick wins" in the form of POCs.

Today, most of the participants across the dozen or so different consortia worldwide are financial services companies. These groups are targeting a number of complicated questions that can really only be assessed with multiple counterparties at the table. How do we settle disputes that span multiple jurisdictions? How do we handle defaults, trade failures, and transaction reversibility? How can we secure, not to mention comply with, privacy requirements in a shared, transparent system? How must we collaboratively manage private key lifecycles?

Consortia are somewhat unique in this space because the integration of inherently shared operational *and* technological processes is largely unprecedented. For example, four members of the R3 Consortium recently announced they had developed a "utility settlement coin," which are digital coins designed to let financial institutions pay for securities without waiting for traditional money transfers to go through, and which would be able to be directly converted to cash at central banks.

Notable Actors: R3, Digital Asset Holdings (DAH), Hyperledger Project, numerous country-specific consortia (e.g., Russia, Switzerland, China, etc.)

2.3.8.6 ENTERPRISE TECHNOLOGY VENDORS

As in other markets, agile innovators like startups place pressure on the technology giants. In the blockchain space, IBM and Microsoft have dominated blockchain activity; both companies have service offerings integrated into their legacy offerings (Watson & IBM Cloud in IBM's case and Azure in Microsoft's case). Both companies have also invested significantly in open source development of the technology, contributing code to important communities like the Hyperledger project, Ethereum, and ConsenSys, and supporting countless startups. While these two currently lead the public projects the market has seen from large technology enterprises, it is important to note the conspicuous absence of many other formative players in the "tech giant" and database markets. Amazon and Google have

recently announced partnerships with Digital Currency Group (DCG) and fintech systems integrator GFT, respectively, to allow enterprise experimentation using their servers. But additional insight on such proofs has been minimal. Tractica has heard little from others in the space, such as SAP, Oracle, Teradata, Salesforce, etc.

Competition abounds. Another emerging trend among employers of large teams of engineers is providing "blockchain bootcamps" for their employees' development. Examples include Google, Capgemini, Accenture, Deloitte, and even Zappos.com.

2.3.8.7 MINERS

In the Bitcoin world, miners are the nodes (individuals' computers or groups of computers known as "mining pools") that use special software and sometimes hardware to calculate highly complex math problems as quickly as possible with proof of work, thereby creating a new block. In a distributed network, the competition for who can accurately and most rapidly solve the computation is incentivized by Bitcoins in exchange. The Bitcoin incentive serves the short-term goal of rapid computations, as well as the long-term impact of luring more people to mine, thus creating a stronger decentralized network.

This constituency is the foundation of integrity for public blockchains like Bitcoin and Ethereum. Yet, the role of miners is unclear for private blockchains. Some argue that the banks themselves would become miners, others think banks would (or would continue to) entrust other companies such as those who, today, host their payments infrastructures. Or this could become the role of the Society for Worldwide Interbank Financial Telecommunications (SWIFT)—a messaging network today used to securely transmit information and instructions enabling international payments. Even others suggest that auditors or even consumers could become miners for banks via P2P transactions. As financial institutions reckon with the standardization of [crypto] currency, the role of miners in private blockchains will likely take a clearer form.

2.3.8.8 INVESTORS

Investors from both small boutique firms and corporate venture teams worldwide are pouring money into the blockchain space. According to CB Insights and KPMG, Bitcoin and blockchain companies closed 74 deals, raising a total of $474 million in VC in 2015 alone. Silicon Valley sponsored roughly half of all blockchain investment worldwide, according to Coinbase. Including the rest of investors worldwide, more than 130 different companies invested in blockchain in 2015. The influence of investment, particularly by enterprises, will directly impact the development of this technology.

2.3.8.9 CONSUMERS

Generally speaking, blockchain will remain invisible to consumers for the foreseeable future. Barring the fact that we are, of course, all consumers, this technology will not be one driven directly by consumer demand. Emerging notions and blockchain-enabled use cases around identity and self-sovereignty have the potential to place much more power (in the form of data control and provisioning) directly into the hands of consumers. While this would never happen overnight, the sheer number of increasingly "connected" consumers has and will continue to shift economic and social structures and narratives.

SECTION 3
TECHNOLOGY ISSUES

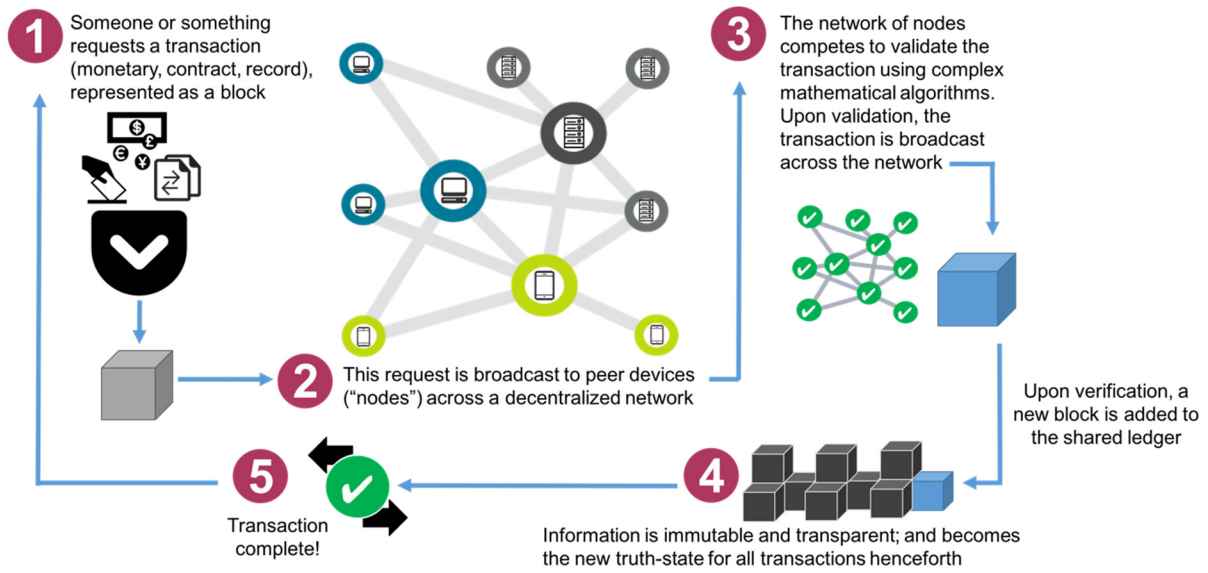
3.1 AN EXPLORATION OF BLOCKCHAIN ARCHITECTURE

To understand the potential and limitations within the blockchain space, one benefits from an exploration of the technological architecture.

First, why implement a blockchain, or a "chain of blocks?" A blockchain implementation has two kinds of records: transactions and blocks. Each block holds time-stamped batches of individual transactions. Blocks are files containing the indelible store of records, which, once transacted, cannot be altered or removed. Each time-stamped block must refer to the preceding block to be valid, and is then used to validate the next block in the blockchain, thus the immutability of the chain.

At any given time, the chain of blocks represents the "present truth" for all on the network. The figure below depicts the five essential steps for transaction validation on the blockchain.

Figure 3.1 How a Blockchain Works



(Source: Tractica)

Step 1: Someone or something requests a transaction. Once submitted, a transaction is represented as a block.

Step 2: This request is broadcast to peer devices (nodes) across a decentralized network.

Step 3: The network of nodes competes to validate the transaction using complex mathematical algorithms. All validating nodes (devices) in the network run agreed-upon consensus algorithms against all of the same transactions, thereby validating (or invalidating) each transaction.

Step 4: Upon verification, a new block is added to the shared ledger and the transaction is broadcast across the network. Information is immutable and transparent; and becomes the new truth-state for all transactions henceforth.

Step 5: Transaction is complete! All parties are updated.

It is worth noting that transactions themselves can take on different forms other than purely money. Currency-based transactions leveraging cryptocurrency are the mode for funding and executing monetary transactions, such as the Bitcoin blockchain. But transactions stored on a distributed ledger can also represent or involve events, objects, individuals, etc. These kinds of transactions are supported by "smart contracts." These are self-executing computing protocols or programs that enforce pre-defined rules and modify data accordingly.

While this framework offers the core characteristics of a blockchain transaction, the reality of this extremely nascent market is wild fragmentation in which, depending on the use case, organization, network structure, and size, one encounters many different blockchain configurations that use a variety of different mechanisms for consensus. There are three primary "types" or patterns of blockchains emerging today, each offering various pros and cons depending on the adopter's use case.

3.1.1 Public Blockchains

The original blockchain, the architecture underlying Bitcoin, is a public blockchain, also known as permissionless, trustless, or decentralized blockchains in which, via a consensus algorithm, anyone may contribute to the shared ledger. A public blockchain is distinct in its consensus architecture in that it involves miners. Transactions are validated and processed by a decentralized network of volunteers (miners), usually hosting dedicated hardware to perform high-speed and complex calculations, called "hashes." They do this in order to find solutions to a complex mathematical algorithm in return for a handsome reward (12.5 Bitcoins; roughly $8,125 per block mined). Public blockchains often use "proof-of-work," meaning miners must show proof of their computational work in how each block is hashed.

In public blockchains, digital currency (e.g., Bitcoin BTC) or tokens (e.g., Ethereum's ETH) is used to pay or execute smart contracts and process transactions. In order to prevent fraud or spam, these blockchains (and the integrity and security of the system) incentivize miners through expensive rewards in order to publish blocks.

Examples of public blockchains include Bitcoin, Ethereum, and NXT, among others.

3.1.2 Private Blockchains

By contrast, private (or "permissioned" or "sandbox") blockchains are those that consist only of known stakeholders. They are designed for agile application development and rapid deployment, more similar to typical software-as-a-service applications. Today, these sandboxes allow single enterprises to configure high throughput and control the nodes within the network without having regulatory frameworks in place to allow them to interact with public networks. Private blockchains are made up of known nodes, as there must be legal recourse among parties with low trust and competing agendas. Unsurprisingly, more corporations and organizations are looking at (and investing in) private blockchains than public blockchains in order to "safely" learn more about blockchains and pilot use cases. Private blockchains also do not require digital currency or tokens for transaction processing. Rather than requiring the prover to perform a certain amount of computational work (proof-of-work), private blockchains often use a proof-of-stake system, in which the prover must show ownership of a certain amount of money.

Examples of private blockchains today include, but are certainly not limited to Ripple, Blockstream, Clearmatics, Eris, MultiChain, and many others.

Consortia such as Digital Asset Holdings and R3 are developing software for blockchain, but it remains to be seen if these could be considered "true" private blockchain platforms.

An emerging alternative to DLTs takes private blockchains a step further. Distributed concurrence ledgers (DCLs) eliminate the "crowd" factor in creating consensus and transactions are processed only by the counterparties involved in the transaction. If the update across each counterparty is not equal, this signals that a problem needs addressing, and if not, the transaction fails and no contractual obligation ensues. The company behind DCLs, DisLedger, claims the significantly smaller "network" providing consensus in a DCL architecture eliminates redundancy, which in turn reduces power consumption, data storage needs, and costs, and increases processing speed.

3.1.3 Semi-Private or Hybrid Blockchains

Also known as "consortium" or "shared-permission" blockchains, only verified participant nodes are allowed to publish blocks. Because they are smaller and remain tightly permissioned with optimized consensus algorithms, semi-private blockchains facilitate much faster transaction speeds than public networks. Like private blockchains, semi-private blockchains also do not require digital currency or tokens to process transactions, although tokens can be useful for incentivizing adoption.

Ultimately, private blockchains can connect to both consortium blockchains and public blockchains, enabling what many interviewees envision long-term as a "blockchain of many blockchains" similar to the Internet of many *intra*nets.

Hyperledger (also known as the Hyperledger Project) is a collaborative effort founded by the Linux Foundation that offers elements of both private and public blockchains. The function of the project is to align independent efforts, develop open protocols and standards for a variety of blockchains, and modularize different consensus, storage, permissioning, contracts, and identity components designed for different use cases—some permissioned, others not.

Despite tremendous buzz and investment in the space, many of those closest to the technology admit that it is, in fact, a very simple advancement in technology. It has the ability to store states (e.g., transactions or events) in a transparent manner, despite its complex mathematical and computational composition.

"Blockchain can do deceptively little," observes Bart Suichies, CEO of amazingminds and former technology lead at Philips Blockchain Lab. "But what it does—an immutable log that acts as a single shared source of truth—is enormously valuable. It's a bit like asking what is the worth of the wheel? Technically, it just turns, it's not much value; but what you can do with it is priceless."

3.1.4 Blockchain as a Bundle or À la Carte

As the distributed ledger space continues to evolve, so do the nomenclature and configurations to support specific use cases. Tractica identified an emerging trend within the broader blockchain space in which singular functions or characteristics of DLT are "unbundling" to meet specific requirements, wherein some features fit the business case and others do not. Core "modules" of blockchain may be applied as singular functions and include, but are not limited to:

1. Transaction Distribution
2. Consensus
3. Rules of Validity & Linkage
4. Immutability
5. Identity Authentication & Private Keys
6. Supervisory/Regulatory Nodes
7. Anti-Double Spend
8. Built-in Assets

There are a variety of approaches within each of these that abstract characteristics of blockchain for different applications. In "consensus" approaches, for example, proof-of-work and proof-of-state enable very different modes of records verification; one is about proving computational work, and the other is about proving ownership or storing the existence of the record or activity associated with the record.

"Blockchain as a term has today become a bit like Kleenex," explains Jesse McWaters, Financial Innovation Lead for the World Economic Forum. "We must abstract away from blockchain as a singular concept to understand its utility in specific areas. We'll eventually wonder why we were so caught up with what 'blockchain' was, and understand that its unique attributes will be part of a wide swath of technology from which we pick and choose."

Industry consortium R3's recent release of Corda, a distributed ledger platform (not fully considered a blockchain) articulates its utility for financial services as one that solves specific problems with specific properties. R3's CTO, Richard G. Brown, rejects the notion that blockchain as a bundle is appropriate for all financial services use cases, instead asserting, "The right approach is to treat them as a menu from which to select and customize… different combinations, in different flavors, for different business problems." As the space matures and vertical-specific use cases take form, vendors will advance specific functions to differentiate themselves.

Bundled or à la carte, blockchain should not be viewed as a sort of panacea. And, like other architectural innovations, it will be most effective when leveraged alongside a host of other emerging (and existing) technology trends.

3.1.5 A Chip off the Old Blockchain

Blockchain applications are, by and large, a software implementation today and exist as cloud-based deployments. But with regard to matters of scale, one must ask if this technology could be a device-based or firmware-encoded deployment as well. Could we have blockchain on a chip?

The answer remains unclear, but the overtures may be pending. There are signs of very early activity to explore the notion. Some larger players on the hardware side are looking toward blockchains to manage existing relationships, such as those selling switching networking solutions into hardware thinking about how to leverage data centers when they already have hardware in the network, as well as optimizing latency for transactions.

Another way to assess this question is to look at Bitcoin's mining history. Within the last 5 years, the electronic circuitry underpinning Bitcoin mining has gone from central processing unit (CPU) to graphics processing unit (GPU) to graphics performance analyzer (GPA) down to the ASICs. Such ASICs in the market today are similar in size (approximately 14 nanometers) to the ASICs from the Intels or AMDs of the world.

Qualcomm's investment in 21 Inc., a startup that developed an embeddable Bitcoin mining chip, raised eyebrows and sparked speculation around whether Qualcomm would want to integrate Bitcoin payments into its suite of offerings. Speculations range from Bitcoin's wallet-enabled smartphone processing chips to enabling entirely decentralized and autonomous appliances.

Practically speaking, blockchain-enabled chips could bridge many use cases between connected devices and distributed ledger-based transactions. Fleets of vehicles, drones delivering goods, or municipal infrastructure communicating among each other seamlessly, interoperably, and in ways that can be audited would simply be more efficient and secure on a blockchain. Yet, what is necessary for this "autonomous world" is embedded trust that ensures those accessing the network are indeed who or what they say they are. "Hardware should have a way of asserting its identity," says Kartik Natarajan, Co-founder of Applied Blockchain, a strategic advisory firm. "Manufacturers must start building that into devices, whether at the chip level, firmware level, or otherwise."

3.2 THE LACK OF INTEROPERABILITY AND UNIVERSAL STANDARDS

Interoperability, or the ability for disparate nodes and networks to work with each other, is a requirement for a connected world and a mandate for new architectures to work alongside existing ones. Interoperability is not just about devices or systems cooperating, it is about enabling shared value and eliminating unnecessary friction and intermediation between interactions. In the blockchain market, where simplification is the primary value prop, easy integration is essential for adoption.

3.2.1 IN THE RACE TOWARD BLOCKCHAIN, CUSTOMIZATION SLOWS INTEROPERABILITY AND THWARTS SIMPLICITY

In the blockchain space, the imperative for interoperability is inherent to some degree. After all, the very nature of a distributed network means that *multiple participants must agree on common formats* and protocols. Adoption relies on the need for creating and/or updating shared standards across industry participants in order for successful migration to new DLTs. Such standards are also critical for integration with existing or incumbent transaction systems.

It is also very unlikely that chains will live in isolation. Consider the emerging use case around post-trades, which involve both transfer of *ownership* and transfer of *money.* An entity may want to use currency from one chain and purchase an asset on another chain. While there are a few ways to configure the transfer or information between chains, it is not hard to see why interoperability between private chains, side chains, and platforms is inevitable to ensuring its efficiency and adoption.

Second, interoperability can be a strategic security measure. If participants agree on protocol and other componentry specifications, the risk of errors arising decreases, given that the same error would have to appear across a majority of implementations to impact the chain.

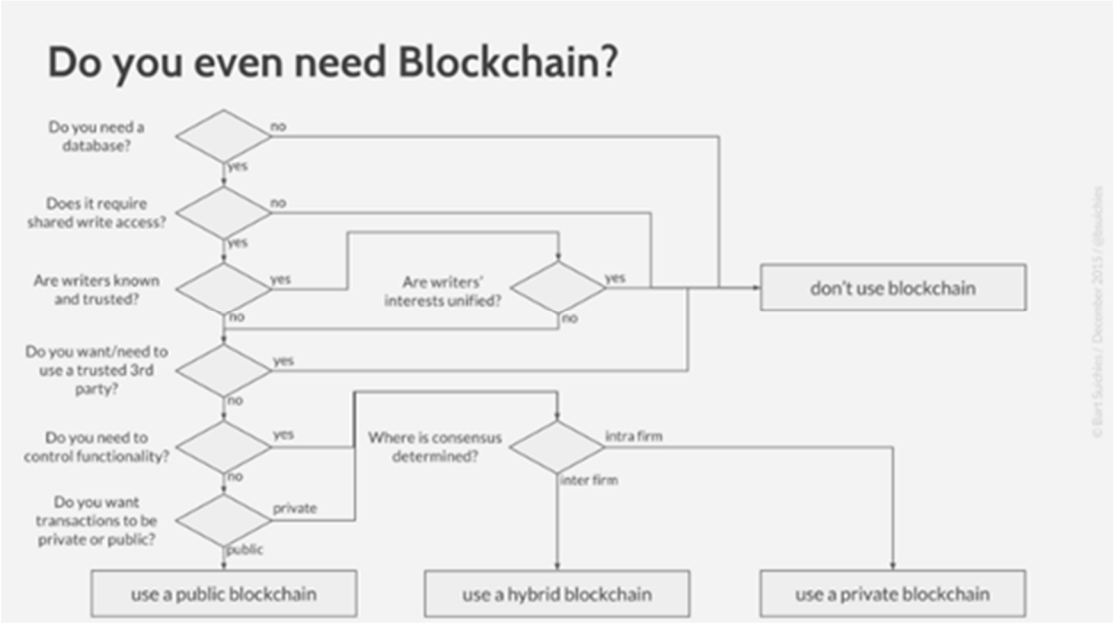
Consortia such as the Linux Foundation's Hyperledger Project are working on developing standards through entirely open source frameworks. "A primary objective for us," explains executive director of Hyperledger, Brian Behlendorf, "is how can we get individual developers working on a common roadmap at the architectural level." Hyperledger's Fabric protocol began as IBM's open blockchain research codebase, but the technology company has since transitioned it to the Linux Foundation's infrastructure.

3.2.2 INCUMBENT SYSTEMS: OVERHAUL OR INTEGRATION?

Most industries are far from entirely overhauling *all* of their incumbent systems and databases and putting them on a blockchain. The reality today is that blockchain technology for the enterprise, while full of promise and potential efficiency gains, is still extremely immature. Most POCs and pilots remain just that, and there are very few examples of any in-market, full-production implementations in any industry.

Aside from the fact that blockchains are not appropriate for all business use cases, industries have already sunk billions of dollars in investment into current (often "home-grown") systems. Perhaps of equal importance is that users (enterprise and consumers) most trust the systems to which they are accustomed.

Figure 3.2 Blockchain Appropriateness



(Source: Bart Suichies)

Blockchain applications must consider other enterprise systems to incorporate a wide range of adjacent business activities and systems, including but certainly not limited to other vertical business applications, business application management, analytics, dashboards, inventory, customer relationship management (CRM), counter-fraud management, compliance, etc., many of which rely on systems of record (SoRs) and relational databases.

Blockchain also still lacks universal standards and definitions. Juxtapose this against generally risk-averse and highly business-model focused institutional cultures, and it is unlikely that blockchains will replace entire capital market infrastructures in the near term. Most blockchain applications providers understand this and are building specific application programming interfaces (APIs) and other integration plug-ins to enable future hybrid systems as the market accelerates and proves more value. A blockchain integration becomes a systems design project, introducing a host or critical considerations around duplicative transaction processing, auditability, enterprise systems and SoR integration, transaction volumes and velocity, regulatory compliance, and design intention, strategy, and rollout.

3.3 SECURITY CONSIDERATIONS

Although the largest and most mature blockchain platforms (e.g., Bitcoin Blockchain and Ethereum) have yet to ever be hacked, there are diverse external vectors that place a range of threats on a wide range of actors (e.g., users and developers), devices, and networks all inherent to the system's integrity (or lack thereof).

Not all blockchains are created (or used) equally, and it is not impractical to ask if a larger attack surface translates to greater vulnerability. Could replicating files on a distributed ledger potentially offer hackers more places to penetrate? Blockchain is inherently distributed (i.e., identical and interconnected versions of it exist in different locations) and encrypted, so transactions are easy to see, but difficult to manipulate or change.

Scaling down the number of participants and connected nodes also has downsides: fewer participants (as on a private/centralized blockchain) means it is technically easier for one or a few "bad eggs" to possess more than 51% of the computing power, making network takeover more feasible. Therefore, private blockchains are not generally viewed as securely immutable (unchangeable), and have less perceived inherent trust and value than publicly distributed blockchains. This also renders the network *more vulnerable* early on in it its lifecycle as fewer nodes means less distributed/more centralized actors and a greater possibility of manipulation. This "chicken and egg" conundrum is a central component to POCs and why many of those experimenting with blockchain are doing so on a small scale, but with low-risk or even dummy data.

Another threat that surfaced during Tractica's research was that of miner collusion, in which those responsible for processing and broadcasting blocks (miners) could view enough identifiable information about a transaction to collude against a group of participants by withholding those transactions from inclusion on a block. For example, in an e-voting context, a group of miners could potentially refuse to accept any and all votes from a particular candidate or issue. In a monetary context, a group of miners could conceivably refuse all transactions coming from a specific individual's wallet; if the individual does not see it, miners could get away with it. This is a highly debated issue on public blockchains like the Bitcoin blockchain, but it is also relevant in the private and hybrid blockchain world. Such limited chains may be in a worse position as they can be hijacked by a smaller number of players and because they have fewer participants checking on miner behaviors.

In the case of miner collusion and other threats to the integrity of the chain, hackers and bad actors are at a great risk of exposure. Other participants can typically identify precisely where foul play began and, in the public blockchain world, the network places great emphasis on public exposure. If people lose faith in the system, it dies and there is no way to recoup the cost of investment. Thus, as one Bitcoin expert put it, "no one will kill the golden goose!" And so the Nash Equilibrium is maintained.

Even amid significant advances in security fortitude, cybersecurity will continue to be an extremely difficult and ongoing (if not intractable) challenge for businesses and governments. Ensuring blockchains that are deployed in production are secure and safeguarded is paramount to users actually trusting the system, and by extension, the viability of the technology. Meticulous controls must exist across the entire system, not just within the components of a distributed ledger system, but in all input and output data, across third parties, users, training, and governance procedures.

3.4 TECHNOLOGY SUPPORTING PRIVACY

From a technology perspective, blockchain enables new capabilities for protection. Many of the security benefits outlined in Section 2.2.4 underscore improvements in privacy. This section will focus on those most directly impactful to obscuring and protecting individuals' sensitive data.

Although not new or unique to blockchain, cryptography and digital signatures, which are an inherent part of blockchain architecture, offer an embedded layer of security compared to traditional database architectures. The most commonly discussed privacy protection in blockchain is private-public key cryptography. This is a cryptographic system that uses two key types and a digital signature:

- **Public Keys:** Can be disseminated across a group of permissioned users or nodes
- **Private Keys:** Known only to the individual user/controller
- **Digital Signatures:** Used to sign a message with the private key, but can be verified by all who possess public key

There are two ways to use this mechanism. First, parties can use a public key to authenticate the origin of the message with the paired private key. Second, parties can encrypt a message with a public key so that only the private key holder can decrypt it.

Private keys are made up of long and complex sequences of numbers and letters, so they are not easy to remember, thus people trust external parties (e.g., online wallet services and exchanges) with their private keys. Critics point to these third-party authority certification requirements (often used to develop public keys) as a weakness, in the event they are hacked. This will continue to place hacker targets on such external parties.

Another notable cryptographic technique for blockchain is **zero-knowledge proofs** (ZKPs). ZKPs allow two parties to prove that a proposition is true without revealing any information about the event, typically a transaction in the case of blockchain. With ZKPs, "there's no way to distinguish between encrypted/hashed files with various computational properties. For instance, there is no way to distinguish between that file being a sequence of transactions whose sum is $100, and a song, or a JPEG picture," explains Professor Eli Ben-Sasson of Technion, Israel Institute of Technology. ZKPs also underlie other cryptographic signature types, such as zk-SNARKs and zCash. ZKPs and blockchains complement one another insofar as ZKPs enable parties to be confident about certain properties of an event, but blockchain provides the consensus-based distributed ledger, which holds the "canonical source of truth."

State channels are another emerging solution developed for scale, but that benefit privacy as well. In a state channel environment, instead of using the blockchain as the primary processing layer for all transactions, the blockchain is used only as a settlement layer. Thus, it only processes the final transaction registered after a series of interactions, and executes complex computations only in the event of a dispute.

Another important concept for privacy on a blockchain is the concept of secure MPC, sometimes known as "homomorphic" encryption. This is an encryption mechanism that allows the sharing of data with third parties without it ever being decrypted. It allows untrusted computers to run computations on highly sensitive data as though it were in its original form, but without exposing the data to hacking or surveillance. It could allow the "chaining together" of different services, so that different companies could calculate different attributes of a transaction (e.g., exchange rate, tax, shipping, etc.) without seeing the full unencrypted data.

"Homomorphic encryption is a bit like being able to see the shadow of something but not the object itself. In this case, the object is data." explains Nell Watson, renowned technologist and associate faculty at Singularity University. "It doesn't risk compromising the identity of that individual."

MIT's Enigma Project is a blockchain-based homomorphic encryption "decentralized computation platform with guaranteed privacy." It uses MPC to encrypt data by splitting it into pieces and randomly distributing indecipherable chunks across hundreds of nodes (other computers) in the Enigma P2P network. This Bitcoin blockchain-like approach means each node performs calculations on its specific discrete chunk of information. No single machine ever has access to data in its entirety; rather, nodes can only compute authorized functions on the data, before being recombined.

Businesses could store proprietary data on the blockchain and use permission systems to allow employees (or even software programs) to analyze records without risking the leakage of any individual data points. This could also reduce risks associated with outsourcing data processes.

In the project's white paper, its creators foresee a transformation in how individuals manage, even monetize their own data. "With guaranteed privacy, autonomous control and increased security, consumers will sell access to their data. For example, a pharmaceutical company looking for patients for clinical trials can scan genomic databases for candidates. The marketplace would eliminate tremendous amounts of friction, lower costs for customer acquisition and offer a new income stream for consumers."

Blockchains will use a variety of cryptographic techniques and digital signatures to prove identity and authenticity, and enforce read/write access rights. So far, no single technique has emerged as the industry standard for privacy protection, although the above holds promise.

3.5 BUT CAN BLOCKCHAIN REALLY SCALE?

The question of scalability is a prism of many sides: data storage, network bandwidth, processing power, energy consumption, participants, and even context. The question of scalability in this space remains hotly debated, with those arguing physical limitations and environmental impacts on one end and others arguing that next-generation blockchains will have far lower computational requirements than today. Can blockchain really handle the intense scale of "all" data and transactions in a given environment? While this is certainly the narrative within the blockchain space, it bears scrutiny.

3.5.1 TRANSACTION VOLUME AND STORAGE

Transaction volumes already range in the billions per day ($4.5 billion in the financial sector alone). Visa, for instance, claims its payment system can process 56,000 transactions per second if needed, although it averages about 2,000 transactions per second. Billions more transactions are happening each day in healthcare, in media, and increasingly in industrial and energy sector applications. Claims of displacing and recording current systems with blockchain have to account for both transaction data and other data (e.g., files, payments, customer data; structured, unstructured, etc.). Creating an immutable record of all of these data may be technically feasible, but is it tenable?

From a bandwidth and timing perspective, we are certainly tightening the latency. In the last 3 years, blockchain transaction times (i.e., the roundtrip time for blockchain-based transaction confirmation) have decreased from around 20 minutes on the Bitcoin blockchain,

to around 7 seconds on Ethereum. But there are still limitations. The current transaction delay issue is rooted in the fact that blocks are limited to 1 megabyte in size, which holds about seven transactions per second. (Compare this to Visa and we have a long way to go.) While Ethereum is a significant improvement, it has far less testing than the Bitcoin blockchain to justify support of trillions of real-world transactions.

From a cost perspective, it is not yet clear whether indirect savings (see Section 2.2.5) outweigh increased costs as the blockchain grows. As chains grow, so do the very large transfers of data constantly taking place across networks, and large investments in significant computational power to carry out verification. Although there is an inverse relationship between cost and network processing power, the overall cost of running, growing, and sustaining a blockchain system may grow to be quite large over time, due to the large storage space required for each copy of the blockchain and greater energy consumption and uptime costs.

Then there is the question of storage. For transactions, microtransactions, and IoT applications, the amount of data generated is astronomic and growing rapidly; replicating this data across multiple, tens, hundreds, or thousands of nodes on a distributed network is not a sustainable solution for businesses or for the planet. This leads to a conclusion that enterprises will place some, but not all data on a shared network. But which data? And who decides? While some of this logic could be written into the logic of the solution, the relative value of data may change over time depending on who is assigning value, and according to which strategy. For many enterprises, the culture around data storage today is “collect it all now and figure out how to use it later,” particularly as companies are trying to pivot to sustainable “data-driven business models.” Global spending on cloud storage was an estimated $22.6 billion in 2015 according to IDC.

Other unforeseen models could shape the narrative of this story as well. Current cloud storage services are centralized, but emerging blockchain-based decentralized storage players, such as Storj and Sia, are building end-to-end encrypted distributed storage platforms, allowing users to “rent out” their unused disk space.

3.5.2 Energy Consumption

To assess scale in the context of energy consumption, first remember the original Bitcoin blockchain proof-of-work concept of mining (introduced in Section 3.1.1.1). The massive network of miners ensures the consensus and security of the system, but so much replication of computing power also consumes a tremendous amount of electricity. One analyst found that a single Bitcoin transaction requires as much electricity as the daily consumption of 1.6 American households, and that number is growing as the Bitcoin blockchain network grows.

The recent U.K. government’s report, *Distributed Ledger Technology: Beyond Blockchain*, estimates that the energy requirements to run the Bitcoin blockchain, one of the only public and in-production blockchains today, are more than 1 GW and may be comparable to the electricity usage of the entire country of Ireland.

Limitations of scale on blockchain emerge when the *full* ledger is distributed across *all* participants and when *all nodes must have access to all transactions* at *the same time.* If velocity of the transactions is too much for blocks to handle (because the blocks are too small), transaction recording overflows the block size. In the current state of permissionless blockchain architecture, this network effect is hyperbolic, and simply requires too much computing, storage, and network to justify. Ultimately, Moore’s Law and more efficient silicon development could help reduce power consumption in future blockchain architectures, but this question remains unclear.

3.5.3 Scalability of Private Blockchains

For enterprise adoption, blockchains simply must meet volume and speed requirements, while still providing greater efficiencies than current environments. This demand is another driver toward private blockchains, wherein proof-of-stake systems could replace mining. While the proof-of-work method used in public cryptocurrency contexts like the Bitcoin blockchain asks users to repeatedly run hashing algorithms or other client puzzles to validate electronic transactions, a proof-of-stake system requires only that the prover show ownership ("stake") of a certain amount of money—a *far* less resource-intensive process. Other characteristics of private blockchains help drive scale and efficiency:

1. Limited participants involved via permissioned networks
2. Paring the size of the ledger in certain circumstances
3. Incorporating business analytics into transaction verification
4. Partial centralization of ledgers

This also comes down to a question of when blockchain is the proper solution. In some cases, a centralized database may just make more sense. Businesses must account for scale limitations and opportunities when weighing the risks and benefits of blockchain deployment.

Using blockchain to scale in one area could reduce power consumption inefficiencies elsewhere. While we are far from this reality today, one can envision massive, shared, and permissioned blockchains upon blockchains, which could, in aggregate, make redundant thousands of existing disparate and proprietary systems today. Although blockchain computing architectures are highly complex and require significant computing power, they offer the potential for greater scale through liquidity across a wider network.

3.6 Decentralized Autonomous Organizations, The DAO, and Current Implications

DAOs are blockchain-based decision-making structures without centralized control. A group of people write programs via smart contracts to enable governance in the system; ventures invested in the DAO would back contractors elected by the group to carry out proposals. Buy-in via tokens representing voting rights allows each person to participate in proposals for how the DAO spends money and votes on proposals submitted by others.

3.6.1 The Rise and Fall of The DAO

The first DAO was the Bitcoin Blockchain network, governed by consensus across thousands of nodes, but "*The* DAO" refers to a specific DAO developed by Slock.it, a German startup developing a blockchain-based smart locking platform. The company considered the creation of The DAO "a gift to the community" and entirely separate from its own monetization model. The DAO was built on the Ethereum blockchain. The project broke the record for the largest crowdfunding campaign in history, raising over $150 million across 11,000 contributors in just a month; greater support gathered far faster and wider than its creators originally anticipated.

During the initial crowdsale, several participants expressed concerns of vulnerability in The DAO's code. Lawyers warned The DAO had overstepped its crowdfunding mandate and securities law adherence in multiple countries, and participating token holders may not understand the full scope of risk and responsibility. As the Slock.it team worked to resolve a non-cash-threatening "recursive call bug" that emerged just a few days into the launch of The DAO (before it began to execute on the 50+ proposals ready and waiting for voting), the system was attacked.

The unknown attacker began draining ether from The DAO collected from the sale of its tokens into a "child DAO," to the tune of 3.6 million ether. Numerous contributors tried to split The DAO to prevent the drain from continuing, but the requirement for consensus was not reached in time. Given that the "child DAO" has the same structure as its parent, funds were not able to be accessed for a 28-day initial funding period. The price of ether dropped from over $20 to under $13 in just 6 days.

The fate of The DAO was in question. The Ethereum Foundation, Ethereum (for which The DAO made up 15% of all ether), and the numerous startups working on DAOs and smart contracts, all watched with varying levels of participation how the powers that be in this grand decentralized experiment would respond (via consensus voting).

Blockchain architecture demands that at least 51% of the nodes on the network must "re-write the truth" (i.e., agree to a sort of collusion) in order for the system to be diverted from the truth created by transacting blocks on a distributed ledger. This sort of collusion is part of the inherent challenge of breaching security on the blockchain and underscores the trustworthiness of the system; indeed, a 51% attack had never occurred since the advent of the Bitcoin or Ethereum blockchain.

After much debate, the Ethereum community decided to hard-fork The DAO on the Ethereum blockchain with an absolute withdrawal feature, designed to effectively restore all ether to their original contract. The hard-fork intervention violated the philosophy of decentralization for a part of the Ethereum community, and these "purists" have chosen to maintain the original "unforked" blockchain, currently known as Ethereum Classic, with its own distinct cryptocurrency.

In many ways, the story of The DAO was short-lived, but continues to unfold. By most accounts, The DAO in its original form is dead; but the vision remains, albeit bruised, but with greater account for risk next time.

3.6.2 Implications from a Cautionary Tale

While the first DAO may only live on as a cautionary tale, decentralized autonomous organizations are a revolutionary concept. Their design is purposed to loosen the reigns of state powers and allow for new dynamic forms of organization and economic structure. Rolling out such a structure will not happen overnight, and perhaps not for years to come, but as blockchain continues to grow, this concept is unlikely to fade.

The fall of The DAO also illustrates risks of early (and perhaps too rapid) blockchain deployment in which lots of money, people, and decisions are invested. First, any system with many nodes is subject to diverse attack vectors and programming faults. The DAO constituted entirely new territory in terms of regulatory and corporate law. How would regulatory bodies treat contracts executed on The DAO? Who had financial liability and over what precisely?

Poorly formulated smart contracts and a general lack of governance structures created vulnerability in the system, so that a particularly clever Ethereum-fluent hacker was able to redirect millions of dollars' worth of digital currency away from the network's decision-making and into his or her own structure. Smart contracts, pre-defined and questioned governance structures, and other vulnerabilities must be addressed before rolling out this technology to "prime time."

SECTION 4
ENTERPRISE USE CASES FOR BLOCKCHAIN

4.1 ENTERPRISE APPLICATIONS AND USE CASES FOR BLOCKCHAIN

Although financial services have sponsored the majority of investment in blockchain, the applicability of DLT touches a wide range of industries and use cases. While these are very early days in the blockchain market, elements of blockchain architecture (functions articulated in Section 2.2.1) have strong potential to disrupt many existing structures and business models. Tractica's research finds use cases for blockchain fall under the areas depicted below.

Figure 4.1 Enterprise Use Cases for Blockchain (Parent Categories)

(Source: Tractica)

By and large, adoption of blockchain will be slow for the coming 2 to 5 years. As with most technological innovations, different industries will adopt pieces of this technology at varying paces. But unlike other recent technological advancements, the network effect compounds blockchain's potency, utility, and efficiency; the more institutions that adopt blockchain simultaneously, the faster its impact.

Tractica's analysis of more than 30 use cases surfaced a set of criteria that signal applicability of blockchain technologies. Industries leading blockchain adoption will be those for whom the following characterize the current state.

Criteria for Blockchain Adoption and Prioritization:

- **Multiple Actors:** Multiple parties must log information to complete a transaction
- **Shared Repository:** Multiple parties must access a single "truth source" to conduct business
- **Governance:** Multiple intermediaries currently handle logging and/or reconciliation
- **Transactional Dependencies:** Parties must depend on other parties to conduct business
- **Trust:** Trust is minimal or lacking across parties
- **Technological Dependencies:** A single source of "truth" streamlines other business efficiencies

- **Regulatory Requirements:** Compliance requirements are high, difficult to manage, and costly to ensure

Industries most likely to lead adoption will be those for whom these characteristics are most costly today.

4.2 PAYMENTS, TRANSACTION PROCESSING, AND SETTLEMENT

4.2.1 PAYMENTS

Primary Industries:

- Banking
- Retail
- Online Retail
- Online Services
- Online Gaming

The Case for Blockchain-Enabled Payment:

Using blockchain to enable secure payment between parties was the original use case of this technology. Emerging after the crash of 2008, Bitcoin addressed fear, uncertainty, distrust, and doubt in the financial landscape. As Wall Street executive turned cryptocurrency expert, Jason Liebowitz put it, Bitcoin was designed to offer a solution to the question, “Where can someone store value if the financial system fails?" The answer: The Internet.”

The Bitcoin blockchain is heralded by most blockchain practitioners as the technology's largest and longest running success story to date. In the current model, if a customer is holding Bitcoins in their wallet and wants to sell them, it usually takes days for the transaction to process to their bank account. Bitcoin holders must go through an exchange platform that accepts digital currency, set up an account, transfer Bitcoins, and wait for the exchange to send a payment to your bank. Today, there are two leading companies, Coinbase and Circle, that facilitate Bitcoin purchases with fiat currency and serve as withdrawal mechanisms to convert Bitcoin back to fiat. This enables numerous online companies—retailers, services, media platforms, etc.—to accept Bitcoin and some other altcoins. What began with a P2P Bitcoin exchange is now nudging its way into large banking institutions.

As for large financial institutions, this is an area where a majority of parties must collectively embrace, regulate, and build for it to become useful and replace current modes of interaction. As governments have shifted from gold to fiat to more easily distribute wealth within society, digital currency presents a similar solution.

Until cryptocurrencies are regarded as federally backed currency, adoption will be slow. Skepticism due to nefarious associations with Bitcoin and cryptocurrencies create uncertainty in the short term, but the functionality and security of the platform over the last 7 years since its inception is irrefutable. Regulatory uncertainty and the need for updated monetary policy will keep adoption phased. Pressure from consumers and irresistible cost savings achieved through speed/efficiency, security, AML, and transparency/trust will likely justify eventual adoption by financial institutions.

Figure 4.2 Partial List of Companies that Accept Bitcoins as Payments

List of Companies Who Accepts Bitcoins as Payment!

Many companies are accepting bitcoins, many are not. Here is a list of the biggest (and smaller) names **who accepts bitcoins** as a currency.

- **WordPress.com** – An online company that allows user to create free blogs
- **Overstock.com** – A company that sells big ticket items at lower prices due to overstocking
- **Subway** – Eat fresh
- **Microsoft** – Users can buy content with Bitcoin on Xbox and Windows store
- **Reddit** – You can buy premium features there with bitcoins
- **Virgin Galactic** – Richard Branson company that includes Virgin Mobile and Virgin Airline
- **OkCupid** – Online dating site
- **Tigerdirect** – Major electronic online retailer
- **Namecheap** – Domain name registrar
- **CheapAir.com** – Travel booking site for airline tickets, car rentals, hotels
- **Expedia.com** – Online travel booking agency
- **Gyft** – Buy giftcards using Bitcoin
- **Newegg.com** – Online electronics retailer now uses bitpay to accept bitcoin as payment
- **1-800-FLOWERS.COM** – United States based online floral and gift retailer and distributor
- **Fiverr.com** – Get almost anything done for $5
- **Dell** – American privately owned multinational computer technology company
- **Wikipedia** – The Free Encyclopedia with 4 570 000+ article
- **Steam** – Desktop gaming platform

(Source: 99bitcoins.com)

Examples:

Scores of online companies and websites accept Bitcoin payment (see Figure 4.2 above). These include large corporations, such as Overstock.com, Subway, Rakuten, K-Mart, Sears, Dell, Tesla, T-Mobile (Poland), Tiger Direct, and many others.

In June of 2016, a digital bank called WB21 became the first financial institution to accept Bitcoin, in effect, a complete disintermediation of the current Bitcoin exchange process. It supports Bitcoin exchanges across any of the 18 world currencies it currently offers. This also allows WB21 customers to deposit money from any of the 180 countries in which they support accounts, in real time, thereby avoiding wire transfers.

Meanwhile, Barclays bank announced a partnership with Bitcoin "bank/exchange" Circle in which the company will use Barclay's Corporate Banking to store sterling for its customers, as well as the infrastructure to allow transfers from any U.K. bank account back and forth with Circle. The U.K. Financial Conduct Authority issued Circle an e-Money license to expand the efforts.

"As the first digital currency company in the world to be granted an e-money license, Circle will also offer the benefits of digital money to Europe's 500 million consumers, and ultimately enable anyone with sterling or euros to send and receive value for free and with an experience familiar to anyone who uses messaging or social media," according to Circle co-founders Sean Neville and Jeremy Allaire.

4.2.2 PEER-TO-PEER CROWDFUNDING AND LENDING

Relevant Industries:

- Entrepreneurship
- Arts & Entertainment
- Venture Capital
- Personal Finance

The Case for Peer-to-Peer Crowdfunding and Lending:

Crowdfunding is the transaction mechanism that allows a project, venture, or other cause to raise monetary contributions from numerous individuals. In the last 5 years, the crowdfunding market has grown significantly, raising over $34 billion in funding in 2015 alone, and financing thousands and thousands of activities, from startups to artistic projects, medical treatments, funeral costs, and beyond.

Crowdfunding benefits from increased trust, as well as the inherent speed and precision made possible by blockchain-enabled payment itself. In most models, crowdfunding is either reward-based (e.g., receive a CD for helping a musician fund her new album); equity-based (e.g., gain equity into the cause); software value token-based (e.g., receive digital tokens to use for other purposes such as gaming); or donation-based (e.g., donate to a charity to assist a charitable cause). Debt-based crowdfunding, also known as P2P lending is another form in which individuals participate in a marketplace of directly matched lenders and borrowers in which investors buy securities in a fund that backs loans between borrowers. They make money off of high-risk loan interest rates, but such risks are not backed by the government.

Crowdfunding taps into the wisdom and sentiment of the crowd in that it provides a very real and tangible way to observe the appetite, volume of interest, and support for any given idea. In the short term, crowdfunding will enjoy greater scale through blockchain; in the longer term, blockchain could enable microtransactions allowing users to crowdfund projects using their devices, revenue generated from their devices, or other assets.

This space is poised for continued growth. Blockchain architecture is not only a technological extension of the notion of P2P, but addresses the current challenges the crowdfunding space faces today, chiefly trust, security, identity/copyright authentication, compliance, and fulfilment.

Examples:

There are countless crowdfunding platforms on the market today, IndieGo-Go and Kickstarter are the largest, but a few are currently running blockchain platforms. IndieSquare is one example of a startup that has created a Bitcoin wallet app so that users can “tip” content creators for their work.

Crypto Coins Enterprises DK (CCEDK) is a Danish startup doubling down on blockchain, both running on blockchain and serving as a crowdfunding platform for blockchain initiatives. What began as a Bitcoin exchange is shifting to the world of crowdfunding by uniting global investors and ordinary people interested in investing in blockchain technology with innovators and startups working on DLT applications. CCEDK acts as the escrow in the transactions, allowing investors to trade their investments using OpenLedger, a company that provides administrative and legal services for investors. The company aims to be the preferred marketing and crowdfunding partner for blockchain startups.

4.2.3 International Currency Transfer

Relevant Industries:

- Banking
- Capital Markets
- Remittance

The Case for Blockchain-Enabled International Currency Transfer:

Blockchain technology can help streamline international payments, between both individuals and corporations by eliminating the need for brokers to verify the transaction. Building authentication, payment, and automated currency exchange algorithms directly into a distributed shared ledger addresses the three main issues with international payment today.

First, transferring money across borders is opaque; it is difficult to understand exactly what is happening where, with whom, and how fees collected are broken down for each transaction, and precisely what things like "corresponding banking fees" are anyway. Reporting is streamlined through the use of smart contracts, which also have the impact of reduced operational errors. DLT enables direct transactions between sender and beneficiary banks, effectively circumventing altogether the role of correspondent banks.

Second, it is slow. Historically, the processing time for cross-border payments, involving numerous banks and brokers, has been between 3 days and 2 weeks, depending on scope. Real-time settlement of international money transfers would reduce liquidity and operational costs, which have the potential to increase profitability.

Third, it is costly. For consumers, typical transaction fees are between 10% and 20% of the transaction sum; businesses must go through brokers, which take a 2% to 5% fee. A number of blockchain activities are underway in the international payment space today. A company called Abra reduces the transaction fees down to .03% per transaction. Abra users are also not required to have a bank account to use the service.

Applying DLT across international payments, as well as in other financial use cases, such as post-trade clearing and settlement, also helps eliminate fraud within the system.

Examples:

Singapore is an example of a country working on eliminating invoice fraud among banks by granting each invoice a unique cryptographic hash that banks share, so that if another bank registers a duplicate invoice (without the unique key), the entire system is alerted.

The British arm of Spanish bank Santander (U.K.) is piloting among staff a blockchain-enabled international payment application. It incorporates Apple iOS's Touch ID technology for users to biometrically secure transfers between £10 and £10,000. Payments can be made from British pounds to Euros (sendable to 21 countries) and U.S. dollar payments to the United States only.

Numerous other blockchain-enabled remittance startups are emerging worldwide, including China's BitSpark, Africa's BitPesa, and Mexico's Volabit, among others.

4.2.4 TRADE FINANCE

Relevant Industries:

- Capital Markets
- Financial Services
- Logistics
- Shipping
- Commodities Trading

The Case for Trade Finance on the Blockchain:

Use cases for DLT are particularly well suited for numerous applications within financial services given their requisite processes, complexities, regulations, number of counterparties, and current opportunities for abuse. This report will address some, but not all of the financial processes to which blockchain could be applied. Below is a discussion of the broader umbrella of trade finance as it includes numerous categorical use cases ripe for DLT. These are areas under development in many of the current POCs and pilots are underway by financial institutions.

Trade finance includes an extensive set of processes required to execute on a transaction between two or more parties. Depending on the specific type of transaction, these include, but are not limited to: customer bank validation along multiple phases of transaction setup and execution (in compliance with KYC regulations); issuing letters of credit; review of multiple documents sourced from different locations; investigation of actors' legal structures' screen for anti-terrorism and sanctions violations including AML and others; scoring and classification of risk; archiving of reviewed documents; etc. Trade finance remains a prudent way for any company to do business internationally and ensures that cross-border business is protected against late payments, delayed delivery, geopolitical instability, currency fluctuations, and expected or unexpected risk factors.

Trade finance services generally require thorough, intensive, multi-stakeholder, long, and costly processes, making them prone to error. According to Goldman Sachs, it is estimated that about 10% of trades are subject to error today. This leads to a tremendous amount of manual oversight and intervention. Using blockchain to store financial details could significantly improve efficiencies in document approval, creating new financing structures, and risk reduction. Enabling direct interactions between import and export banks reduces friction by disintermediating correspondent banks. Further, the fact that blockchain can automate rules-based settlement through smart contracts programmed into the system signals significant opportunity for improving resolution time, cost, and labor efficiencies, and shortening the settlement window. DLT could improve real-time visibility for regulatory oversight and automated compliance as well. Efforts across numerous financial institutions are targeting blockchain application in supporting at least one or more opportunities within this use case.

In order for DLT to gain wider adoption in this area, however, many regulatory and legal frameworks will require re-writing. Furthermore, incumbent technology systems are not disappearing and interoperability between DLTs and legacy platforms (as well as between multiple DLTs) is essential. The wide range of counterparties must also buy into these frameworks and new processes required for blockchain deployment—no small feat considering the range, variety of jurisdiction, long incumbent legacy, and volume of assets at stake.

Examples:

Scores of large financial institutions worldwide are investing in blockchain talent, initiatives, and consortia to target these use cases. Some include Bank of America, Wells Fargo, Credit Suisse, and Banco Santander, as well as financial groups from large manufacturers like Toyota and Mitsubishi.

One such financial institution, which wished to remain anonymous in this write-up, is working to pilot this process in the area of documentary trade, specifically in how letters of credit are communicated between counterparties with complete visibility into the real-time status of transaction, creating an immutable and auditable database for all transactions between four parties, each serving as a node. This financial institution's pilot eliminated the need for SWIFT entirely.

"We are a leader in this instrument within the trade finance industry and so we feel we have a great responsibility to look into the opportunity around this because there is a lot of room for optimization," explains the project lead, who preferred anonymity. "Today, the process of documentary credit uses disparate systems for applying, issuing, advising, creating presentations, checking data, and payment. It's like we're still issuing checks while the rest of the world has moved on to wire transfer and mobile payment. But the need for documentary trade—buyers not wanting to pay suppliers before they have their goods and suppliers not wanting to release goods until they have their payments—isn't going away. Documentary trade is an old industry that still relies on paper, industry expertise, and lots of fine print to make sure counterparties are doing what they need to do. There is incredible opportunity to make errors in the current method; if one item is misspelled, if a supplier ships a day late... The more we can get everyone creating data at source and sharing over one system, the more efficient the system can be. Blockchain creates a distributed system in which, using individual API layers would enable us to pull data from many systems, corporates, carriers, banks, etc. and interact with that information in a far more practical and secure way."

On the commodities trading side, current paperwork to process oil sales and shipments is still very archaic. The Brent Crude derivative, for instance, consists of just four physical crude oils worldwide: Brent, Forties, Ekofisk, and Oseberg (BFOE). Swiss-based commodity trader, Mercuria, expects this entire market to adopt blockchain-enabled payment by the end of 2017, and in the process, achieve cost savings of some 30%.

4.2.5 Syndicated Loans

Relevant Industries:

- Capital Markets
- Financial Services
- Trade

The Case for Blockchain-Enabled Syndicated Loans:

Leveraged or syndicated loans are one type loan in the trade process eligible for DLT application. These are a specific type of loan extended to companies or individuals who already carry significant debt; lenders consider these loans high-risk and charge higher interest rates to the buyer as a result. Leveraged loans have the longest settlement period (T+21 days) of any other asset class.

The lending process for a syndicated loan is complicated and involves many counterparties: banks must undergo buy-sell matching, which often reduces market liquidity as intermediaries protect their balance sheets from risky loan defaults. When a secondary sale is made, the borrower's consent must be obtained by the buyer. Institutions must then comply with heightened regulatory requirements involving AML, KYC, and Foreign Account Tax Compliance Act (FATCA), which can add 3 to 8 days to the process by requiring the running of background checks on clients. The trade must then be allocated into select sub-funds, then over the course of 3 days, reviewed, queried, and signed by both buyer and seller for confirmation. After 3 to 5 days, buyer and seller agree to the Settlement Date Coordination (SDC) in order for the trade to close. Agents then review this, which typically takes another 3 days, the trade closes, and the trade is recorded in the registry.

This process is rife with inefficiencies, many of which cause disagreements over the economic details of the trade and extend the timeline. Buy-sell matching introduces new parties to the risk equation, each with their own systems, risks, and needs for reconciliation. Required compliance with AML, KYC, and FATCA regulations, for which extensive headcount and duplicative efforts of this process only add to the inefficiencies and settlement time. Buy-side allocations are not always available and are entered manually. Furthermore, there is currently no electronic settlement platform (ESP) connecting brokers for leveraged loans, meaning brokers have no real-time system feeding into their internal systems. Underwriting risk through distributed documentation, transactions, and access could substantially reduce the number of resources required across all of these activities.

Blockchain offers this process a secure, permissioned, private transaction ledger database for all parties to share, update, and easily access with the latest details of the process. This could easily serve as an ESP for all parties. Smart contracts can address many of the disagreements over details because parameters could be encoded into transactions and executed only if they are met. A private blockchain shared between banks could effectively pre-authenticate clients to streamline AML and KYC compliance. Later in the process, it could help streamline FATCA compliance and other legal requirements, which account for the 5-day average amount of time it takes for agent approval. Blockchain is also opportune for streamlining numerous processes in post-trade reconciliation wherein transaction information and asset title transfer are duplicated and distributed across all counterparties.

Examples:

Blockchain technology consortium R3 just announced that it, along with Credit Suisse and a host of other agent banks, service providers, fund managers, and technology companies, has just finished “the first phase” of a syndicated loan POC. The participants who collaborated and provided testing resources to the project include R3 consortium members BBVA, Danske Bank, Royal Bank of Scotland, Scotiabank, Société Générale, State Street, U.S. Bank, Wells Fargo, AB, Symbiont, Synaps Loans, Ipreo, Oak Hill Advisors, Alliance Bernstein, and the list goes on.

4.2.6 POST-TRADE CLEARING AND SETTLEMENT

Relevant Industries:

- Capital Markets
- Financial Services
- Trade

The Case for Post-Trade Clearing and Settlement on Blockchain:

The total cost to the finance industry of clearing and settling trades is estimated at $65 billion to $80 billion a year, according to a report last year by Oliver Wyman. Yet, despite this volume, the industry is rife with inefficiencies and antiquated ways of transaction. Post-trade processing includes extensive and multi-party coordination to execute, making it slow, costly, and inefficient today. This can include, but is not limited to: clearing and settlement (buyer-seller deal detail comparison); custody and asset servicing; collateralization; change records of ownership; arranging for transfer of securities or cash; and transaction approval. Sometimes, these transactions require international courier services. At numerous points in this process, costly challenges emerge, such as multiple versions of a single trade recorded across multiple systems; constant amendments and changes to account information requiring updated settlement instructions; and multi-day processing time (T+3 days), which ties up capital in liquidity in the process. Throughout the lifecycle of an equity trade, numerous stakeholders and intermediaries play a role (in addition to buyer and seller), including: Central Counterparties (CCPs) Clearing Houses, the Depository Trust & Clearing Corporation (DTCC), Central Securities Depositories (CSDs), banks (including custodians), and brokers.

Banks are now exploring how they can exploit the technology to speed up back-office settlement systems and free billions in capital tied up in current methods of processing trades on global markets. Blockchain helps automate each (potentially all) of these reconciliation phases more efficiently. First, its distributed, secure, and shared ledger could reduce trade errors and the need for manual intervention (intervention that takes place today across many of the aforementioned stakeholders), as well as enable real-time compliance. In fact, blockchain's architectural requirement for authentication and verification across the network would inherently reduce the need for manual intervention addressing the constantly changing nature of account information and settlement instructions because they would be automatically encoded and contracted accordingly. Secondly, a reduction in manual intervention and trade errors translates to more efficiency in back-office functions and fewer headcounts needed to reconcile internally and across other counterparties. Third, many anticipate blockchain's automation of transaction and account information processing would shorten the overall time needed for settlements, freeing up some liquidity and potentially the volume that capital brokers would be willing to commit to yet unsettled trades. Given the extensive improvements blockchain can offer to the post-trade settlement process (e.g., streamlining reconciliation errors, decreasing or eliminating brokerage fees, shortening settlement windows, and even reducing back-office administration and compliance costs), it is seen as one of the highest value use cases of blockchain technology.

Despite significant activity and investment in post-trade-related use cases for DLT, widespread value creation in this market will require widespread (near universal) adoption across all capital market participants. The proliferation of consortia, DLT protocols, and blockchain applications and services must either consolidate or develop universal standards for interoperability with each other. Standardization is also required at the architecture level—a central focus of all consortia—to agree upon frameworks for everything from asset

classes to account information structures, trading records, permissioning, etc. Elements of post-trade reconciliation span the gamut of identity security and will require iron-clad architectural support of anonymity for capital market participants, privacy protections of sensitive financial data, and KYC-required information, along with the transition of trillions of dollars in transactions to a new technology system. Needless to say, the operational risks may hinder the rollout of DLT for some time to come.

Examples:

In September of 2016, Barclays announced one of the first successful live trade finance transactions on a blockchain in which actual documentation tied to actual physical merchandise with real counterparties was transacted paperless, across borders and time zones in hours instead of days. The documentation of some $100,000 worth of dairy products took place on Wave's (a Barclay accelerator graduate) dedicated blockchain between agricultural co-op Ornua and Seychelles Trading Company, a food product distributor.

Since 2014, Deutsche Bank has been centering its current blockchain research and testing around post-trade processing in areas like payments and settlement of fiat currencies, asset registries, enforcement and clearing derivative contracts, regulatory reporting, KYC, and AML registries. “We are focusing deeply on securities and corporate bonds because they [are] representatively complex as a number of other items in our portfolio and involved a lifecycle," explains Edward Budd, Managing Director and Chief Digital Officer of Global Transaction Banking of Deutsche Bank. “The big finding for us has been in just how much efficiencies can be gained reengineering processes that are broken today by digitizing the entire lifecycle of a bond, particularly when they start digitally.”

Meanwhile, in addition to Deutsche Bank, another three of the world’s biggest banks (UBS, Santander, and BNY Mellon, alongside ICAP, a broker) have teamed up to develop a new form of digital cash they are calling a “utility settlement coin” that they believe will become an industry standard to clear and settle financial trades over blockchain. The companies are currently in the process of pitching the ideas to central banks and anticipate a commercial launch sometime in the next 2 years.

There are several rival digital cash systems being developed around settlement. Setl, a London-based group founded by hedge fund investors and trading executives last year, also aims to settle financial market payments with digital cash linked directly to central banks. Citigroup is working on its own Citicoin solution, while Goldman Sachs has filed a patent for a “SETLcoin” to allow trades to be settled near-instantaneously. JPMorgan is also working on a similar project. The utility settlement coin, based on a solution developed by Clearmatics Technologies, aims to let financial institutions pay for securities, such as bonds and equities, without waiting for traditional money transfers to be completed. Instead, they would use digital coins that are directly convertible into cash at central banks, cutting the time and cost of post-trade settlement and clearing.

NASDAQ has become another early mover in this space in its partnership with Chain, a blockchain infrastructure provider, to facilitate issuance and transfer of shares of privately held companies.

4.2.7 PROPERTY TITLE OWNERSHIP TRANSFER

Relevant Industries:

- Real Estate (Residential and Commercial)
- Automotive
- Luxury and High-Value Goods
- Legal
- Government

The Case for Property Title Ownership Transfer on the Blockchain:

The process of transferring ownership from buyer to seller of an asset, particularly of estates like a home, land, or other property, is one that requires numerous middlemen, phases, and reconciliations to execute. Property records and the "chain of title," which includes deeds, mortgages, leases, easements, court orders, and encumbrances, are usually stored in title plants at the county level, which must be maintained and require significant labor resources (thus, higher fees) to search and curate in order to verify a transaction. On top of this, most records remain paper-based; approximately 30% of property titles are found defective at the time of a real estate transaction, according to The American Land Title Association.

Very few buyers buy large estates outright and require loans to finance mortgages. The process for obtaining a loan is time consuming, expensive, and involves banks, lawyers, and real estate agent coordination. Even once a loan is obtained, buyers must typically go through escrow services and title companies for third-party verification that the buyer can indeed pay the mortgage and all parties can avoid fraud. Such third-party verification carries considerable costs (typically between 1% and 3% of the total value of the property) and adds extra time to the process.

The very process of ownership transfer has its own set of stallers for which blockchain-enabled identity mechanisms (tied to buyer, seller, or even home) could provide instant "truth" of credit history (for buyers) and proof of ownership (of sellers). Homes could even have information attached to them to streamline the transaction, including but not limited to history of development, repairs, refurbishments, ownership chain, and associated costs. Blockchain could help centralize property records, while also validating them by distributed consensus, thereby reducing risk of human error and processing and reconciliation time. This could enable significant cost savings because cost of title insurance premiums reflect underwriting and distribution expenses more than actuarial costs.

Internationally, the opportunity has other applications as well. In some countries, property transfer fees are exorbitantly high, limiting market participation. Blockchain could also help reign in real estate corruption and property rights abuse.

Despite these potential savings and efficiencies, this market will not adopt blockchain technology overnight. Real estate is a highly fragmented industry across geographies, regulatory environments, and pricing structures; widespread buy-in occurs from mortgage lenders (also a fragmented industry); and long-term infrastructural investment takes place across all parties.

Examples:

Sweden's national land survey is testing a blockchain-powered system for registering and recording land titles in order to reduce risk of errors and digitize real estate processes securely and with transparency for all parties involved in the transactions, including banks, government, brokers, buyers, and sellers.

In both Ghana and the Republic of Georgia, initiatives are underway to place land registries on blockchain to eliminate tampering and to signal against perceptions of corruption. In Ghana, this initiative is underway across 28 communities. Property title transfer using blockchain applications in developing countries that lack formal land registries may indeed outpace adoption in highly developed countries with long-standing institutionalized land registries and regulations.

4.2.8 Property & Casualty Insurance Claims Processing

Relevant Industries:

- Insurance (Individual and Commercial)
- Healthcare
- Automotive
- Construction
- Energy

The Case for Property and Casualty Insurance Claims Processing on the Blockchain

Insurance companies are investigating the use of blockchain to support property and casualty (P&C) claims for both individuals and companies. The current claims process requires extensive manual documentation, submission, and review resources to verify a claim. Entering these events on a distributed ledger could streamline both claims processing and subsequent payouts and service contracts associated with financing and executing repairs. It is likely that certain sub-use cases in this industry will gain traction faster than others. Connected devices or in-home devices, for example, could have insurance policies encoded into smart contracts so that when sensors detect damage, claim and repair processes, as well as payouts, are automatically triggered and executed. Incidents such as car accidents or health-related issues, often more dangerous or sensitive in nature, will continue to require human discernment.

Automating insurance policies once they are written into smart contracts is a compelling notion, although it remains to be seen just how automated each phase (event claim, review, payout) can really be, and whether the benefits outweigh the barriers, without compromising associated counterparties. Scalability, security, and low standardization across the industry remain significant hurdles for adoption at both corporate and consumer levels. Furthermore, insurance coverage is based on numerous factors (read: data sets), including but not limited to physical assets, location, health history, claim history, education, other risk factors, and beyond. Another fundamental hurdle is incorporating each of these respective streams and their associated counterparties onto a shared ledger for the purposes of insurance.

Examples:

InsurETH is a startup focused on the flight insurance market and offers P2P flight insurance policies. Through smart contracts, payouts will be initiated when cancelations or delays are

reported from verified flight data sources, so that customers are assured that payouts arrive as quickly as possible.

4.2.9 MICROINSURANCE

Relevant Industries:

- Insurance (Individual)
- Agriculture
- Collaborative Economy

The Case for Blockchain-Enabled Microinsurance:

Insurance companies are also looking at blockchain technology to support secure, efficient, but short-term insurance coverage applicable in two primary contexts. The first is in support of current microinsurance use cases protecting low-income individuals' health or property, and the second is in the context of the shared economy.

In the first context, insurance is provided to low-income folks to protect themselves through typical risk-pooling schemas. In the second context, if a person wants to share or lend an asset to another person, such as a car, a house, a luxury item, etc., it follows that both parties may want to insure that transaction. Through hashing, timestamping, and digital signatures, digital assets that represent real-world properties, such as physical objects, documents, or source code, can be issued and transferred; transaction processes recorded, notarized, and reported; and any modifications to the property recorded on an immutable ledger.

The critical challenges associated with placing microinsurance on the blockchain are similar to those outlined in the above section on P&C insurance claims processing.

Examples:

Consuelo (the Spanish word for "consolation") is a mobile payments platform provided by Saldo.mx, a Mexican company providing blockchain-enabled cross-border mobile payments and microinsurance to migrant workers. The product eliminates the intermediary claim adjuster.

Another project called LenderBot is the pilot concept developed by blockchain application company, Stratumn in partnership with Deloitte and Lemonway. The project allows users to use social media (Facebook's messenger app), blockchain-enabled signatures, and cryptographic timestamps to enter into a loan contract insuring high-value items like cameras, mobile phones, and other devices. The bot executes on smart contracts between the three parties (Facebook, Lemonway, and the user), notarization is finalized, and Lemonway enables payment within the Bitcoin blockchain.

4.3 MICROTRANSACTIONS

4.3.1 REWARDS AND LOYALTY-BASED MICROTRANSACTIONS

Relevant Industries:

- Advertising
- Food, Beverage & Hospitality
- Retail

- Retail Banking
- Travel

The Case for Blockchain-Enabled Loyalty Programs:

Rewards programs are a common tool for driving customer engagement, retention, and additional revenue across a variety of sectors, including financial services, big-box retailers, specialty stores, airlines, hotels, drug stores, grocery, mass merchants, gaming, restaurants, car rental providers, cruises, fuel/convenience stores, and others. There are two primary kinds of loyalty programs: proprietary (single provider) programs and partnership programs where customers can achieve rewards from and are applicable to multiple providers. The problem, however, even in partnership programs, is that most bonus points go unused. As businesses are awakening to the opportunity to leverage data for highly contextual marketing, the need arises for a shared database to manage high volumes of transactions and enable permissioned access and program execution in real time.

The ability to provide integration across and protection to existing customer loyalty programs and rewards is another prospect for blockchain application. Although brands are beginning to offer single loyalty programs that aggregate and reward interactions across multiple product or service experiences, the reality is that, today, these programs are expensive to run due to so many disparate systems and databases across contributors. This hinders cost-effective deployments, provides botched user experiences, and offers little that enables brands to shift loyalty offerings or tactics easily.

This is an area with relatively lower risk of blockchain deployment compared to use cases involving capital markets, healthcare, or government. Another accelerator of adoption in the loyalty space compared to blockchain use cases in other sectors is that this space enjoys relatively fewer regulatory overheads in compliance than others. Finally, a future in which enabling easier and more accessible rewards is connected with individuals' increased control of their own digital identities (see Section 4.1.4.1) could change how consumers are incentivized to engage with specific brands.

Examples:

One company specializing in blockchain for the loyalty space, loyyal, leverages blockchain technology to align vendors for rapid piloting of loyalty programs across numerous stakeholders or "multi-branded coalitions."

China Unionpay (CU), the third-largest payment network by value of transactions processed, behind Visa and MasterCard, recently announced a blockchain POC project in collaboration with IBM to develop for a loyalty bonus points exchange for its 200+ members across 150 countries.

4.3.2 Digital Media Microtransactions and Rights Management

Relevant Industries:

- Music
- Art
- Digital Content
- Application Development

The Case for Digital Media Microtransactions and Rights Management Using Blockchain:

The music industry has faced significant disruption as the Internet and digital media culture has placed intense cost pressures on artists, and enabled new business models for corporations. One use case made possible through widespread blockchain adoption is the disintermediation of the numerous middlemen industries (e.g., music platforms like Apple and Spotify; music labels; copyright licensing bodies; advertisers; etc.) that currently collect the lion's share of revenue generated from music. Royalty payments depend on airplay statistics gathered and maintained by these intermediaries.

Blockchain-related efforts in this space aim for the disintermediation of the many intermediaries that collect revenue from the creative output of artists and place revenue back into their hands. Early experimentations in this use case illustrate possibilities for artist-consumer collaboration, advocacy alignment, and rights transfer. While most movement in this use case has taken place in support of musicians, many of the same challenges, disruptions, and opportunities exist for other content creators, such as artists, content marketers, graphic designers, videographers, and application developers. This is among the more crowd-driven use cases for blockchain and, given current powers and business structures in the music industry, it is hard to imagine record labels and other brokers for music access and copyright would want to adopt blockchain if it risked compromising margins.

Examples:

One of the most notable examples of this use case can be seen in the brainchild of singer/songwriter Imogen Heap. Heap partnered with Ethereum, as well as ConsenSys' Ujo project to release her new song on the blockchain and customize rules for how they wanted the tracks to be consumed. The other compelling element to Heap's POC is that she enabled users to download certain instrument tracks within the song, pay for just those tracks, and license them for their own musical endeavors.

Australian-based Bittunes provides a blockchain platform that allows both musicians and fans to be paid (in Bitcoin) for P2P sharing of their music, effectively monetizing the exchange of data.

Ascribe.io is another startup working on blockchain run registry of intellectual property (IP), certificates of authenticity, ownership, and artwork properties enabling artists to upload and watermark their artistic IP and share work only with those assigned.

4.3.3 Digital Advertising Management

Relevant Industries:

- Advertising
- Media & Content Creation

The Case for Blockchain-Enabled Digital Advertising:

Although the advertising industry has a firm grip on the current business model for the Internet, in many ways, it is still deeply challenged in achieving its fundamental goals. The first challenge is collecting and managing trillions of customer engagements (digital and physical) to feed them into analytics engines that derive the most value from that information.

The second challenge is to leverage such real-time information into a massive "omniscient" graph of customer (attributable) consumption habits, both verifying identity and protecting proprietary data.

Brands must go through numerous intermediaries today (media packagers, telecoms, payment service companies), so the decentralized nature of a blockchain could help streamline the critical need for permissioning on the part of all counterparties, and perhaps most importantly, the consumers themselves. Combining blockchain technology with multi-key encryption would enable a user-controlled identity graph that could massively shift power in the ad and marketing world, from centralized media and marketing companies to end consumers. Individuals could also conceivably choose to sponsor sites, advertisers, and/or content producers through microtransactions. Such transactions can take place through companies on the blockchain or directly between consumers and artists.

While this scenario may be further out than others, interim blockchain-enabled advancement in advertising also includes the ability to streamline payments settlement across multiple counterparties, as well as help verify ad-delivery, which are two significant challenges the industry faces today.

Examples:

BitTeaser is an online advertising network allowing any size webmaster to make money off of ads. The company runs an advertising platform similar to Google's AdSense, but runs on the Bitcoin blockchain, without the minimum $100 payout (which prevents smaller sites from benefiting), and with which revenue can buy tokens. It supports both cost-per-impression (CPM) and cost-per-click (CPC) models and allows webmasters to earn money through affiliate commission rates of up to 10%, by submitting articles and donation options to finance third-party campaigns. It delivers what it calls "teaser" (banner) ads, and can display all click-thrus in real time, accessible to all users at any time.

Another company called Brave provides an ad-blocking browser that is working on enabling Bitcoin payments users can send directly to the content providers they wish to support.

4.3.4 Online Gaming

Relevant Industries:

- Gaming
- Gambling
- Lottery

The Case for Online Gaming Using Blockchain

The gaming industry is looking to blockchain to help automate payment and transaction processing. Beyond just using bitcoin for gaming, public blockchains can provide a data-rich shared public ledger that can empower gamers to take in-game asset ownership and trade to another level. Gaming comes in many flavors (gambling, online games, sports games, etc.), but generally relies on trust that when rules of the game are upheld, merit-based rewards will follow. Additionally, gamers often buy or win digital assets, but trading, sharing, or cashing out on assets is complicated and difficult to authorize. Blockchain gaming offers potentially unrivaled transparency over the full gaming lifecycle: from the supply chain, customer acquisition (payment to affiliates), and service delivery, and mitigates (or potentially eliminates) counterparty risk with a gambling house or in P2P wagering. "On-

chain games" are a concept in which all game logic, including "truly random" chance number generation, as well as asset issuing, are run on a blockchain and are independent from any external institution.

Examples:

BitShares PLAY, a startup created on the decentralized autonomous company (DAC) called DACx, and operated by ZAFED, a Chinese financial services company, is one emerging player aiming to disrupt online gaming through on-chain probability games, quiz games, and chess games, as well as games that involve both strategy and probability like Bingo. Another unique component to this platform is what they call "multi-person vote-based SPG," or the idea that instead of single player versus single player games, single group versus single group games can be played in which individuals within the group bet on how the round should be played. The subsequent move is determined by the group and the weight of each ID's vote depends on the balance in the account and play reputation. PLAY's multi-person vote-based SPG concept sets a precedent and structure for prediction markets. Instead of betting on the next move on a chess board, users can vote on real-world events, whether or not or how something will happen.

Another company called FreeMyVunk (Vunk = Virtual Junk) is addressing the issue of in-game digital asset trading, sharing, and processing using a distributed ledger in which all goods are registered and processed as crypto-tokens.

Another example to watch is Kibo, the first ever blockchain-run online lottery. This is a blockchain and Ethereum smart contract-based lottery aiming to bring full transparency to ticket purchasing, drawing, selection, and payout, as rules are "hard-coded" into the code and thus immutable. It is also accessible from anywhere in the world and does not require banking infrastructure, only an Internet connection to participate. At the time of this report's publication, Kibo is in its initial coin offering (ICO) phase and has not yet ended. The goal for of the ICO is to sell 100 million KIBIT tokens (KBT) to the public. KBT represents a stake of the platform and is similar to shares of a company. After the platform's full launch, 4% of its turnover will be distributed to KBT holders. The amount holders receive is determined by the amount of tokens each holder has purchased.

4.3.5 Decentralized Energy Transmission and Distribution

Relevant Industries:

- Energy & Utilities
- Oil & Gas

The Case for Decentralized Energy Transmission and Distribution Using Blockchain:

Every event in an energy transaction has information attached to it. Today, the vast majority of energy provision is owned and operated by large utility companies that send electrons over very long distances to residential and commercial properties. Blockchain technology presents a number of opportunities for making more efficient energy transfer. One likely adopter in the short term will be those counterparties involved in wholesale energy trading and corporate energy procurement, such as industrial plants, large data centers, and corporate retailers. While still significant, the scope and regulatory structures in place in the wholesale energy trading space are comparatively fewer (to overcome) than utility transmissions and distributions for commercial and residential properties.

What today are sometimes called virtual power plants (VPPs)—a software-defined mechanism for aggregating all kinds of distributed energy resources (residential, commercial, and industrial) to enable more reliable power plants—could be a conceptual foreshadowing for blockchain. The primary objective of a VPP is to achieve a proper and sustainable balance of the electricity grid, while simultaneously achieving the greatest possible profits for asset-owning or energy-generating participants. Blockchain thrives in contexts of such operational and financial harmony.

Utility providers could leverage blockchain to decrease costs associated with long-distance transmission and leverage the technology to measure energy outputs very accurately and in ways that cannot be manipulated. Other shifts in costs that result from decentralized energy transfer include reducing the need for additional power plant generation and all of the expensive utility infrastructure (poles, wires, substations, and related equipment) for transferring energy across long distances. Meanwhile, as emerging forms of power generation (e.g., solar panels, microgrids, and energy storage installations) gain traction and enable local power generation, blockchain does not just offer new opportunities for energy suppliers, but for end users as well.

Prosumer/heavy power generating customers, businesses, and even passive consumers could all contribute to a decentralized energy grid that mediates transactions and allocation among all. The impact of distributed P2P energy metering and transfer has significant impact on traditional energy plant business models. First, it enables the opportunity for power consumers and P2P energy transfer, incentivizing people to take a proactive role in their energy consumption and generation. A homeowner with their own energy source may sell surplus electricity back into the grid. Energy transfer may be delivered in cryptocoins, which could mitigate risks around changes in government subsidies for renewable energy and/or if energy retailers wish to pay people less for what they produce, which has made net energy metering problematic in certain regions.

Another impact of such a system could be the creation of entirely new business models. Metering of energy information may involve sensors and thus other contextual information, such as temperature, pressure, etc., which could enable energy providers to package and sell data to previously irrelevant ecosystem constituencies.

Electricity, as well as other energy markets, such as wind, oil & gas, etc., may also see impacts in energy/commodities trading and/or the IoT. Blockchain's impact on commodities trading, through accelerated sales, shipments, and transactions is addressed in Sections 4.1.1.4 and 4.1.1.5. Reference Section 4.1.3.1 for an expanded look at how blockchain could streamline the IoT, sensor data transactions, and shared record-keeping.

The primary challenges facing this use case today are high regulatory barriers and the generally slow-moving pace of energy markets in the developed world. Most of the technological building blocks for such a system exist today.

Examples:

Companies like SolarCoin are getting users to buy into solar energy for rewards in SolarCoins. They are also beginning to look at ways of monetizing this data, effectively leveraging sensor data stored on blockchain technology to enable new business models through more reliable, and transparent data gathering and secure data to develop additional related applications on top of the platform.

German energy provider innogy (formally RWE) is piloting a decentralized P2P energy trading platform using blockchain. The project, which has been in the works for some 2 years,

began by using real historical data to simulate a borrowing tree in which energy was generated and then shared to others based on need. The company recently partnered with blockchain application provider ConsenSys and is now building a local energy marketplace with real buyers and sellers. In an evolution from the customer-to-customer (C2C) models, the marketplace works by matching the excess energy production of prosumers with larger consumers (e.g., supermarkets, libraries, small businesses) in nearby regions. Profile matching helps drive efficiency by complementing usage patterns throughout the day.

"Our first minimum viable product (MVP) represents a distillation of understanding a customer need and developing a commercial product that makes sense for buyers and sellers, while utilizing blockchain to enable the transactional layer," explains Sam Warburton, blockchain venture developer and innovation lead for innogy. innogy is conducting testing and proofing on all transactions with the goal of delivering real energy across the platform by the end of 2017.

4.4 ASSET MANAGEMENT

4.4.1 THE INTERNET OF THINGS, MACHINE-TO-MACHINE COMMUNICATIONS, AND DEVICE INTERACTIONS

Relevant Industries:

- Industrial
- Manufacturing
- Industrial
- Smart Cities
- Building Automation (Residential & Commercial)
- Aerospace
- Automotive
- Logistics
- Robotics
- Telecommunications

The Case for Blockchain and the IoT:

M2M communications have been powering industrial and automation applications for decades, but thanks to the emergence of cloud and mobile technologies (and reduced costs and barriers to entry), the M2M space has seen a new wave of adoption and investment, what many now refer to as the IoT trend. This is a pervasive trend in which embedded sensors that connect to the cloud systems and the Internet are manufactured into everything from heavy machinery and equipment, to stoplights, cars, HVAC systems, livestock, in-home appliances, and beyond.

Unsurprisingly, parties interested in the IoT and blockchain run the gamut, with the most activity occurring in financial services, industrial manufacturers, utilities companies, and legacy technology giants like IBM.

- **Manufacturing:** Discrete, process, machinery, equipment
- **Industrial:** Utilities, energy, smart cities infrastructure
- **Building Automation:** Lighting, HVAC, energy, etc.
- **Aerospace:** Airplanes, spacecraft, drones
- **Automotive:** Cars, trucks, public transportation
- **Smart Home:** Electronics, appliances, energy
- **Healthcare**: Surgical equipment, wearables, medical data
- **Logistics:** Supply chain, distribution, packaging, scanning
- **Robotics:** Robots (commercial and residential)

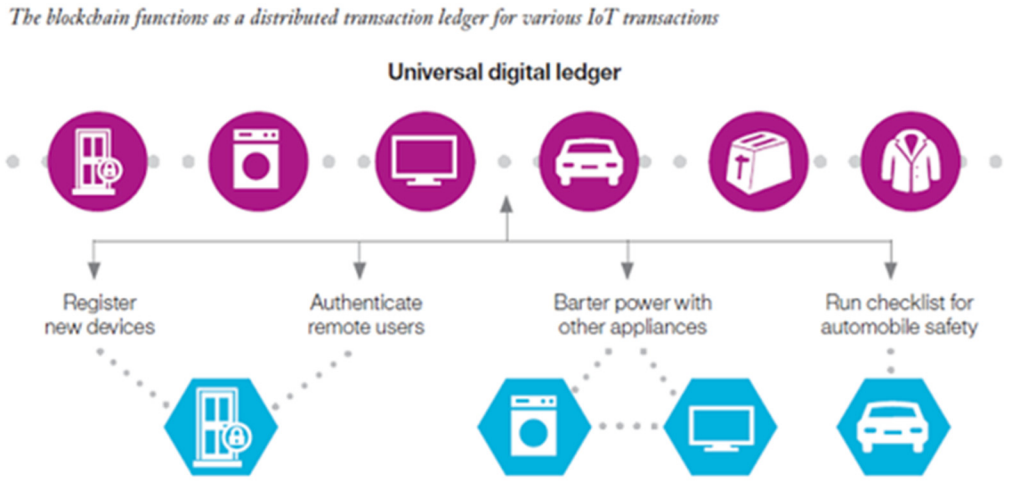
The IoT currently suffers from a variety of trust issues (security, privacy, surveillance, reliability, ubiquitous advertising, subscription fees, ownership versus access) that all blur its value and threaten the prospect for wider adoption. This space also faces issues of economic and engineering challenges associated with scale, as current IoT solutions are expensive due to high infrastructure and maintenance costs associated with centralized clouds, adequate server support, and networking equipment. Furthermore, diversity of ownership (i.e., controlling devices and cloud infrastructure) limits sharing and interoperability. Today, there is no single platform that connects all devices.

A future of "millions or billions" of devices communicating with each other efficiently requires that their interactions and transactions exist on an immutable database of shared, secure, and highly permissioned access. Blockchain may serve as a key enabler for the IoT because it has the potential to facilitate commerce between connected devices in scalable architectures and ensure repeatable outcomes/expectations. This is required to 1) establish value and 2) define trust between stakeholders and machines.

Consider the following examples of connected device interactions that could be enabled through blockchain:

- A connected washing machine registers itself to a shared ledger containing all historical information about its sourcing, manufacturing, distribution, etc. If the machine has an issue, or its user needs assistance, the machine itself could authenticate other users (e.g., a service agent) to update features, ensure security, run an automated safety or cleaning checklist, etc. Sensors inside a washing machine autonomously negotiate with peer devices to optimize energy use and schedule cycles during hours of lower electricity demand; the machine communicates with its manufacturers (or others) and downloads new washing and security features as they are developed; and it negotiates with suppliers to re-order detergent when running low.
- Parts and equipment within a car, building, manufacturing, or any production facility could autonomously sense their need for repair, contact nearby suppliers, and negotiate pricing and appointments for service and repairs.
- Energy allocation in a smart city is distributed across millions of devices (e.g., solar panels, industrial plants, charging stations, traffic lights, smart meters, autonomous cars, etc.), enabling efficient real-time interactions, such as traffic routing, energy harvesting, and local energy distribution.

Figure 4.3 Blockchain Offers the IoT a Universal Digital Ledger



(Source: IBM)

A decentralized approach to IoT networking and M2M interaction would not only provide a standardized communication model to process (perhaps trillions of) microtransactions between devices, but could also significantly reduce costs associated with scale (e.g., installation, integration, maintenance of large centralized data centers, etc.) It could also distribute computational and storage needs across devices in the network, instead of relying on central servers. From a security standpoint, this mitigates the risk of network failure because the integrity of the system is no longer reliant on penetrating single nodes.

Using a decentralized IoT network for more scalable, cost-effective asset management, automation, and interoperability is an attractive prospect for the millions of companies worldwide investing in connected devices and infrastructure. Still, myriad challenges remain: when can blockchain be adequately proofed to handle enormous volumes of transactions; for public blockchains, massive amounts of processing power and energy consumption are currently required for encryption and verification computations; not to mention the question of (redundant) storage required for distributed ledger verification. These questions also apply at the device level, where computational power is far more limited today.

Other challenges lie in interoperability (or a lack thereof) at the device level. The IoT space is extremely fragmented today, with a lack of universal standards required to justify placing networks upon networks of devices on a blockchain in the first place. Furthermore, device autonomy presents unchartered questions: who is responsible and liable for device malfunction; how is revenue generated allocated; who “owns” the data: manufacturers; retailers; network providers; consumers; insurance providers; or other service providers?

All of this does not take into account the inherent friction between an entirely “open” device interaction ecosystem, such as the one hypothesized in the above example, and the push toward service-based business models that manufacturers are developing today. Put simply, if devices themselves can shop around for optimal pricing, services, energy, etc., the strategy of securing customers by way of locking them into subscription models quickly grows obsolescent.

Of course, the greatest challenge facing the union of blockchain and the IoT remains security, including protecting not only data, contracts, files, devices, and networks, but maintaining privacy, authenticating identity, preventing theft/spoofing, developing governance for autonomous device coordination and settlement, and of course, designing regulations and compliance into transaction execution.

Examples:

IBM and Samsung's ADEPT project brought to life a distributed ledger facilitating various types of IoT transactions between devices, including: device registration, authentication of remote users, device-to-device power bartering with other appliances, automatically triggering safety procedures, etc.

Filament is a notable startup focusing on the IoT by developing connected modules that run on a blockchain to allow industrial assets to act as autonomous agents “at the edge.” Called “taps,” these sensors execute smart contracts themselves, as opposed to smart contracts running in the cloud, and they communicate via low-power, long-range, decentralized mesh networks without requiring a central network authority. Blockchain is used to authenticate devices and charge for network services using Bitcoin.

4.4.2 Supply Chain Management

Relevant Industries:

- Manufacturing
- Agriculture
- Logistics
- Shipping
- Distribution
- Retail
- Luxury
- Recycling & Waste Management

The Case for Blockchain and Supply Chain Management:

A supply chain consists of all entities and processes involved in getting an item from raw materials to final product for use. Supply chain processes today are opaque, generally not well understood beyond a few degrees of separation, yet made up of ever-growing and evolving networks of products, people, and counterparties. As monitoring and control technologies advance and increase, so too do consumers’ demands for transparency and integrity regarding manufacturing processes. In current supply chain systems, we have few ways of truly ascertaining monetary costs at each phase, not to mention critical issues, such as how much child labor, slave labor, political coercion, violence, or even environmental harm goes into product production. Even with ethical standards introduced, as seen from the United Nations and the United States, limited visibility into the chain renders standards difficult to implement and monitor. The fragmentation of supply chain information only proliferates waste, ignorance, lack of recourse, and apathy.

Blockchain's impact along the supply chain for assets and products is potentially multifold. Storing information that is generated and collected along the lifecycle of a product on a

blockchain introduces: 1) context into and 2) efficiencies across each phase. Consider use cases for blockchain across the following areas of supply chain:

1. **Product Inception:** The sourcing of seeds for agriculture; health and history of the soil or other raw material; the sourcing of parts or compounds for manufacturing, for instance, can be authenticated and transacted via immutable ledger providing "truth" verification (detailing their sourcing) across later phases of the supply chain.

2. **Product Development:** The growing of the crops; the development of equipment, machinery, or other products, each of which have installation requirements, certificates of compliance, and date of production data associated with them can be added to a blockchain to prove authenticity, quality, safety, compliance, and other criteria for product integrity. If an item or piece of an item is 3D printed, verification of its material may also be required.

3. **Product Distribution:** As products move from supplier to wholesalers, they have numerous interactions with individuals, companies, and environments. Tracking any product, but particularly agricultural, medical, or other environmentally sensitive products through the distribution process (with sensors) helps preserve their integrity, compliance, safety, and viability later in the supply chain. Using a distributed ledger to store and act on locational, temperature, pressure, and interaction data serves many functions, such as logging information, preventing tampering, and automating processes and services using that data.

4. **Product Trade Financing:** Product trade relies on cross-border transaction processing involving letters of credit, factoring, and other time and labor-intensive approaches to financing. These use cases are outlined in the Trade Finance section above, but could be incorporated into broader supply chain ledgers to accelerate shipments, increase liquidity and transparency, and even the economic playing field between developed and developing countries.
5. **Product Retail and Use:** The very experience of researching, shopping for, and purchasing an asset can be impacted by blockchain as its application in earlier phases of the product's lifecycle can streamline authentication, validation, compliance, and trust at the time of its consumption or use. A retailer can be sure it is selling products sourced from where suppliers say it is sourced; airlines can be assured parts are compliant and in good working order; pharmaceutical, high-value, or luxury items could have product authenticity "baked in" to their digital identities to streamline value transfer, reduce fraud, and prevent risk.

6. **Product Recycling/After-Market:** As product lifecycles grow inevitably more circular, visibility into the life of the product on a shared, trusted ledger could help streamline recycling, demolition, or resale.

It is also worth noting that blockchain in the supply chain context is a good example of where elements of blockchain componentry may be cherry-picked depending on the industry and specific use case. Security, identity, and permissioning impact anti-counterfeit measures in the supply chain; smart contracts, oracles, and custom code support security and compliance adherence; decentralization allows multiple parties to be involved in any supply chain to participate in shared (permissioned) record-keeping and reference data; and payments and contracts transfer to expedite reconciliation of the deal and the transfer of money and assets from one party to another.

The primary challenge facing this use case is the sheer number of parties that would need to adopt decentralized ledger technology to enable visibility into the broader supply chain. The broader the network adoption, the greater the value and efficiency, the inverse of which is also true. Another significant challenge lies in the vast and geographically varied regulatory compliance mandates that would first require assessment for application on DLT, and encoding and testing inside of the architecture itself before use in production.

Examples:

Hailed as one of the strongest in-production examples of a distributed ledger platform, Everledger uploads source and item specifications for the diamond industry, creating permanent records to protect the authenticity of the diamond throughout its life. Everledger publishes certain data on a public blockchain for anyone to view authenticity, but also leverages a private blockchain with tightly controlled permissions given only to those authenticated to modify or access provenance records.

"The diamond market is well suited for early adoption of blockchain. For one, the industry is hyper consolidated: you could count the number of mining companies on two hands; the middle layer is supported by a generation of diamond cutters mostly residing in India, and there are only a handful of certificate houses around the globe. From there, are a series of banks and of course, thousands of retailers. 'From the mine to the market,'" explains Leanne Kemp, CEO of Everledger. "Everledger sits in the middle part of the pipeline where transparency is paramount for preventing fraud, reducing numerous fees (per diamond), increasing industry liquidity, and also for providing a public ledger such that consumers have full visibility around what they are buying."

Everledger has registered more than 1,000,000 diamonds globally on its immutable platform. Diamonds have very clear cut specifications, but Everledger is also entering into the fine arts market, using the platform to track (and prevent fraud and theft) of priceless pieces of art as they travel for international exhibitions. Provenance, ownership, exhibition history, gallery information, literary references to that work of art, as well as size, subject, title, and medium are tracked. The object's authenticity is verified by the institution before proof of provenance, defined attributes and unique data points are collected and written into the blockchain. This provides a digital provenance record for financiers, insurers, and current and future art owners.

Walmart recently announced a large-scale pilot in conjunction with Beijing's Tsinghua University, IBM, Hyperledger, and Jinluo, China's second largest pork provider, to improve food safety across its supply chain. Pork is the most popular meat consumed in China, but has high prices associated with food safety and product integrity. By placing farm origination details; batch numbers; factory and processing data; expiration dates; storage temperatures; and shipping information onto a shared ledger—one shared by just three nodes during pilot—Walmart and China aim to lower costs, manage product shelf life, and increase food transparency for all in the chain. While starting with three nodes, scaling to ten nodes alone "could save billions of dollars," according to Paul Chang, IBM's head of global supply chain solutions.

4.4.3 Interorganizational Record-Keeping

Relevant Industries:

- Financial Services
- Agriculture

- Healthcare
- Accounting
- Manufacturing
- Electronics
- Retail
- Entertainment
- Education/Academia
- Government

The Case for Shared Record-Keeping Using Blockchain:

According to the International Standard for Organization (ISO), the definition of records is "information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business." A ledger is a system of record-keeping; a decentralized ledger is one shared and maintained by numerous parties. What blockchain enables is a sort of "transactionalization" or "financialization" of records, where instead of merely collecting records in one static repository, records can be collected and exchanged, based on transaction rules, contracts, and permissions. It is also worth noting that such records do not have to be tokens or items of value, and that blockchain can store any kind of data, financial or otherwise.

One could reasonably argue that record-keeping is less of a distinct use case, and really the inherent characteristic of the technology; indeed, it underlies every other use case outlined in this report. But to consider the use case for interorganizational record-keeping is to consider the potential applicability of this technology for any organization. It is also distinct insofar as record-keeping is not exclusively used for compliance or authentication, but always for invoicing, reconciliation, and analysis.

As humans continue to digitally measure every quantifiable reality possible, from weather to soil, municipal parking, advertising impressions, genomics, and everything in between, the ability for organizations to securely exchange data more widely and more rapidly (while maintaining security) becomes essential for generating new value. Using a blockchain for interoperational record-sharing could significantly reduce costs of systems integration, data storage, systems maintenance, and so on. The verification process for distributed ledgers can also augment the authenticity and reliability of data referenced, increasing the overall value of the "shared ledger" compared to many disparate private databases. Through encryption, hashing, and meticulous permissioning, development of smart contracts, multi-party computational security, and (likely) configuration of multiple blockchains and sidechains, secure sharing across many untrusting parties could be possible.

Blockchain offers a way for all organizations to jointly manage a shared archive, preventing malicious actors from corrupting it. But this is easier said than done. Barriers to this are numerous and we still have a number of technological hurdles to clear and extensive experimentation between today and a fully interoperable world with *standardized and secure* data collection, sharing, transaction, and logic. Also, encryption and transparency requirements vary widely across industries. Then, there are challenges that are more difficult to unseat, such as trust, paranoia, competition, proprietary business cultures, etc.

Examples:

All of the examples across use cases involve some type of interorganizational record-keeping. Supply chain, real estate, compliance, and healthcare are a few areas where the number of organizations required to adopt a DLT constitute a very large critical mass before anyone sees substantially greater value.

Tallysticks is an invoice automation software that creates immutable invoices using blockchain technology. Through integration with existing accounting and enterprise resource planning (ERP) systems (e.g., IBM, Sage, Dynamics, etc.), invoices can be reconciled in real time. The company is also creating an invoice financing marketplace wherein businesses of any size can privately offer invoices for sale by connecting them to investors on a globally accessible factoring platform that allows for customizable auto-lending and pre-configured payment terms.

4.4.4 Physical Asset and Anti-Counterfeit Certification

Relevant Industries:

- Manufacturing
- Electronics
- Agriculture
- Healthcare
- Pharmaceuticals
- Luxury Goods
- Rare Earth Minerals
- Retail
- Entertainment
- Education/Academia
- Trade Skill Labor
- Accounting

The Case for Asset and Anti-Counterfeit Certification Supported by Blockchain:

Fraud exists among assets and products just as it does among people and processes. For physical assets, counterfeit exists at the product or component level, or even at the elemental level, such as in medication, chemical, or non-genetically modified organism (GMO) products. In 2015, the International Chamber of Commerce (ICC) claimed that the value of counterfeit goods exceeded some $1.7 trillion globally, roughly more than 2% of the world's total economic output. Interpol estimates that more than 1 million people die every year from counterfeit drugs (e.g., HIV/AIDS medication, antibiotics, anti-depressants, weight loss supplements, etc.), a lucrative business for organized crime groups.

Fraud also exists at the document level, for example, cash or other physical or digital assets such as coupons, tickets, or other tokens. Today's solutions for addressing the expensive problem of counterfeit are limited to special (sometimes expensive) equipment (e.g., labels, holograms, scanners, temperature-sensitive inks, watermarks, etc.), not to mention training agents with the skills to effectively use this technology.

Certifications linked to the identity of an individual's education or skill integrity, such as academic degrees, trade skills certifications, or compliance training certifications are yet another area counterfeit is rampant. So-called "degree mills" create more than 100,000 fake degrees each year, ranging from $1,000 to $10,000 per certificate; they also work with "accreditation mills," similarly fake institutions verifying fake degrees with fake accreditations. Verification of degrees is much more difficult when they come from overseas, as most degree mills are set up in ways that make it very difficult to identity or track down those running the operation. Costs are hard to quantify, but can be grave. Consider the costs of potential damage done by an individual with a fake medical degree providing surgery or a fake nuclear engineer working at a power plant.

In the case of skills certifications, verifying the degree on a shared ledger would help prevent fraud and enable easier authentication of advanced degrees globally. As for physical assets, placing the full history and integrity of a product, its sub-components, or any transfer of ownership and other authenticating details onto a distributed ledger from the beginning of an asset's lifecycle could play a significant role in reducing fraud and counterfeit. Upon sending a product, its information is registered in the distributed ledger and can be verified by anyone with access. A part or product could be labeled with a unique identifier that could be the product's public key, and as the product moves from one party on the supply chain to another, the number is signed with the sending member's private key. Any diversion from the product's intended path is viewable in real time, making it easier to track and identify stolen goods.

This use case could help prevent counterfeit asset development and exchange across numerous markets. Still, challenges remain, particularly around security and determining the "openness" (i.e., public, private, hybrid blockchain(s)) needed to bring forth the value. Similar to challenges in the supply chain use case, the need for wide buy-in and implementation across the network (e.g., the network effect) is what drives value to all counterparties; this value is limited unless the system is adopted by a majority.

(For an assessment of anti-counterfeit use cases involving individuals' identities, reference Section 4.1.4.3.)

Examples:

In addition to Everledger, the blockchain-based platform specializing in diamond registration and verification (referred to in Section 4.1.3.2), Blockverify is another company focused on product labeling and supply chain information storage in the blockchain, allowing users to check for counterfeit, diverted or stolen goods, or fraudulent transactions. In addition to diamonds, Blockverify is developing solutions for tracking pharmaceuticals, luxury products, and electronics.

4.4.5 Decentralized Online Storage

Relevant Industries:

- Information Technology
- Enterprise Storage

The Case for Decentralized Online Storage:

The original concept for DLT is decentralized, meaning DLT involves, even relies on thousands of computers or "nodes" to mine hashes and update the blocks (ledger) through a consensus mechanism. This architecture now supports decentralized cloud storage (also

sometimes called the cooperative storage cloud) where users can store their encrypted data and documents on a blockchain across many computers using cryptocurrency, spending a fraction of the cost compared to cloud-based storage systems.

The primary challenge associated with this blockchain application is trust, as users and particularly enterprises will be slow to place confidence and their most critical, proprietary, and sensitive documents on distributed network, even if such a network may indeed be more secure.

Examples:

A startup in the space, Storj, is also adding an additional business model to this by enabling users to "rent out" their own storage they are not using. The platform is currently working on polishing the interface and developing the backend to enable file transfers, communications, and other desired storage features before rolling out beyond a beta phase. It recently joined Microsoft's network of vendors supporting its Blockchain-as-a-Service (BaaS) offering with the goal of creating a new marketplace for storage.

4.5 IDENTITY AND ACCESS MANAGEMENT

4.5.1 IDENTITY ACCESS AND ENDORSEMENT MANAGEMENT

Relevant Industries:

- Government
- Financial Services
- Healthcare
- Education
- Collaborative Economy
- Telecommunications
- Media

The Case for Blockchain-Enabled Identity Access and Endorsement Management:

Identity on the blockchain exists dually as the user ID mechanism on a blockchain and also more broadly as the concept for who or what defines the participant in a transaction. This discussion will focus primarily on the former in order to illuminate the opportunity blockchain presents to safeguarding and streamlining identity when it is digitized.

In a formal "authenticatable" sense, our identities are linked to government-issued documentation. Although some of these can change, our names, addresses, Social Security number, passport, birth certificate, estate titles, marriage certificates, and other licenses are effectively contracts a person has passively with the state. (Refer to Section 4.1.4.2, which examines the use case for documentation and e-Residency services.)

Financial identity consists of account numbers, credit card numbers, personal identification numbers (PINs), and other identifiers we have with banks. Employment ID numbers, insurance account numbers, and vehicle registration numbers are examples of other identifiers we use in transactions. In an informal sense, our digital identities as they exist today are often tied to an email account, username, password, and data or content we ourselves generate in, for example, a social media or online community context. Today, none

of these identity mechanisms, be they state-issued, commercially issued, digital, or otherwise, are unified.

Placing identity documentation on a blockchain unites and streamlines both the authenticity of government-issued identifiers with the digital scalability of online identifiers. This could simply allow for much faster processing of KYC verification or fraud prevention, as outlined in Sections 4.1.5. But identity on blockchain could potentially digitize and verify identity in ways that are not easily verifiable today, such as reputation, endorsement, engagement, community participation, and so on. Decentralized social networks are also aiming to unify reputations across disparate social sites.

Encoding this onto a decentralized immutable ledger expands “identity” as a user ID mechanism. For example, consider a unified ledger containing ratings and endorsements from other counterparties with whom you have interacted or transacted. This becomes a powerful trust-enabler in a sharing economy context, in which sharing or renting high-value and/or very personal assets with strangers (like homes), trust and reputation are the more immediate currency than fiat.

Taking the potential of this use case deeper, consider the range of “authenticable” identity mechanisms that could serve as levers for trust, each applicable in different areas, but centralized to a single user-controlled digital identity.

- Resident ID (state-issued documentation, registration, address, etc.)
- Banking ID (account, asset, equity, credit, financial history, etc.)
- Biological ID (biometrics, medical history, genetic history, etc.)
- Employment ID (employer, role, accounts, security clearance, etc.)
- Trade/Certification ID (Trade, education, certification, etc.)
- Loyalty (company-issued loyalty programs, memberships, etc.)
- Device History (past and present login history across devices)
- Reputation (an individual's standing within any business or social interaction)
- Other ID (lifestyle, hobbies, general ID authentication, etc.)

What emerges as a long-term prospective outcome of digitizing identity on a blockchain is what many in the industry call “self-sovereignty,” or the idea that the individuals could control and leverage their own identity information themselves, offering tiered access only to those companies with which they want to engage. The democratizing impact associated with a shift of power, such as users controlling their own data, is a powerful one and will not come without significant push back from corporations that leverage user data monetization as central to their business models. Several banks and some governments are actively considering their roles as stewards or authenticators of identity, thereby retaining a central relationship with consumers, but leveraging blockchain to safeguard and permission data in ways not currently employed; for example, a user could allow a certain company to access only the data relevant to that company, instead of “all or nothing” models in place today.

Included in the umbrella of identity on the blockchain is also the notion of devices themselves becoming identifiable, authenticatable, and financially autonomous actors on the chain. In effect, anything that is connected to the Internet could become an actor capable of financial and operational (read: information) transactions. As mentioned in Section 4.1.3.1, devices in many sharing economy contexts, as well as those involved in a number of the distributed

energy, M2M/IoT-enabled, and other use cases will take on a number of autonomous roles involving exchange. To extend the autonomous car example, the car itself could:

- Manage, negotiate, exchange virtual currency and/or tokens
- Search the Internet for best prices, local mechanics, nearby charging stations
- Connect with other devices, to fulfill a delivery order
- Purchase electricity to charge itself
- Drive itself to locations it or other actors instruct (e.g., service, grocery, pick-up, etc.)

It quickly becomes apparent that devices themselves could accrue wealth and numerous transactional relationships with little or no human involvement. Identity management of devices is essential not only for monitoring, but holding accountable and safeguarding an economy in which machine interactions play an infrastructural role.

A number of challenges stand in the way of placing identities on the blockchain in a scalable and consumable way. First, this use case requires companies that are currently competitive (or estranged) to share data, but will they be willing to give up control to create more value for the customer? Second, there is a current imbalance in enterprise versus consumer understanding and influence in blockchain development. Who is deciding the fate (the objectives, the code, the integration, etc.) of such systems? Another challenge is around security and is a single identity management portal more vulnerable than many disparate ones? Can consumers handle management of private keys reliably, responsibly, and with what protections?

In reality, there are potential security and privacy downsides with any solution, but blockchain may offer more mechanisms for safeguarding (or deterring malicious actors). There are also regulatory issues to address, such as redefining identity, evidentiary access, accountability, consumer protections and consent, etc. These challenges are compounded when thinking about the rights and agency of devices themselves, when they, too, become actors on the chain.

Examples:

ShoCard is a digital identity mobile app geared toward consumers to protect privacy and unify a digital authentication standard similar to showing a driver's license. User identity data includes passports, financial information, and biometrics like fingerprints, facial maps, iris patterns, voice, and more. The information is encrypted, hashed, and written onto the blockchain with public/private keys, out-of-band communication, and two-factor authentication for safer storage and exchange from anywhere. Users control who receives temporary access to the private information on the chain. Currently, the company is working with banks and travel technology provider SITA to streamline KYC and traveler identity verification, respectively.

Tradle, which is developing blockchain-based technology that allows customers to verify identity data once, then forward that data as a package to interested parties without having to re-enter it, is one example of a platform serving both user control and consent, as well as that for AML/KYC compliance, insurance, and other enterprise use cases.

General identity parameters are, of course, a central module to any blockchain application, whether for patient protection and privacy in healthcare applications, M2M communications in manufacturing or supply chain, or financial account identity in the KYC context. Notable companies developing robust identity modules include Gem, ConsenSys' UPort, BitNation,

Blockstack, and others.

Another prism through which to consider identity, reputation, and personal content management using a blockchain is that of decentralized social networks. The idea of distributing software anyone can deploy across a network that is interoperable with other sites, platforms, and services and serves as a sort of "public utility," instead of a proprietary centralized ecosystem. A company called Synereo is championing this notion, aiming to provide its supporters dApps to connect, share, and exchange value directly, without the need for a central authority.

4.5.2 GOVERNMENT SERVICES, DOCUMENTATION, AND E-RESIDENCY

Relevant Industries:

- Government
- Entrepreneurship
- Crisis Services
- Real Estate

The Case for Government Services on the Blockchain:

Storing government-issued identity documentation, verification, transfer of capital, ownership registration, and other digital public services access on a blockchain constitutes another potential use case for blockchain technology. By registering titles, physical and/or IP, licenses, certificates, and other documentation on the blockchain, governments could potentially grant citizens the opportunity to more efficiently conduct transactions with each other, minimizing their dependence on lawyers, notaries, and other middlemen. Government services on the blockchain could range widely, from entrepreneurial programs to archival, land registry, disaster relief, and eligibility for countless other services. Storing tamper-proof verifications of citizen documentation, verification, registration, etc. helps save money, but could also profoundly impact society.

Today, there more than 10 million people around the world that are denied a national identity, and thus access to many services, from seeing a doctor to opening a bank account, not to mention voting or access to relief resources. This does not include the more than 200 million people worldwide in the midst of refugee crises, nor does it include human trafficking. Many millions more are undocumented in other ways, or forge their documentation. Birth certificates, deaths, works, taxation, migration, ownership, marriage licenses, and other identity-related documents verified on the blockchain would be unforgeable, time stamped, and publicly viewable for anyone to see, regardless of socio-political dynamics.

BitNation, for example, has created a project called Refugee Emergency Response to help solve the refugee identity crisis by restoring rights and services to the displaced in Europe. Voluntary autonomous identification and reputation systems (plus governance protocols) could reduce human trafficking, while also potentially eradicating government services (even borders) altogether.

It is also worth noting that in order to support and deliver any or all of the services mentioned above, which often involve numerous other departments, agencies, businesses, etc., a distributed ledger could streamline more rapid contract agreements, tendering, and settlement across counterparties.

Of course, the public sector is complex, fragmented, and manifests very differently across geographies and ruling parties. Even if inherently centralized (in stable countries), many governments remain highly disconnected at the local level with respect to organizational structures, data sharing, budgets, and other inconsistent capabilities. This renders most governments very slow moving entities and, in addition to high uncertainty, lack of trust, and skepticism on the part of consumers, spells major hurdles for wide-sweeping government adoption of blockchain in the short term.

Examples:

The Estonian government has been pioneering e-Residency, and the idea of government services stored, accessible, and delivered using a blockchain. The program, which already has more than 10,000 participants (from around the world), offers anyone (Estonians and non-Estonians) willing to pay 100 Euros a digital ID card and easier access to Estonia's residency and entrepreneurial services. This digital identity streamlines people's participation in Estonian banking, payment, company formation, company registration, document signing and exchange, tax declaration, and prescription filling. A small country welcoming immigrants, innovation, and investment, the program is aimed toward welcoming independent entrepreneurs to the Estonian economy.

It is worth noting that e-Residency is not citizenship or physical residency and an e-Resident still needs a visa to stay in Estonia. The program is still early, new capital generation is unclear, and concerns around double taxation and accountability related to international agreements loom.

In the United States, Delaware is working on moving state archival records to a distributed ledger. It is also encouraging private companies to register with the state by keeping track of equity and shareholder rights on the blockchain.

The U.K. government is currently looking at blockchain to manage grant distribution.

4.5.3 IDENTITY ANTI-COUNTERFEIT

Relevant Industries:

- Government
- Financial Services

The Case for Identity Anti-Counterfeit Enabled by Blockchain:

Identity fraud and forgery is a significant problem for countries worldwide and typically often underpins illegal activities, such as identity theft, illegal immigration, organized crime, and age deception. Typical forged (or stolen) documents include passports, Social Security cards, driver's licenses, birth certificates, and other government-issued documentation. To combat this problem, institutions invest in numerous costly security techniques (some of which carry other risks) like biometric authentication, specially designed printing materials, recruiting and training for inspectors, and technologies designed to identify forged documents or components.

Placing authenticated identity documentation onto a distributed ledger could help reduce this costly and corrupt practice, not only by streamlining identity authentication and access to government services, civil rights, and the like, but by limiting the capabilities of those who forge identity documents to drive human trafficking and other organized crime. Many of the themes and challenges discussed in identity access and documentation use cases (described above in Sections 4.1.4.1 and 4.1.4.2) apply to preventing identity fraud.

Examples:

Startups like OneName, ShoCard, ChainAnalysis, BitID, CryptID, and Civic are all focused on anti-fraud and identity theft using blockchain.

CryptID is an open-source ID system that uses blockchain, Factom and a triple-factor authentication to prevent identity counterfeit. As the company describes it, “the unique identifier is something you have, the password is something you know, and the fingerprint is something you are.” All data is encrypted and transferred to the blockchain, at which point, the data cannot be manipulated by any authority or by CryptID itself. The company then issues a quick response (QR) code that contains the customer’s unique ID number.

4.5.4 VOTING

Relevant Industries:

- Government
- Elections

The Case for Blockchain-Enabled Voting:

In a very real and increasingly important way, election fraud threatens the very fabric of democracy. By casting votes as transactions, blockchain could be applied to voting for elections, proxy voting in investment scenarios, and other forms of online voting. Voting via blockchain leverages both identity and transaction components, wherein an individual’s identity, authenticity, and eligibility dictate their ability to make transactions and could reduce fraud and many other integrity concerns.

In election voting, the current system typically relies on officials (people) counting (often) paper-based votes. In this model, there is very little way to detect a breach of security, tampering, or even if all of the original ballots cast were counted. Even when machines are used, there are risks of reliability and malfunctioning, not to mention bugs or hacking. With a publicly accessible blockchain, everyone can view and count the votes themselves in real time. Because of the decentralized way blockchain verifies transactions and immutably registers the event, no votes could be changed, removed, or added illegitimately. Cryptography protects ballots against tampering, and voters could conceivably change their votes using their private key and unique voter ID. In addition to blockchain voting applications and machines, some of the companies working in this area are developing redundant forms of audit trails, customizable ballots for super simple user interfaces, and administrative dashboard interfaces.

This technology could also be applied to online voting, where collaboration between individuals is essential. Examples might include voting for contests, event outcomes, games, community-oriented platforms, and so on. For these less critical scenarios, a public blockchain solution could assuage trust issues around control of the platform, ballot counting, and verification, thereby increasing participation.

Despite a strong democratic thirst for better and more reliable voting integrity, many hurdles (and experiments) stand between our current state and large-scale blockchain-based voting systems. Some caution the emergence of new risks introduced as a result, such as hackers targeting users' cryptographic keys through malware or interception, particularly if voting from personal devices like smartphones. Other challenges that surfaced center around the risk of miners hijacking an election by refusing to count votes if they are able to identify where blocks originate. The greater challenge may be less technical, and more social; voters' trust in credentials, security, and outcomes will dictate the longer-term vote of confidence in blockchain.

Examples:

Companies working on this issue include Blockchain Technologies Corp (BTC) and VoteWatcher, along with an application developed by the Australian Post to use blockchain to host elections.

One notable startup, FollowMyVote, is addressing the challenge of online voting via blockchain by allowing voters to use webcams and a government-issued ID. It recently issued an open invitation for hackers to penetrate its platform while simulating a mock U.S. Presidential election in November of 2016.

An example to watch is one emerging in Australia in which a new political party, the Flux party, is using blockchain technology to provide citizens an app in which they select how representatives should vote. Flux party representatives in the Australian Senate must then vote on every piece of legislation before them as directed on a proportional basis by registered voters using the app. The Flux party is a minority party today, but in a country ripe for increased democratic engagement, it provides an intriguing mode of voter participation.

4.5.5 Proxy Voting

Relevant Industries:

- Stocks & Investments
- Government

The Case for Proxy Voting Using Blockchain:

Proxy voting typically enables remote investors to vote during annual corporate shareholder meetings without having to physically attend. Proxy voting occurs when an individual casts a vote on behalf of a shareholder of a corporation to provide decision-making inputs across a variety of corporate matters, such as approving a merger or acquisition, electing new board directors, stock plans, and others. Verification is required for the authentication of the identity casting the vote, how the cast vote was recorded and counted, and a third party is responsible for delivering proxy statements and collecting votes, which is a costly distribution process.

Shareholders vote via personal accounts using a digital signature, the nominee registers the security holder's vote onto the blockchain with their digital signature, resulting in an ID number created and used to confirm that the vote has been received. One of the key benefits of placing proxy voting on a blockchain is to improve retail investor participation. Today, on average, institutions vote 83% of their shares, while retail investors vote just 28%, according to Investopedia.

In some cases and in other countries, proxy voting applies beyond investments, such as men proxy voting for disenfranchised women, one person voting for an entire family or village, or members of Parliament voting on behalf of other members. Blockchain can help streamline this process with the disintermediation of third parties and streamlining of the distribution process, saving paper, increasing transparency, and automating reconciliation. This use case still faces many of the same challenges as online voting using blockchain, namely around trust, implementation, and unforeseen risks.

Examples:

In February 2016, NASDAQ partnered with Estonia to support its e-governance platform to allow and authenticate shareholder participation, including voting and proxy voting, with companies listed on NASDAQ's Tallinn Stock Exchange. FollowMyVote has created a blockchain platform to support secure, authenticated, privacy-protective voting, both in proxy voting and in other private and public voting applications.

Russia's central securities depository, the National Settlement Depository (NSD), recently announced it has successfully tested an e-proxy voting prototype during bondholder meetings using a blockchain and aims to launch it across the Depository in 2017.

4.5.6 PATIENT RECORDS MANAGEMENT

Relevant Industries:

- Healthcare
- Medical Research
- Insurance
- Manufacturers
- Legal

The Case for Patient Records on the Blockchain:

Placing patient records, also known as electronic medical records (EMRs), on a blockchain is another area of intense focus for blockchain platforms, healthcare institutions, manufacturers, research institutions, and insurance companies alike. A number of the companies working in this area are exploring how to use blockchain to enable "data economics" or the secure, anonymized, exchange of Big (medical) Data to empower researchers. The other essential part of healthcare data economics as enabled by blockchain is the idea of a shared, interoperable database between hospitals, medical services, mobile apps, and other suppliers, such as insurance, manufacturers, and so on. One of the most costly inefficiencies in today's healthcare system is the lack of interoperable (and secure) databases, a cost totaling approximately $18.6 billion and over 150,000 lives lost per year, according to the Premier Healthcare Alliance.

Given the extensively siloed nature of healthcare systems and databases, not to mention the billions of dollars lost in disjointed healthcare processes, patient misdiagnoses, maltreatment, malpractice, incomplete records, and the labor involved in reconciling these issues, the medical industry has numerous incentives to streamline the massive amounts of data it collects for more efficient and secure use. Security, fraud, hacking, and data ransom attacks have been increasing over the last few years.

The ability to provide permissioned access across stakeholders, contribute to medical research, ensure supply chain integrity, equipment performance, more relevant data inputs, and patient experience are all additional incentives blockchain could potentially offer the healthcare industry. Most importantly, the efficiencies in data pave the way for better care, thanks to broader, more detailed, and accurate context delivered to doctors, but also personalized patient-centric data-driven recommendations for care, clinical trials, therapies, and so on.

Of course, healthcare is a highly regulated industry with extremely high risks and a legacy of powerful players lobbying for more profits and resistant to change. This industry moves slowly because of the high consequences of failure, and because investments in current technologies and systems run deep. This is an industry where blockchain adoption is about integration with existing systems, not overhaul or replacement.

As in other use cases, regulatory challenges loom over EMR and blockchain. Existing regulations like the Health Insurance Portability & Accountability Act (HIPAA), Health Information Technology for Economic & Clinical Health (HITECH), and what constitutes as meaningful use of data require assessment, as well as close coordination to translate evolving legal structures into code and smart contracts.

Data integrity remains an ongoing challenge, as integrity checks must be encoded, regulated, and addressable. Consider the risks, for example, of a medical device being hacked, and false data streaming into an immutable ledger. Security and privacy are two of the central barriers to creating an EMR backbone, not only with regard to external malicious actors, but potential abuses or even inadvertent errors by medical providers themselves. Then there are instances of potential disenfranchisement, if insurers, for example, were able to access data on hospital visits to determine eligibility of coverage, or modeling for premiums.

Examples:

In the United States, a number of companies are working on EMR-blockchain use cases, notably Gem, the Hyperledger Project, IBM, Philips, and MedRec. Another startup,

Blockchain HealthCo, is working on allowing users to monetize the use of their data by research institutions.

MedRec is a system that was developed by a team of graduate researchers out of the Massachusetts Institute of Technology (MIT). The system uses the Ethereum blockchain to manage medical records. It links medical records across hospital and clinic databases, but is designed to offer patients control over their data. Patients can select healthcare providers, as well as researchers and specific family members. The project boasts a few novel initiatives, such as the inclusion of personal data from wearables like Fitbit and Apple Watch, as well as from the genetic testing analysis tool, 23andMe. It also incentivizes its miners—those who validate blocks and add them to the blockchain—who are medical researchers with access to census-level data of the medical records. This unites both research institutions and healthcare companies on a shared distributed ledger.

Part of the Estonian government's adoption of DLT introduced a medical records initiative in which patients can view who interacts with their medical records at any time.

Du, a telecom provider in the United Arab Emirates (UAE) announced a pilot program to facilitate the secure transmission of electronic health records between hospitals and clinics. It will work in partnership with the Global Blockchain Council, alongside 40 other organizations (banks, enterprises, startups, and regulators) to develop the blockchain-based solution.

4.5.7 Genomic Data Management

Relevant Industries:

- Healthcare
- Medical Research
- Legal

The Case for Genomic Data Management

Our genomes are intrinsically our most personal assets. DNA holds incredible insight into our expressions as individuals. With the advent of numerous technological innovations in healthcare and wearables, this information is increasingly being captured, stored, and commoditized. It is also subject to myriad current cybersecurity threats facing companies and individuals.

One use case being explored from both security and research standpoints is the idea of placing an individual's genomes on a decentralized ledger. Once data is stored and replicated over many peers and blocks, it is far less likely to ever be lost or hacked. Smart contracts could be used to allow individuals to control who accesses their data, even enabling payment for it. Long term, future generations could have greater insight into the genomic make-up, medical lives, and context of their ancestors, which is important data with the rise of “precision medicine.”

This is a very emerging space and one that will likely move slowly given the intensely sensitive nature of this data and general skepticism of blockchain in its early days. While also moving slowly, placing patient records (EMRs) on distributed ledger systems may, in some cases, include genomic data. All challenges related to blockchain-based EMR apply to genomics, underscoring the risks of security and privacy.

Examples:

A company called Genecoin provides a blockchain-based storage mechanism for healthcare records and genomic data to be backed up using Bitcoin. Users sample their DNA and then Genecoin turns it into data and stores it on the Bitcoin blockchain. It is then irrefutably tracked, managed, controlled by the individual, and time-stamped.

4.6 AUTOMATED COMPLIANCE

Relevant Industries:

- Government
- Law
- Financial Services
- Insurance
- Healthcare
- Pharmaceuticals
- Energy & Utilities
- Oil & Gas
- Manufacturing
- Industrial
- Real Estate
- Agriculture
- Food, Beverage & Hospitality
- Travel

The Case for Automating Regulatory Compliance on a Blockchain:

In the United States alone, regulatory costs add up to approximately $1.8 trillion dollars—a number that exceeds the gross domestic product (GDP) of many of the world's major economies, according to the Competitive Enterprise Institute. Regulations are important to consumer, business, and environmental protection, but there is tremendous inefficiency between regulatory writing, implementation, and execution, particularly as the world grows evermore connected and globalized.

Regulators can use blockchain's underlying immutable ledger technology to observe (in real time) companies' adherence to compliance standards because the distributed methodology for collecting the information renders it as a documentary of the truth. Regulators could have read-only access to private blockchains allowing them to play a proactive role in analyzing the information, dramatically reducing time, efforts, and costs associated on regulatory reporting.

Blockchain can also help support compliance indirectly through, for example, adding the "steps needed for compliance" to the ledger (proof-of-process), allowing regulators to monitor actively rather than retroactively. In trade finance, for example, compliance could be encoded (through smart contracts) into the blockchain so that regulators could oversee the occurrence of customer screening in compliance with counter-terrorism and international

sanctions. In manufacturing, the details of a product's specifications and radio frequency emissions, for instance, could be tracked through a sensor and included in the ledger. Such compliance use cases vary widely as regulatory compliance varies widely by industry and geography.

The opportunity for blockchain-automated compliance is well illustrated by Volkswagen's (VW) recent emissions scandal. The automotive manufacturer was found to have deployed a "defeat device" on its cars after finding they were emitting nitrogen oxide levels that exceeded environmental protection regulations. Although blockchain alone would not have been able to stop Volkswagen from tampering with its data or automotive architecture, it would have very likely deterred VW from committing fraud. Why? Because car data documentation would have immutably stored the original emissions onto the ledger and regulators would have had access to such documentation, potentially even in real time.

The challenges inherent in re-writing, writing entirely new, and automating compliance are, in most cases, the greatest barriers to blockchain adoption. This does not even account for the overarching question of when regulators should take a proactive and immediate approach to blockchain regulation versus a wait and see approach so as to avoid premature hampering of innovation.

Regardless, the challenge is one of cooperation and coordination, not just among diverse counterparty stakeholders, but across international regulatory principles. How will companies encode compliance into a system that is not limited by jurisdiction? What definitions must be reconsidered, such as the classification of assets, and who decides? How can regulators, lawyers, business practitioners, and developers coordinate to ensure contract law is adequately reflected in automated or smart contracts? Is legislation sufficient, or would regulators need to regulate distributed ledger code? If an issue is found in the code, how would remedies be enforced and against whom? How can regulation both enable blockchains to scale while protecting privacy, safeguarding permissions, and enabling security? How are regulators' own interests involved in this development? (See Section 2.3.4.1 for a deeper discussion of challenges associated with blockchain regulation development.)

In contemplating a shift to a decentralized transaction architecture, most counterparties are looking to regulators to provide guidance, legal protections, and governance. This is no small feat.

Examples:

The New York Department of Financial Services (NYDFS) published the "BitLicense" regulations for virtual currency businesses in June 2015. The regulations were designed to prevent money laundering and improve cybersecurity for individuals using virtual currency. The regulators claim they developed the parameters not by assessing whether digital currency was "money" or "currency" as defined by current law, but by focusing on regulating the specific activities involved, such as transmission, exchanges, and selling, and the licensure of associated actors and intermediaries.

Another significant development worth watching is the recent vote by the European Parliament Members (MEPs) to build a task force (overseen by the European Commission) to build understanding and develop proposals and recommendations as necessary. "To avoid stifling innovation, we favor precautionary monitoring rather than preemptive regulation," reads the resolution published by EU authorities in June, 2016. The charge of the task force, as laid out in the report, is to regulate "… if and when the time is right to do so and if and when the structures to do so are in place. That of course doesn't mean that we

shouldn't do anything right now. For example, we greatly welcome the suggestion of the commission to apply the Anti-Money Laundering Directive immediately for virtual currencies." The report goes on, "… the key to smart regulation in such an environment of dynamic innovation is for the regulator to develop sufficient capacity, including technical expertise."

4.6.1 Anti-Money Laundering and Know Your Customer Verification

Relevant Industries:

- Retail Banks
- Investment
- Trade
- Real Estate
- Automotive

The Case for Streamlining AML and KYC Compliance Using Blockchain:

The World Bank estimates the amount of money laundered each year amounts to somewhere between $2 trillion and $3.5 trillion. To combat this tremendous problem, AML compliance and penalties cost banks approximately $18 billion annually. The size of this problem, coupled with the vast number of transactions and actors involved in international financial systems, not to mention the lack of data mutualization and duplicative efforts, means that AML procedures are extremely manual and labor intensive today. Manual processes, such as scrutinizing suspicious payment transactions, onboarding new clients, intensive reporting, compliance program maintenance, and recruitment costs, account for ~80% of total AML budgets, according to Goldman Sachs.

To verify the identity of new clients (a process known as onboarding), banks (retail and investment), insurers, creditors, and other institutions must conduct customer due diligence (CDD) processes in adherence with stringent regulations classified under KYC laws. These laws require banks and customers to provide proof of anti-corruption (e.g., AML, bribery, fraud, counterfeit, terrorism, politically exposed persons, etc.) documentation for review in order to participate in services. Banks must independently conduct due diligence on prospective clients, even if other banks have verified the same client. According to Deloitte, KYC requests can take 30 to 50 days to complete on a satisfactory level.

Blockchain technology addresses numerous issues regarding inefficiencies in the current AML and KYC climate, and significant potential for cost reductions through headcount reduction, penalty avoidance, and technology expense reductions. First, a distributed, permissioned database of past and present transactions could streamline record keeping, reporting, and auditing, as well as efficiency in transaction surveillance by codifying rules around transparency, completeness of account information, and, ultimately, a reduced rate of AML false positives. Second, a secure, distributed, and highly permissioned ledger of client information shared between financial institutions could reduce redundancy without compromising due diligence for client onboarding. Third, it could enable real-time compliance monitoring and the ability to detect and target foul play far more rapidly than possible today. It could also potentially account for regional variations in KYC requirements; the United Kingdom, India, New Zealand, the United States, and others have distinct rules, subject to change based on political context.

This is a use case ripe for blockchain; as pressure mounts from investors and analysts for banks to reduce costs, most banks are only expecting compliance costs to increase, not to decrease. In 2015, American banks broke records for the amount they were fined due to failing KYC guidelines. It also follows that, in light of banks' interests in other areas, such as post-trade settlement and reconciliation, the use of a common ledger for KYC and AML verification will augment any efficiencies gained.

Due to extensive regulation, blockchain application in AML/KYC environments will continue to face extensive hurdles, including: governments legitimizing distributed ledger processing of fiat currency in order for banks to adopt and rely on it; enough (or a critical mass of) banks participating in mutualized data structures to "move the needle" on onboarding verification across counterparties; and for these shifts to occur across jurisdictions. Laws and provisions around customer data storage, access, and protection require assessment. Banks also face a general shortage of financial *and* technical skillsets to support development. Moreover, legacy IT systems slow adoption at scale. For now, however, numerous pilots and related consortia activities are underway.

Examples:

Select financial institutions have announced DLT pilots targeting KYC and AML, although at the time of this report's publication, none are in production. Some examples include Crédit Mutuel Arkéa, Thomson Reuters, and Rakuten Securities (in partnership with Japanese blockchain company Soramitsu).

While not run in a blockchain today, another notable solution is SWIFT's KYC Registry, which now has more than 2,500 financial institution members across some 200 countries. The registry is a centralized repository holding a standardized set of information required for KYC compliance; it is a centralized database, owned and monetized by SWIFT. The company released a white paper in September of 2016 outlining the role of standards (new and repurposed) in DLT.

IdentityMind Global is company that assists financial institutions with KYC and AML compliance through what it calls an eDNA platform. This is a collection of attributes that includes email, phone, geolocation, and passport verification; device validation, dark web insights; document verification; social network analysis; email reputation; and business information that define an individual when they transact online. As users transact, eDNA evolves, making fraud and counterfeit nearly impossible.

A startup called ChainAnalysis works with financial institutions to comply with KYC regulations as they evaluate and onboard new businesses in the Bitcoin space.

4.7 Prediction Markets

4.7.1 Decentralized Prediction Markets

Relevant Industries:

- Stocks & Investment
- Commodities Trading
- Insurance
- Elections
- News

- Weather

The Case for Decentralized Prediction Markets:

The concept of prediction markets allows individuals to buy and/or sell shares in the outcome of an event that places a market price on that outcome. Software sets the odds, collects the bets, reports the inputs, and disperses the rewards. That price reflects the probability that that event will occur. Many assert inherent informational value in prediction markets because they aggregate the sentiments and beliefs of market participants, in effect, forecasting the odds of an event. In some ways, like a more automated, transaction-heavy form of crowdsourcing, prediction markets have wide application potential and could be used for hedging against or forecasting everything from information in financial markets, to weather risks for insurance or agriculture, and to news and business decision-making.

Such a platform would almost have to run on a blockchain in order to avoid abuse, manipulation, and offer a shared, immutable, real-time ledger for all participants. While a powerful concept, prediction markets face extensive regulatory uncertainty. They require wide adoption, yet remain poorly understood by most. Another significant issue to address is reputation of users, bets, the veracity of outcome reporting, and their importance to the integrity of the system.

Examples:

Augur is one such blockchain platform working on facilitating prediction markets to support betting on outcomes, using reputation tokens to incentivize reliable reporting, distributing and redistributing rewards based on accuracy and strength of participation.

Another example comes from ConsenSys' Gnōsis component, a "pluggable" framework based on smart contracts to incentivize information betting and support prediction markets. According to ConsenSys, Gnōsis is underlying a variety of forthcoming projects involving the development of information aggregating wisdom markets, risk hedging, insurance, information trading, securities, decision making, and financial markets.

4.8 GAME CHANGING USE CASES DEPEND ON REGIONAL ECONOMICS

While many have argued that the Bitcoin blockchain was blockchain's first "killer app," the vast reach this technology *could* have suggests Bitcoin is really only the tip of the iceberg. Today, the application of DLT beyond Bitcoin remains, by and large, in the POC experimentation stage. It is simply too early to predict when and where blockchain will hit.

One dynamic about which we can be certain, however, is that use case adoption will depend on regional economics. While companies are assessing the applicability of blockchain based on a variety of criteria (see Figure 3.2), regional economics and what characterizes "readiness" for blockchain vary widely. For the purposes of this discussion, a number of factors set the backdrop for adoption velocity:

- Existing regulations and regulatory frameworks
- Incumbent IT systems investment and performance
- Current security requirements
- Number of industry counterparties involved
- Global or cross-border requirements
- Extent of costs/loss associated with the problem (fees, time, fraud, labor, life)

- Cultural/economic openness to innovation

The relative agility and size of a country like Estonia, for example, has allowed it to accelerate its e-Residency program. The comparatively limited scope and existing geographic and economic consolidation of the diamond industry's supply chain have allowed companies like Everledger to address all of the market constituencies in a relatively short amount of time. Companies like loyyal are targeting the loyalty space, given the size of the opportunity relative to far fewer regulatory hurdles they must clear compared to use cases in financial, healthcare, law, real estate, and so on.

SECTION 5
KEY INDUSTRY PLAYERS

Over $1 billion has been invested in the blockchain/distributed ledger space since 2015, across hundreds of companies touching every industry. Financial institutions, merchants, enterprises, governments, consortia, academia, and a vast number of developers are working furiously to push this nascent market to fruition. What follows is a summary of key industry players representing some of the most significant movements, investments, pilots, and incumbents in the blockchain market today.

5.1 BITCOIN BLOCKCHAIN

Year Founded:	2011
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	Luxembourg
CEO:	Peter Smith, Nicolas Cary, Ben Reeves
Number of Employees:	35
Services:	Bitcoin Exchange, Bitcoin Wallet, Bitcoin APIs, Block Explorer and Search

Company Profile:

Founded in 2011, the Bitcoin Blockchain is a web-based bitcoin platform that many point to as the most mature and successful blockchain to date. The platform is designed for safe, secure, and the easy use of bitcoins for both consumers and enterprises worldwide. In particular, it offers the most widely used Bitcoin APIs, the industry destination for block searching and exploring, and (currently) the most popular bitcoin wallets. The company has grown rapidly in the last few years, experiencing a rapid 2,100% expansion in a year-and-a-half as Blockchain exploded from 100,000 users to over 3,000,000 users. As of 1Q 2016, the company reported approximately 10 million active wallets. In October 2014, it announced a $30 million Series A financing co-led by Lightspeed Venture Partners and Wicklow Capital.

Many point to the Bitcoin blockchain as the only true blockchain in production and run at scale (both in terms of the number of nodes and volume of transactions). The Bitcoin tokens represent actual value instead of a representation of value, and this is what enables nearly instantaneous and zero-cost asset settlement of payments. Unlike its younger, broader public blockchain counterpart, Ethereum, which facilitates P2P contracts via its own currency and app vehicle (ether), Bitcoin blockchain deals only with cryptocurrency payment transactions and store of value specific to Bitcoin. The Bitcoin blockchain's block time is around 10 minutes, compared to Ethereum's, which is only seconds. Finally, the two differ in terms of hash algorithm, programming languages, and other basic builds.

Tractica found a variety of industry participants pointing to the Bitcoin blockchain as the likely fundamental infrastructure for digital value transfer, given that it is the only production-deployed, open-protocol solution that has been up and running reliably via independent miners for multiple years.

5.2 ETHEREUM

Year Founded: 2014
Annual Revenue: N/A
Ownership: Decentralized and Non-profit
Headquarters: N/A
CEO: Founders include Vitalik Buterin, Gavin Wood
Number of Employees: N/A
Services: Public decentralized ledger platform, programming language

Company Profile:

Ethereum is a platform and associated programing language that can be used to decentralize, trade, and secure transactions, both monetary and non-monetary, supporting the registering of events and activities by hardware, processes, individuals, and contracts. Developed through an online crowdsale in July to August of 2014, it remains an entirely public blockchain platform, distinct from the Bitcoin blockchain in that it supports more than financial transactions, more types of cryptocurrencies and tokens, and features smart contract functionality. It also features its own Ethereum Virtual Machine (EVM), which executes P2P contracts using its own ether cryptocurrency.

The Ethereum software project was originally developed by a Swiss company called EthSuisse, which has been transformed into the non-profit Ethereum Foundation, an open research, development, and education forum for the development of Dapps, protocols, and tools.

In its short life, Ethereum has enjoyed significant growth, even if its value has been somewhat volatile. Although its association with The DAO, a platform for the autonomous governance of investment capital (in ether) that failed due to poor governance and a bug in the code that was exploited, Ethereum's integrity remained intact. The Ethereum community resolved to hard-fork ("a backward-incompatible change" according to Wikipedia) The DAO and reversed the hack, although the drama brought about a drop from $21.50 to $15 in the price of ether during the attack. Since then, Ethereum has continued to double down on its development of security and smart contracts, particularly because the wide variety of applications the platform supports also implies higher complexity in software (which is difficult to encode and secure).

More and more institutions and enterprise blockchain software companies are also developing Ethereum-based applications. Some startups, such as ConsenSys and Smart Contracts, are building exclusively on Ethereum. IBM, Microsoft, JP Morgan Chase, Slock.it, Deloitte, R3, and many others are all working on developing Ethereum-based applications using private and/or hybrid Ethereum blockchains.

Since its inception, Ethereum's overall value in the price of ether, number of wallets, and use in public and private applications has grown exponentially. In May 2016, the market capitalization of ether was estimated to be around $1 billion; a figure that is almost certain to increase as many financial (and other) institutions continue to leverage elements of Ethereum for their own application development and testing, supporting use cases far beyond Bitcoin.

5.3 BLOCKCHAIN TECHNOLOGIES CORP

Year Founded: 2013
Annual Revenue: N/A
Ownership: Subsidiary of Global Arena Holdings
Headquarters: New York, New York
CEO: Nick Spanos
Number of Employees: 30
Services: Blockchain accelerator, blockchain application development

Company Profile:

Founded in 2013, and then acquired by Global Arena Holdings (GAH) in 2015, Blockchain Technologies Corp (BTC) is a tech company that acts as an early-stage investor, incubator, and seed accelerator program featuring six startups using blockchain technology. Currently, startups under the BTC umbrella include Slidechai LLC, Digital Assets Vending Inc., Cryptos, Overseas BC Marketing, and Blockchain Apparatus LLC. The company tends to develop blockchain applications for consumer-facing markets, and is perhaps best known for its work on products supporting blockchain-based voting and Bitcoin automated teller machines (ATMs). The acquisition of BTC by GAH inserts blockchain into the heart of a publicly traded company. It also allows its other subsidiary, Global Election Services (GES) to leverage blockchain technology and scale blockchain-enabled voting worldwide.

BTC has developed its own blockchain called VoteUnit to support blockchain-based voting. The company has also worked to target other weaknesses in the current voting market by equipping new voting machines with commodity hardware, making parts easy to replace, offering open-source software code so anyone can audit its function, and providing back-up paper, DVD, and blockchain audit trails. The machine stays disconnected from the Internet to keep malicious actors from manipulating the votes as they are coming in, and burns the ballots to a DVD before it is connected to the Internet. Global Asset Holdings, its parent company has a subsidiary Global Election Services, which holds more than 4,000 labor union elections a year, the testbed for BTC's blockchain-enabled voting project.

BTC is also known for providing Bitcoin ATMs, which it calls Digital Asset Vending Equipment (D.A.V.E.) Bitcoin ATM machines. Since its founding in 2013, BTC has been working to both develop the hardware behind these machines and to expand its presence into locations worldwide. Functionality in any jurisdiction is also enabled through machine compliance with all necessary KYC regulations. They run on Android, are open-source, and widely compatible out-of-the-box. It has partnered with the Bitcoin Center NYC to increase public exposure and test machines in a live environment.

Additionally, BTC specializes in blockchain-enabled notarization and time stamping to avoid forgery and save time. It is also developing a self-executing will system; upon death, a person’s will automatically references official death files and distributes pre-defined assets without expensive court battles questioning the integrity of the will.

5.4 FACTOM

Year Founded: 2014
Annual Revenue: $1 million
Ownership: Private
Headquarters: Austin, Texas
CEO: Peter Kirby
Number of Employees: 30
Services: Blockchain platform, blockchain application development

Company Profile:

Founded in 2014, Factom is both an open-source platform built as a public utility and a corporation that builds applications on top of that platform. The company targets enterprises with BaaS applications designed to change how businesses manage data and keep, verify, and audit records of all types. Factom's specialization is in automatic "fingerprinting" of documents so that records can be easily analyzed for changes and scanned for integrity on an ongoing basis. It also touts advancements in addressing so-called "blockchain bloat" by taking high volumes of transactions and blocking them with one hash, using one transaction to represent all, and circumventing issues around speed, costs, and size limitations. Factom's blockchain technology secures data for large private and public organizations by cryptographically isolating or providing a cryptographically unique fingerprint of the data to Factom's immutable, distributed ledger. This immutable data serves as a proof-of-existence and source of truth for all future business processes.

Last year, the company announced a partnership with the Land Registry of Honduras, although the project was later stalled. The company recently showcased its technology by developing a blockchain-secured version of the Gutenberg Library, which contains some 29,000 books. This POC was less about the library, and more about showing how Factom's API works; pointing to healthcare, law, and real estate for areas of real impact.

The company is working actively to set up a business community to help build out its own vertical use cases on top of Factom so that Factom can collect and monetize transactions. Factom's business model earns a small transaction on top of each transaction. The year 2016 has brought a number of notably developments for the Factom. Additionally, in the first two quarters of 2016, Factom has been formalizing new partnerships with other complementary offerings, such as Smart Contract, DataYes, and Rongdu Technologies. In June of 2016, the Department of Homeland Security's Science and Technology Directorate (S&T) awarded a $199,000 contract to Factom to study possible blockchain-based advancements related to digital identity in the IoT, specifically by creating an identity log that captures the identification of a device, its manufacturer, security issues, lists of available updates, and permissioned authorities. In June, Factom also landed a deal with the Chinese Government, working to help develop administration projects for smart city applications, such as storage, auditing, and verification of records. At the time of this report's publication in 2016, it has received $3.04 million in funding across four rounds of funding via Koala Innovations and Plug and Play.

5.5 CHAIN

Year Founded: 2013
Annual Revenue: N/A
Ownership: Private
Headquarters: San Francisco, California
CEO: Adam Ludwin, Devon Gundry
Number of Employees: 20
Services: Blockchain platform and developer community

Company Profile:

Founded in 2013, Chain is a blockchain platform solution designed for financial services institutions. Chain offers an open-source blockchain protocol, what it calls the Chain Open Standard, built around financial service institutions' requirements for security and, particularly, scale. (The platform boasts the ability to handle tens of thousands of transactions per second.) The solution has been and continues to be developed *alongside* some of the world's largest financial institutions—partners of Chain's for over a year in some cases—including Visa, Citi, NASDAQ, Fidelity, Capital One, and others.

One partner, NASDAQ, has launched one of the only in-production private blockchains today, known as Linq, with Chain to support trading shares in pre-initial public offering (IPO) companies. Chain has been working with and across its partners in developing its open standard by first identifying their critical challenges, prototyping a range of financial solutions, such as payments, capital markets, insurance, proxy voting, and so on, and finally, by generalizing success in prototypes into broader standards. Chain bills itself as a blockchain platform built bottom-up, "by and for the financial industry" and built to digitize a variety of different types of financial assets, from currency to gift cards to loans.

The Chain operating system (OS) is one of a few other consortium-driven distributed ledger technologies designed for financial services, among the likes of large, established organizations, such as IBM and the Linux Foundation, as well as smaller players like Hyperledger and R3CEV. Like most others, its open-source structure ensures interoperability and that partners are not locked into proprietary software. Also, like many other providers, Chain's business model is not in the protocol per se, but in developing and supporting applications and networks built on top of the standard.

With more than 10 of the world's leading banks in partnership, Forbes recently estimated the company's worth at more than $130 million. Chain has received more than $43.7 million in funding.

5.6 IBM

Year Founded:	1911
Annual Revenue:	$81.7 billion
Ownership:	Public
Headquarters:	Armonk, New York
CEO:	Ginni Rometty
Number of Employees:	377,000
Services:	Blockchain software, blockchain consulting, developer community

Company Profile:

Founded in 1911, IBM is a global leader in technology innovation and the largest technology and consulting employer in the world, but also one taking a very active role in blockchain development. The company, best known lately for its cognitive computing advancements in Watson and strong legacy in middleware and analytics, is pushing hard into DLT. It is doing this both by building its own blockchain platform (known as Bluemix) and embracing an open-source development model as the largest contributor of code to the Hyperledger project, a collaboration led by the Linux Foundation that includes other large technology companies, such as Intel, Cisco, Accenture, and others. IBM's strategy, both proprietarily and across the ecosystem, is to equip developers with the tools, community, mentorship (through Bluemix Garage), and a choice platform for their rapid prototyping and development of blockchain applications. IBM also offers certified distribution of IBM code submission to the Hyperledger project on Docker Hub, enabling application development across different cloud services or devices. By fostering an open-source community for blockchain development, IBM helps attract developers that do not want their skills or contributions tied to a single company.

IBM's blockchain offerings are tri-part. In addition to its open-source contributions via Hyperledger, IBM offers its own Bluemix Platform, a high-security, cloud-based platform designed for rapid blockchain network prototyping, including network monitoring, logs and ledger states, peer permissioning, API documentation, chaincode (smart contracts) deployment, dashboard analytics, and other modules. Finally, IBM offers consulting services (what it terms as technical pre-sales and delivery services) via its Bluemix Garage program, connecting customers with developers for a series of design-thinking workshops and agile development iterations toward building POCs.

IBM's strategy is to underlie blockchain applications across a variety of industries. In February, IBM invested approximately $60 million in Digital Asset Holdings, a consortia supporting open-source blockchain development for the financial services industry. It is also working with the London Stock Exchange Group and the Finnish business development organization called Kouvola to support their open blockchain technology development. The platform's inherent modularization, plus its tamper-resistant high-security-focused development offers cloud services with the highest Federal Information Processing Standards (FIPS 140-2) and Evaluation Assurance Levels (EAL) in the industry to support the use of blockchain in government, financial services, and healthcare.

It is also vying to be the choice solution for supply chain applications, and is currently being tested by Everledger, a leader in the blockchain market that provides provenance tracking for diamonds, from mines to jewelry stores and beyond.

IBM's partnership with Samsung in early 2015, the Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) concept, was one of the first enterprise blockchain pilots, using a mix of proof-of-work and proof-of-stake to secure transactions to retrieve software updates, communicate with other devices nearby, and facilitate energy bartering. Since then, IBM has

continued to lead the development of blockchain in IoT applications by applying blockchain to its Watson IoT platform, enabling sensor data from devices, RFID, GPS, temperature, appliance state, and barcode events to be incorporated into blockchain-based ledgers, and updating and/or validating smart contracts. This enables IBM to address blockchain opportunities across a variety of industries from logistics to manufacturing, electronics, automotive, and agriculture.

In August of 2016, IBM announced it would merge its internal blockchain team into a business unit called "Industry Platforms," which will encompass AI, cloud computing, Watson offerings, and oversee all related expert and developer ecosystems.

5.7 MICROSOFT

Year Founded:	1974
Annual Revenue:	$93.6 billion
Ownership:	Public (MSFT)
Headquarters:	Redmond, Washington
CEO:	Satya Nadella
Number of Employees:	118,000
Services:	Blockchain software, blockchain consulting, developer community

Company Profile:

Founded in 1974, Microsoft develops, licenses, and supports a range of software products and services. With regard to blockchain, Microsoft as a technology giant was a relatively early entrant to the blockchain space starting in 2014 when it announced partnership with bitcoin payment provider, BitPay. It currently offers a BaaS cloud solution that is powered by Azure, the company's enterprise cloud computing platform. In June of 2016, it released Project Bletchley, an open and interoperable platform composed of modular core blockchain services supporting identity, operations management, key management, privacy, security, analytics, and cryptlets (secure interoperability and integration components). The offering is designed to support the issue of integrating blockchain with existing infrastructures by offering tooling and plug-ins through partners to enable rapid development environments that run in the cloud.

Microsoft's blockchain strategy involves deep partnerships across a number of rising players in the space; chiefly, Ethereum and ConsenSys, but also BlockApps, Storj, Eris, MultiChain, Cetas Decentralized, slock.it IoT, ether camp, Augur prediction, and others. In addition to Ethereum, Microsoft is building its solution across various open protocols, such as Hyperledger and others. The partnership with Ethereum and ConsenSys currently enables Microsoft to extend blockchain "scaffolding" (i.e., Ethereum's contract programming language, Soldity) to its Visual Studio product. Specifically, ConsenSys and Ethereum work together to provide developers smart contract sample code, context-sensitive menus to support smart contracts, automatically generated ABI and binary files and user interfaces for rapid prototyping on the Ethereum blockchain, and private and consortium blockchains based on Ethereum as well. This is a strong move to support Microsoft's broad developer community and signals support for open-source, Ethereum, and ConsenSys communities as well.

In many ways, Microsoft's partnership strategy is built to enable developers. In August of 2016, the company announced it would offer BaaS to all users in its DevTestLab, the testing environment for Azure. At the time of writing this report, Microsoft is already supporting more than 26 blockchains in this environment. It also announced, in conjunction with ConsenSys, R3, Hyperledger, and BlockApps, the development of an industry group, KinaKatu, to

assemble top developers and researchers to share security and functional best practices for smart contracts.

The blockchain division is led by Marley Gray, who previously led Microsoft's technology strategy for the financial services vertical. Yet, Microsoft is taking a broad approach to blockchain, one far beyond financial services. Its partnerships and developer community focus signals an aggressive approach in injecting Azure across any environment. According to a blockchain lead for the program, the long-term differentiation for Microsoft, a leader in document and database technologies, is in understanding how to leverage its existing suite with such wide penetration: Exchange, Office, Windows, BI, database products, and so on. Also, similar to IBM, Microsoft is bundling blockchain with the rest of its suite of cloud services.

5.8 CONSENSYS

Year Founded:	2014
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	Brooklyn, New York
CEO:	Joseph Lubin
Number of Employees:	70
Services:	Blockchain software, blockchain consulting, blockchain infrastructure

Company Profile:

Founded in 2015 by Joseph Lubin, one of the original creators of Ethereum, ConsenSys calls itself a blockchain venture production studio, which develops blockchain software applications developed (primarily) on the Ethereum blockchain. The company has three arms: first, its platform product; second, a series of infrastructure tools including BlockApps, a series of enterprise-level deployment tools for private blockchains; and thirdly, ConsenSys Enterprises, a consulting arm that already included Deloitte, Microsoft, and Manulife Financial as customers. The company expressly identifies its strategy as one of exploring for-profit activity and ecosystem development by building "the paradigm of engineering" for businesses interested in leveraging blockchain. A theme across its projects is the concept of reimagining the user experience (UX) of complex concepts such as wallets and private keys in a way that drives widespread adoption. It already has approximately 100 paying enterprise customers.

ConsenSys is involved in the development of numerous projects, including incubation, coordination, investment, and the formation of joint ventures. Many projects are born and die as POCs, but others have grown into pilots and production systems. ConsenSys is not unique in providing blockchain applications, or even consulting support, but it is notable in that its projects touch a wide range of industries, from accounting to document management, energy, music, enterprise collaboration, and beyond. Some of its current projects include:

- **uPort:** An Ethereum blockchain-based identity management system supporting self-sovereign persona management with heightened security through private keys kept in secure sandboxes.
- **Gnōsis:** ConsenSys' framework based on smart contracts to support prediction markets designed so that the mechanism of market making is pluggable and can be part of the value proposition of each market. Gnōsis will support a variety of forthcoming projects involving the development of information aggregating wisdom markets, risk hedging,

insurance, information trading, securities, decision making, and financial markets.

- **Balanc3:** A triple-entry accounting system framework enabled through smart contracts. It takes double-entry books and instead of payment being a copy, it is literally sharing a software object, so there is no way for either party to falsify that data. ConsenSys is working with accounting consortia and a few different accounting software providers to integrate this capability.
- **Ujo Music:** A blockchain-enabled database of creative rights and rights owners, which automates ownership and royalty payments using smart contracts, designed to reroute value exchange away from intermediaries and more toward creators and end consumers of music, art, and other creative assets in the future.
- **Transactive Grid:** The joint venture with Lo3 Energy, which developed a blockchain-supported microgrid in Brooklyn in which it ran an experiment to meter electricity coming off solar panels including P2P solar sales along a microgrid using blockchain with payments through PayPal.
- **Decentralized Utilities:** Via partnership with RWE, German power and utilities provider, exploring business models for lowering costs related to energy transmission by enabling "prosumer" buyers and sellers to participate in P2P transactions and trading of energy.
- **Wayfund:** An equity crowdfunding platform, a system that allows you to create an arbitrary number of tokens and then can sell them in exchange for something else. Similar to a Kickstarter model, but instead of getting a t-shirt for your donation, you get tokens—tokens in the right regulatory environment, could behave like stocks.
- **Boardroom:** A way to provide governance to enable decentralized decision-making by giving shareholders a centralized system of accountability, voting, appointment, removal, provenance, and link to other Dapps.
- **Virtual Banks:** A joint project with Deloitte to create an entirely digital banking process by leveraging ConsenSys' uPort identity system, triple-entry accounting system, and Balanc3 to offer a digital suite of financial products.

The company is an official partner of Microsoft, Ubuntu, and a number of non-profit affiliations like the Smart Contract Foundation, the Ethereum Foundation, the Cryptocurrency Research Group, and Code to Inspire.

5.9 21.co

Year Founded:	2013
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	San Francisco, California
CEO:	Balaji Srinivasan
Number of Employees:	20
Services:	Machine-based microtransactions with Bitcoin; Bitcoin mining

Company Profile:

Founded in 2013, 21.co is a software company that has created an embeddable bitcoin mining chip able to be integrated into any Internet connected device. The chip makes possible continuous streaming of digital currency that can be used in a variety of applications, from energy to cryptocurrency mining to personal profits. The company envisions a network wherein machines are earning bitcoin on every hypertext transfer protocol (HTTP) request. With a single line of code, a developer can introduce

micropayments and machine-payable service. What this enables is the ability for machines to pay other machines automatically and in real time.

21.co offers two core products: 21 software package is a free offering that enables any device to connect with the 21 Marketplace. The 21 Bitcoin Computer is a $399 computer with native hardware and software support for the Bitcoin protocol. The marketplace enables developers to explore an index of existing applications on the machine-payable web and buy or sell APIs for bitcoin (no credit cards or bank accounts needed).

21.co remains one of the most well-funded blockchain companies, having received some $121.05 million in funding.

5.10 FILAMENT

Year Founded:	2012
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	Reno, Nevada
CEO:	Eric Jennings
Number of Employees:	40
Services:	Sensor development for machine-based microtransactions with Bitcoin

Company Profile:

Founded in 2012, Filament is an industrial IoT platform leveraging distributed architectures to run without the use of cellular or Wi-Fi networks. Instead, Filament offers devices (Taps) to create private low-power wide area (LPWA) mesh networks using LoRa radios without requiring a central network authority. These sensors allow industrial assets to act as autonomous agents “at the edge” and are able to execute smart contracts themselves, as opposed to smart contracts running in the cloud. Blockchain is used to authenticate devices and charge for network services using Bitcoin.

To support its decentralized offering, Filament also uses BitTorrent for P2P file sharing; Jose, a contract management protocol used to manage one’s own permissions; TMesh, for mesh networking; and Telehash for private messaging. The fundamental value prop this technology bundle brings is the ability for users to send only the data they design to the cloud, and leave much of it on the device itself, be it a soil sensor or a robotic tiller. Transactions and accounting occurs at the device level, saving users significant costs in data storage, infrastructure, and time. From an industrial perspective, the Tap + TMesh technology also enable users to retroactively connect devices that previously had no sensors or that cannot connect without network connectivity. Filament specializes in industrial spaces, such as agriculture, mining, oil & gas, and manufacturing. The company has received approximately $7.35 million in investment across 6 funding rounds and 23 investors.

5.11 SLOCK.IT

Year Founded: 2015
Annual Revenue: N/A
Ownership: Private
Headquarters: Mittweida, Sachsen, Germany
CEO: Simon & Christoph Jentzsch, Stephan Tual
Number of Employees: 10
Services: Blockchain software, developer platform

Company Profile:

Founded in 2015 and registered in Germany, Slock.it is an IoT solutions company developing blockchain infrastructure for the sharing economy. Its infrastructure uses blockchain technology to facilitate a trust-based system to enable anyone (organization or individual) to rent, sell, or share their property without a centralized institution through smart contracts. Put simply, it enables and manages temporary access to any physical object. Slock.it's blockchain infrastructure handles secure direct P2P payments via deposits, enabling seamless hand-off through logging events generated by connected devices, such as cars, lockers, apartments, office space, etc.

It runs on the Ethereum blockchain, which is open source, and being distributed, ensures 100% up-time, includes cryptographic security, does not require login, and can be audited by anyone. Ethereum also makes it possible to rent access to any compatible (Bluetooth, Z-wave, ZigBee, Wi-Fi) smart object or space and accept payments without intermediaries. This renders the connected world controllable not just via an app, but by the blockchain as well. In effect, what this means is that Slock.it's market becomes any place there are unused or underused assets, enabling both consumers and enterprises to turn their assets into income.

Slock.it's strategy also includes a large partner ecosystem, including Samsung, Microsoft, Shapeshift, RWE, Ubuntu, SafeShare, IPFS, and is now targeting partners across manufacturing, sharing economy, insurance, real estate companies, hotels, and other cryptocurrency companies.

Finally, Slock.it is quite unique in the market because it simultaneously developed The DAO, which served as both an investment mechanism and open-source computer program that runs on blockchain and defines and automates company governance and proposal execution without legal entity. The DAO launched on April 30, 2016, with a 28-day funding window in which it achieved the largest crowdfunding record of $150 million in funding. But in June, The DAO suffered an attack from an unknown hacker, which drained more than 3.6 million ether (equivalent to tens of millions of dollars) into a "child DAO" that had the same structure as The DAO. After uproar from the entire blockchain community requiring consensus around the solution, The DAO was rolled back through a hard fork wherein funds tied to The DAO were relocated to a new smart contract with a single purpose: letting all original contributors withdraw funds they made. By most accounts, The DAO itself will die due to its enormous failure so early in its life. Slock.it has remained relatively quiet about the incident and is in the midst of speaking with lawyers. Slock.it continues to believe DAOs will play a critical role in the infrastructure of the future service economy.

5.12 GEM

Year Founded:	2014
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	Venice, California
CEO:	Micah Winkelspecht
Number of Employees:	7
Services:	Blockchain application development, semi-consortia for healthcare

Company Profile:

Founded in 2014, Gem is a blockchain application platform that provides developer tools for rapid blockchain prototyping and deployment. In January of 2016, the company pivoted from its origins as a bitcoin-centric API (known then as BitVault) to a broader focus on expanding its tools to support enterprise use case exploration and implementation. Although the company still supports its bitcoin-focused partners, such as Bitwage and Purse, the company is focusing on and investing resources in *consulting/education* and *speedy prototyping* to enable blockchain applications, as the learning curve for financial and other institutions is far greater than among the bitcoin community.

It has a strong focus on applications for blockchain in healthcare, aiming to be the leading platform for blockchain in this market. It fosters Gem Health, a community of healthcare organizations and individuals to discuss the critical infrastructure, challenges, opportunities, and requirements across stakeholders. Specific applications supporting healthcare applications include clinical data, genomic data management, claims processing, and other modules. It also has a partnership with Philips Blockchain Lab to develop a patient-centric approach to blockchain-enabled healthcare applications.

Although healthcare is the company's primary vertical, many of Gem's OS components, such as GemData, a component that connects multiple databases, its Identifier for digital identity management, and Logic Layers, which allows rapid modeling of registries, renders the platform easily transferrable to other arenas. In particular, Gem is focusing on supply chain, manufacturing, aerospace, and energy markets as it scales. Gem is a strong believer in the concept of multiple blockchains interoperating among each other, thus, unlike some competitors, it is compatible with numerous blockchains, private and public, instead of sitting on top of just one. It believes that, in the long term, this strategy helps future proof the platform, given the nescience and current fragmentation of the blockchain market. The company has received approximately $12 million in funding over five rounds of funding since its impetus.

5.13 EVERLEDGER

Year Founded: 2015
Annual Revenue: N/A
Ownership: Private
Headquarters: London, England
CEO: Leanne Kemp
Number of Employees: 30
Services: Provenance tracking through smart contracts and APIs

Company Profile:

Founded in 2015, Everledger is an application provider of a shared ledger for the diamond industry. It is built on the IBM Blockchain IBM Bluemix network and delivered via the cloud and mobile. Hailed as one of the strongest in-production examples of a distributed ledger platform, Everledger uploads source and item specifications for the diamond industry, creating permanent records to protect the authenticity of the diamond throughout its life. With diamonds, 40 metadata points are collected and matched to the laser inscription on the stone, along with information on the stone's origin and history. This is then digitized and stored immutably on the blockchain.

Everledger exemplifies a hybrid blockchain architecture in that it publishes certain data on a public blockchain for anyone to view authenticity, but also leverages a private blockchain with tightly controlled permissions given only to those authenticated to modify or access provenance records. The company works with just about all stakeholders in the diamond pipeline, including miners, insurance companies, owners, claimants, and law enforcement agencies through APIs. Everledger has registered more than 980,000 diamonds globally on its platform, whose information is now immutable. Diamonds have very clear cut specifications, but Everledger is also entering into the fine arts market, using the platform to track (and prevent fraud and theft) of high-value, touring pieces of art. Provenance, ownership, exhibition history, gallery information, and literary references to that work of art, as well as size, subject, title, and medium are all tracked. While many more variables go into the authenticity of art and antiquities, the initial focus is on provenance, art vitals, and transaction processes associated with financing and insurance.

The company recently extended its offering from provenance tracking and services to digitize the UN-mandated Kimberley Process, a three-step verification system created in 2003 with 81 authorized countries to curb the sale of conflict stones and rough or "blood" diamonds.

5.14 XAPO

Year Founded: 2012
Annual Revenue: N/A
Ownership: Private
Headquarters: Zurich, Switzerland
CEO: Wences Casares, Federico Murrone
Number of Employees: 20
Services: Bitcoin wallet, vault, debit card, currency exchange

Company Profile:

Xapo offers customers, both enterprises and consumers, the ability to organize and manage bitcoin funds across accounts, and store exchanges securely. Enterprise customers, particularly institutions using bitcoins, can create unlimited wallets and vaults to partition

funds between functional teams or investment accounts. Xapo offers end consumers the ability to load their bitcoins onto Xapo-specific debit cards that look and function just like any other debit card and are accepted worldwide via Visa and PayPal.

The company differentiates itself on its security capabilities and infrastructure, combining "man, machine, and even mountain." The Xapo Vault consists of multiple layers of cryptographic security, including multi-factor authentication and private key segmentation. Enabled through offline encrypted servers that are never connected to the Internet, these vault-servers sit behind reinforced concrete walls, a steel blast door, and a radio-wave blocking Faraday cage within a decommissioned Swiss military bunker in the Alps. In addition to physical barriers of servers located deep in the Swiss Alps, Xapo also offers a redundant global network of storage vaults (located underground across three continents) to bypass any single security breach or regulatory action. The geographic dispersion of the Vaults is designed to protect assets from being seized by any government entity; if one jurisdiction is compromised, the other vault locations would remain intact. This network is constantly scanned and validated by Xapo via satellite-based X-ray scanning and system-wide security monitoring as well as 24/7 human and automated security guards.

Xapo has raised $40 million from Benchmark, Greylock Partners, Index Ventures, Fortress Investment Group, Ribbit Capital, and Emergence Capital Partners across 16 investors.

5.15 ABRA

Year Founded:	2014
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	Mountain View, California
CEO:	Bill Barhydt
Number of Employees:	N/A
Services:	Transaction platform

Company Profile:

Founded in 2014, Abra is aiming to disrupt the global remittance market by usurping the slow exchange times and high settlement fees (10%+) by using a blockchain-built global digital asset-management system with retail-banking functionality like payments and savings on the bitcoin blockchain. "The people's way to send cash" is the company's tagline.

In effect, anyone with a mobile device and an Internet connection can send money to anyone in the world many times more quickly and with a far lower fee (.25%). It is also working to build real-time currency conversion into its platform so that anyone can convert money from their platform into local currency. Using built-in reputation systems, a global positioning system (GPS), and other shared technology services, Abra is trying to turn its network into a worldwide ATM network. The app allows users to store digital cash on their mobile devices with a credit card or using an Abra Teller, and as such does not require users to have a bank account to use the service. The company has received approximately $14 million in funding since it was founded.

5.16 HYPERLEDGER PROJECT

Year Founded: 2014
Ownership: Linux Foundation
Leadership: Brian Behlendorf
Number of Employees: 10 staff; 30+ members; hundreds of developers
Services: Blockchain framework, open-source community

Foundation Profile:

Hyperledger began as a technology platform within Digital Asset Holdings, but DAH offered Hyperledger the company over to the Linux Foundation's Hyperledger project to open the technology back up to the community. The Hyperledger Project is a collaboration led by the non-profit Linux Foundation and includes more than 30 founding members and other large technology companies, such as Intel, Cisco, Accenture, etc. It is supported and developed by a large diverse community of technical, open-source contributors.

Hyperledger's mission is:

- To create an enterprise-grade, open-source distributed ledger framework and code base, upon which users can build and run robust, industry-specific applications, platforms and hardware systems to support business transactions.
- To create an open-source, technical community to benefit the ecosystem of Hyperledger Project solution providers and users, focused on blockchain and shared ledger use cases that will work across a variety of industry solutions;
- To promote participation of leading members of the ecosystem, including developers, service and solution providers and end users; and
- To host the infrastructure for the Hyperledger Project, establishing a neutral home for community infrastructure, meetings, events and collaborative discussions and providing structure around the business and technical governance of the Hyperledger Project.

To achieve this, the project's work centers on interoperability of stakeholders, protocols, and standards across their various blockchain deployments by developing a modular framework that supports different components for different uses (e.g., identity, storage, access control, contracts, etc.) The project also requires adherence to other charter guidelines consistent with The Linux Foundation's similar collaborative groups.

5.17 R3

Year Founded: 2014
Annual Revenue: N/A
Ownership: Private
Headquarters: New York, New York
CEO: David Rutter
Number of Employees: 70
Services: Blockchain consortium, blockchain research and development

Company Profile:

R3 is a blockchain consortium and technology company. It hosts research, design, and development efforts of blockchain applications in the financial system supporting 45 financial services companies. The company launched with 9 members in 2015 and has since grown its member base to 45, counting many of the largest financial institutions in the world,

including Barclays, Credit Suisse, J.P. Morgan, Bank of America, Wells Fargo, ING, and Santander, among many others, and more recently Microsoft, MetLife Insurance, and Toyota's Financial Services division.

The primary function of the consortium is to build education, mindshare, discussion, community, best practices, and strategic prioritization around understanding where DLTs can be most effectively applied to financial services, particularly around errors and settlement reconciliation. The company is taking strides toward this by developing trials and simulations involving blockchain applied to financial services in a closed environment with as many key stakeholders at the table as possible. To date, R3 has completed two trials, one leveraging Ethereum hosted on Microsoft's Azure platform involving 11 banks and the later trial hosted by multiple providers including IBM, Eris Industries, Intel, and Chain, which involved approximately 40 banks.

R3 is one of a number of emerging consortia centered on blockchain innovation for financial services (among other industries), including DAH, Hyperledger, and Ripple Labs. Consistent with its peer consortia, in April of 2016 R3 released Corda, a DLT for financial services with a protocol it purports is unique compared to existing blockchain architectures, such as Ethereum or Bitcoin, and is not a blockchain per se. First, Corda does not host a native cryptocurrency (e.g., BTC or ETH), rather it uses smart contract code to link algorithms directly to human language in legal documents. Second, not all data is available to everyone; Corda is designed so that only participating members can view or access certain information depending on workflow in order to preserve transaction privacy and trade data.

5.18 DIGITAL ASSET HOLDINGS

Year Founded:	2014
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	New York, New York
CEO:	Blythe Masters
Number of Employees:	30
Services:	Blockchain consortia; blockchain applications

Company Profile:

Founded in 2014, DAH is a blockchain technology provider of three core elements, geared to best serve financial services use cases. DAH's acquisition of Hyperledger in 2015 provided a foundation of DLT, although DAH has offered Hyperledger the company over to the Linux Foundation's Hyperledger Project to open the technology back up to the community. Blythe Masters, CEO of DAH, remains Chair of the Governing Board of Hyperledger. On top of its Hyperledger-based DLT sits DAH's Digital Asset Platform offering, on top of which it offers specific business application development focused primarily on post-trade use cases like settlement latency and counterparty risk mitigation. These applications offer business logic plug-ins and engines, which are connected across applications to the platform and, in turn, convert logic to services performed on the block.

The platform can execute transactions for both public and private distributed ledgers, as well as existing databases. DAH also acquired three other blockchain companies, including Bits of Proof, a bitcoin applications company; Blockchain.io, a vibrant developer community focused on building a software stack for decentralized DNS and identity mechanisms; and Elevence Digital Finance.

DAH also announced strategic partnerships with Accenture, Broadridge, and PWC, global consultants and system integrators with deep relationships in global financial institutions. The non-exclusive partnership means DAH's technology is likely to enjoy faster adoption and scale as offered, implemented, and supported by these companies. Numerous large financial institutions have invested in DAH, including J.P. Morgan, Santander, Citigroup, DTCC, Goldman Sachs, ICAP, and others. The young company has received approximately $67.2 million in investment since February of 2016.

5.19 RIPPLE

Year Founded:	2012
Annual Revenue:	N/A
Ownership:	Private
Headquarters:	San Francisco, California
CEO:	Chris Larsen, Jed McCabe
Number of Employees:	120
Services:	Ripple Payment & Exchange, DLT services, accelerator

Company Profile:

Founded in 2012, Ripple Labs developed its own protocol to support commercial applications of blockchain. Originally called OpenCoin, and created by Bitcoin developers, the company's early days were characterized by building the RTXP protocol for payment and exchange of cryptocurrency. In 2013, it offered the source code to the open-source community for P2P "full nodes." In June of 2016, Ripple obtained a virtual currency license from the NYDFS, making it the fourth company with a BitLicense.

Today, Ripple targets traditional financial services institutions with Ripple Pay Protocol. This "distributed trustless exchange system built around a consensus ledger" is designed specifically to support the unification of banking systems, offers a native currency (XRP), and provides features fitting within existing financial services risk, compliance, and information frameworks. The primary use cases served are international payment, cross-currency settlement, and foreign exchange (FX) market making.

Ripple is not a consortium, but it does play a guiding role in blockchain best practice development and standardization. In partnership with CrossCoin Ventures, Ripple supports a startup accelerator that funds companies working to advance the Ripple ecosystem. Ripple is also a co-founding member of the Digital Asset Transfer Authority (DATA), which provides best practices and technical standards for companies that work with digital currency and other emerging payments systems. The company has won more than eight awards for its innovation in FinTech, including the honor of being named one of MIT Technology Review's 50 smartest companies. Ripple has received approximately $38.6 million in funding since 2012.

5.20 VISA

Year Founded: 1958
Annual Revenue: $13.9 billion in 2015
Ownership: Public (V)
Headquarters: San Francisco, California
CEO: Charles Scharf
Number of Employees: 11,300
Services: Electronic payments solutions provider for businesses and consumers

Company Profile:

Founded in 1958, Visa is a global financial services company that operates the world's largest retail electronic payment network across consumers, merchants, businesses, government entities, and other financial institutions. Visa offers products such as credit cards, as well as a number of other supporting services like risk and fraud management, security solutions, digital goods transaction services, and mobile financial services.

The company has been experimenting in the blockchain space since 2014 and continues to participate in a number of new developments coming out of its payments research program. Worldwide, it has been hiring blockchain developers, including adding 750 engineers at its Technology Innovation Lab in India, focused entirely on blockchain. In 2015, Visa invested (approximately $30 million) in Chain.com, a developer platform for enterprise blockchain applications, alongside NASDAQ, Citi, Capital One, and French telecom Orange.

Visa already provides the credit card for processing the Coinbase Shift Card, a card that process cryptocurrencies, although this simply uses the card as a payout mechanism; the transactions themselves are not using a blockchain. The greater issue for scaled use of blockchain for Visa is dependence, given the sheer volume of transactions it processes each day, an average of 13,000 transactions per second. Amid Visa Inc's acquisition of Visa Europe, previously a separate entity entirely, the company has been developing out an international innovation hub to partner with startups.

The bulk of Visa's investment has been in cross-border remittance and settlement. In the last year, Visa partnered with a number of startups, including Chain, Epiphyte, and BTL's Interbit to create a platform enabling cross-border remittance and settlement to reduce costs, settlement time, and credit risk, and to leverage smart contracts for international transfer and compliance adherence. The idea for the POC is to invite a "handful" of European banks to participate. Similar pilots have been run by R3 and J.P. Morgan Chase.

In October of 2016, Visa unveiled its B2B Connect platform, an offering to enable international money transfers between businesses, having been piloted with 30 banks in 10 countries. Using Chain's software called Chain Core, the system is designed to enable businesses and their banks to transfer money between each other using Visa's rails instead of relying on messaging between intermediaries and/or corresponding banks. This allows payments to move in real time and reduces the need for legal agreements currently needed in case of payment failures. The platform will be available to businesses next year, and would compete directly with the likes of a number of POCs underway with R3 and Ripple.

5.21 BARCLAYS

Year Founded: 1690
Annual Revenue: $25.5 billion
Ownership: Public (BCS)
Headquarters: London, England
CEO: Jes Stanley
Number of Employees: 130,000
Services: Retail banking, corporate banking, wealth & investment management, investment banking

Company Profile:

As one of the world's oldest banks, Barclays provides financial products and services across Europe, the Americas, Africa, and Asia, and moves, lends, invests, and protects the money of some 48 million customers and clients worldwide.

Barclays, like a number of other banks, has been dabbling in blockchain technology since 2014. The company was reported to have planned some 45 experimentations in 2016 alone. None are in full production today and most are mere POCs, like a recent announcement of collaborations with Thomsom Reuters and five other banks to test smart contracts and manage affirmations and post-trade lifecycle processing for over-the-counter (OTC) equity swaps. In September of 2016, Barclays announced one of the first successful live trade finance transactions on a blockchain in which actual documentation tied to actual physical merchandise with real counterparties was transacted paperless, across borders and time zones in hours instead of days. The documentation of some $100,000 worth of dairy products took place on Wave's (a Barclays accelerator graduate) dedicated blockchain between agricultural co-op Ornua and Seychelles Trading Company, a food product distributor. The bank also announced a partnership with Bitcoin bank/exchange Circle in which the company will use Barclay's Corporate Banking to store sterling for its customers as well as the infrastructure to allow transfers from any U.K. bank account back and forth with Circle. The U.K. Financial Conduct Authority issued Circle an e-Money license to expand the efforts.

The company is an active member across numerous industry consortia.

5.22 OVERSTOCK.COM

Year Founded: 1999
Annual Revenue: $1.5 billion (2014)
Ownership: Public (OSTK)
Headquarters: Salt Lake City, Utah
CEO: Patrick M. Byrne
Number of Employees: 1,500
Services: Online retailer, blockchain-based trade platform

Company Profile:

Founded in 1999, Overstock.com is an Internet retailer offering brand names for very low prices. The company's leadership has been outspoken against Wall Street and the Federal Reserve, and been a strong advocate of Bitcoin for years. Overstock began accepting Bitcoin payments in January of 2014, pioneering the use of cryptocurrency for enterprise retailers, in addition to other tactics like placing select items on sale if paid for with Bitcoin, and even offering employees the option of being paid in Bitcoin.

In August 2015, the company unveiled Overstock's tØ.com, a blockchain-based private and public equities trading platform that is P2P. The project is run by Overstock subsidiary, Medici. The platform is designed to "make the trade the settlement" by issuing stocks and bonds as a digital asset, thereby eliminating the time (typically T+3) between equities trading as used by the DTTC. Overstock will thus offer two versions of its stock, one available on traditional trading systems, such as NASDAQ, and another on tØ. This means that Overstock shares will trade in two separate markets, potentially with two separate values.

In December 2015, the company's S-3 filing to offer up to $500 million in common stock, preferred stock, depositary shares, warrants, and units, in addition to debt securities, using DLT, was approved by the Securities and Exchange Commission (SEC). To test the platform fully, Overstock will issue 1 million tØ (blockchain-processed) shares as part of the project, out of a total of 25.29 million shares. At the launch of tØ, Overstock made clear its intention not to keep the platform for Overstock only, but to license the product to enterprise trading firms. In September 2016, it announced Keystone Capital Corporation, a securities broker-dealer will use tØ to provide brokerage services for blockchain securities trading.

Meanwhile, it announced the creation of Revolution 4, a blockchain consortium geared toward inclusion, participation, and collaboration of small businesses interested in exploring the technology, regulatory issues, standards, and requirements for blockchain. This is in stark contrast to R3's strategy, the consortia developed by (and consisting of) corporate financial services veterans and incumbents, which charges membership fees in the many thousands of dollars.

5.23 ADDITIONAL INDUSTRY PARTICIPANTS

Table 5.1 Additional Industry Participants

Company	Founded	Headquarters Location	Ownership	Size	Website
21.co	2013	San Francisco, CA	Private	100	https://21.co
Abra	2014	Mountain View, CA	Private	50	https://www.goabra.com
Anx International	2013	Hong Kong	Private	1,000	http://www.anxintl.com
Armory	2011	Baltimore, MD	Private	10	http://bitcoinarmory.com
Ascribe.io	2014	Berlin, GE	Private	10	https://www.ascrib.io
Augur	2015	San Francisco, CA	Non-Profit	10	http://www.augur.net
Barclays	1690	London, UK	Public	130,000	http://www.home.barclays
BitAccess	2013	Ottawa, Ontario, Canada	Private	10	http://Bitaccess.co
BitFinex	2012	Hong Kong	Private	15	https://www.bitfinex.com
BitFury	2011	San Francisco, CA	Private	20	http://www.bitfury.com
BitNation	2014	N/A	Non-Profit	3	https://bitnation.co/
BitPay	2011	Atlanta, GA	Private	40	http://bitpay.com
BitPesa	2013	Nairobi, Kenya	Private	10	https://www.bitpesa.co/
BitStamp	2011	Aldermaston, UK	Private	10	http://www.bitstamp.net
BitX	2013	Singapore	Private	20	https://bitx.co/
Blockchain	2011	Luxembourg	Private	65	https://www.bitpesa.co/
Blockchain Health Co	2014	San Francisco, CA	Private	5	https://blockchainhealth.co

Company	Founded	Headquarters Location	Ownership	Size	Website
Blockchain Technologies Corp (BTC)	2013	New York, NY	Private	10	http://blockchaintechcorp.com/
Blockstream	2014	San Francisco, CA	Private	35	www.blockstream.com
BTCC	2011	Xujiahui Shanghai, China	Private	70	https://btcc.com
BTCS	2013	Arlington, VA	Public	20	http://www.btcs.com
Case	2014	Rochester, NY	Private	10	http://www.choosecase.com/
Chain	2013	San Francisco, CA	Private	20	https://chain.co
Circle	2013	Dublin, Ireland	Private	150	https://www.circle.com/
Coinbase	2012	San Francisco, CA	Private	115	http://www.coinbase.com
Coindesk	2013	New York, NY	Private	15	http://www.coindesk.com
ConsenSys	2015	Brooklyn, NY	Private	70	http://www.consensys.net
Deloitte (Rubix)	1900	New York, NY	Private	10,000	http://www.deloitte.com/global
Deutsche Bank	1870	Frankfurt, Germany	Public	57,000	https://www.db.com
Ethereum	2014	N/A	Non-Profit	50	https://www.ethereum.org/
Everledger	2015	London, UK	Private	30	http://everledger.io
Factom	2014	Austin, TX	Private	30	https://www.factom.org
Filament	2012	Reno, NV	Private	40	https://filament.com/
Gem	2014	Venice, CA	Private	10	https://gem.co/
Gemini	2014	New York, NY	Private	10	http://gemini.com
GoCoin	2013	Singapore	Private	20	http://www.gocoin.com
HSBC	1865	London, UK	Public	155,000	http://www.hsbc.com
Hyperledger Project	2014	N/A	Non-Profit	10	https://www.hyperledger.org
IBM	1911	Armonk, NY	Public	377,000	https://www.ibm.com
Kraken	2011	San Francisco, CA	Private	30	https://www.kraken.com
Lisk	2016	Berlin, Germany	Non- Profit	12	https://lisk.io
LocalBitcoins	2012	Helsinki, Finland	Private	10	https://localbitcoins.com/
Microsoft	1974	Redmond, WA	Public	118,000	https://www.microsoft.com
Monax.io	2014	New York, NY	Private	15	https://monax.io
MultiChain	2016	London, UK	Private	3	http://www.multichain.com/
NASDAQ	1971	New York, NY	Public	3,000	http://business.nasdaq.com
Overstock.com	1999	Salt Lake City, UT	Public	1,500	https://www.overstock.com
Paymium	2011	Paris, France	Private	10	https://paymium.com/
PayPal	1998	San Jose, CA	Public	15,000	http://www.paypal.com
PeerNova	2013	San Jose, CA	Private	30	http://www.peernova.com
Philips	1891	Amsterdam, Netherlands	Public	77,000	https://www.philips.com
Provenance	2014	London, UK	Private	10	http://www.provenance.org
R3	2014	New York, NY	Private	70	https://r3cev.com
Rakuten	1997	Tokyo, Japan	Private	5,000	http://global.rakuten.com/corp
Ripple	2012	San Francisco, CA	Private	120	https://www.ripple.com
Santander	1857	Madrid, Spain	Public	78,000	http://www.santander.com

Company	Founded	Headquarters Location	Ownership	Size	Website
Slock.it	2015	Mittweida, Sachen, Germany	Private	10	http://slock.it
Smart Contract	2014	San Francisco, CA	Private	10	https://smartcontract.com/
Société Générale	1864	Paris, France	Public	146,000	http://www.societegenerale.com
Solarcoin Foundation	2014	N/A	Non-Profit	10	http://www.solarcoin.org
Stellar	2014	San Francisco, CA	Non-Profit	20	https://www.stellar.org
Storj	2014	Mableton, GA	Private	20	http://storj.io
Stratumn	2015	Paris, France	Private	10	https://stratumn.com/
Symbiont	2015	New York, NY	Private	15	http://symbiont.io
Tallysticks	2015	London, UK	Private	10	http://www.tallysticks.io
Tendermint	2014	San Francisco, CA	Private	5	http://tendermint.com/
Uphold	2013	San Francisco, CA	Private	75	https://uphold.com
Vagogo	2008	Palo Alto, CA	Public	10	https://www.vogogo.com
Visa	1958	San Francisco, CA	Public	11,300	https://www.visa.com
Xapo	2012	Zurich, Switzerland	Private	40	https://www.xapo.com

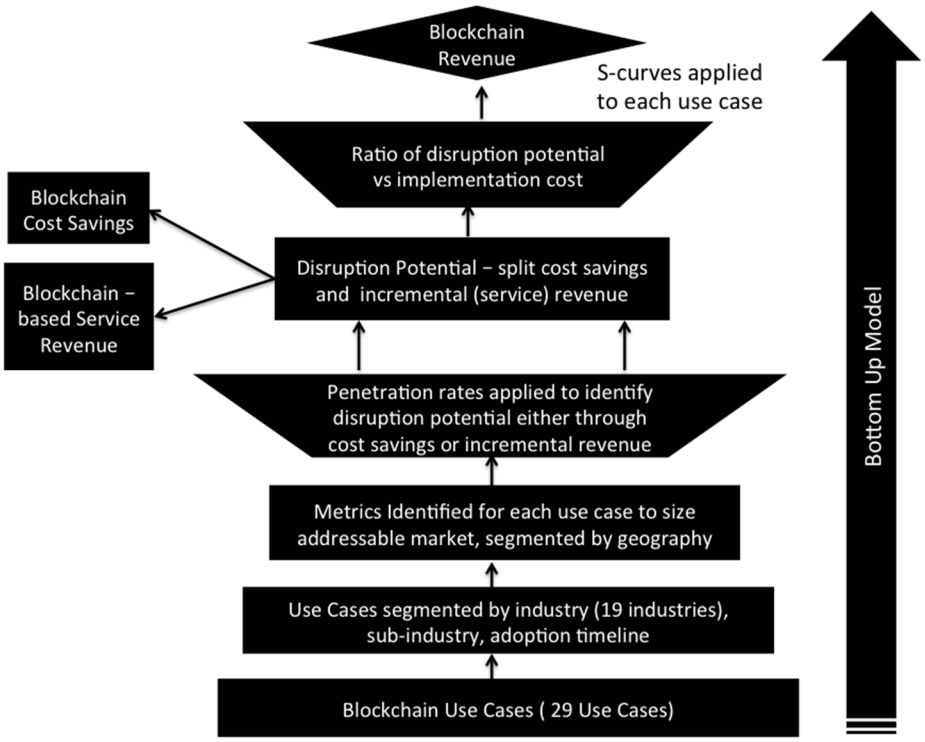
(Source: Tractica)

SECTION 6
MARKET FORECASTS

6.1 FORECAST METHODOLOGY

In preparing this forecast, Tractica utilized a bottom-up model to estimate blockchain revenue potential using blockchain use cases as the foundation. A baseline of 29 unique blockchain use case categories have been shortlisted through both primary and secondary research, focusing on both near-term and future applications of blockchain that have a realistic adoption timeline. The revenue potential is the cost of implementing blockchain solutions for a particular use case in a particular industry segment. For example, the blockchain revenue for payments in the financial industry is the revenue potential for IT vendors, system integrators, database vendors, and consulting firms in implementing a blockchain payments solution within a financial institution.

Figure 6.1 Blockchain Forecast Model Methodology



(Source: Tractica)

The methodology for estimating the revenue potential is explained in Figure 6.1. Each use case was explored in depth to identify industries of sub-industries where the use case could be applied. For example, the use case of supply chain management using blockchain has applications in multiple industries, including manufacturing, agriculture, logistics, and retail. Metrics were identified for each use case, in separate industries with the goal of finding the addressable market for blockchain solutions. Appropriate geographical splits were estimated for each metric. Each use case is known to have an addressable market or a disruption potential, which could be either cost savings and efficiencies brought about by the

implementation of DLT or incremental revenue earned from a blockchain-based service. The model applies a split on the disruption potential to estimate the cost savings and service revenue for each use case. It should be noted that some use cases are purely cost savings-based with no blockchain-based service revenue, and vice versa.

Blockchain revenue (the implementation cost of developing and deploying the blockchain solution) is calculated based on a ratio of implementation cost versus disruption potential. One of the benchmarks used to estimate this ratio is found in the financial implementation of blockchain. Based on research and interviews conducted by Tractica, the ratio of implementation cost versus disruption potential for the financial sector is between 15% and 20% today. Using this as a benchmark for a use case that has a large cost of integration with legacy systems that operate on a large scale, appropriate ratios were calculated for other use cases and industries. S-curves were then applied to each use case to estimate revenue across the forecast period from 2016 to 2025.

A further breakdown of the revenue is also presented, with revenue segmented by consulting, talent, hardware (cloud, on-premise, modules), software development, database, application integration, support, and management. Separate ratios were estimated for each use case to provide this software/hardware breakdown.

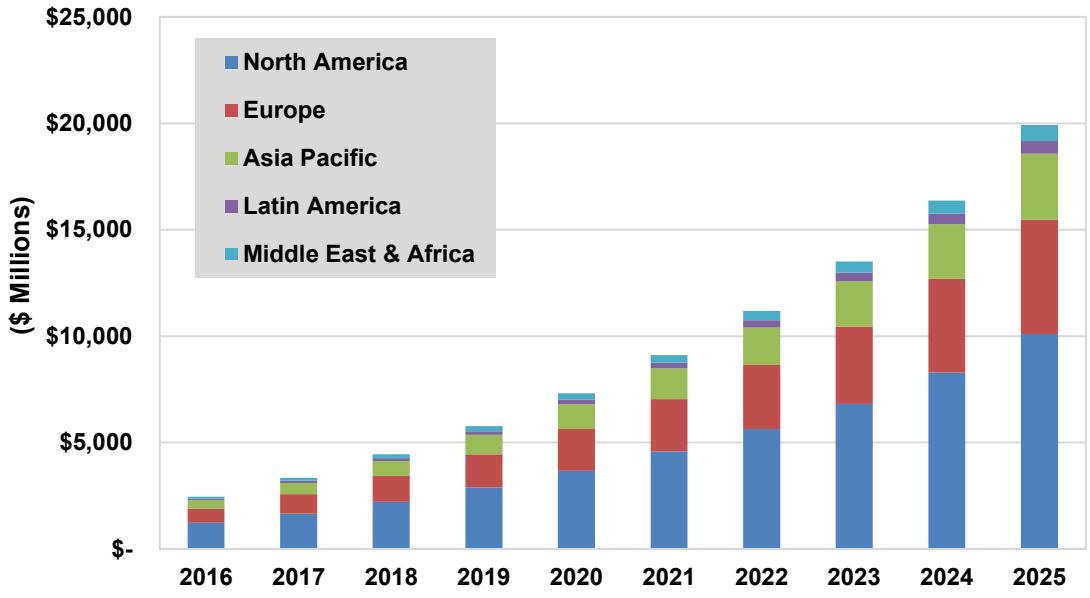
While the model does not account for new or future use cases that could emerge during the forecast period, Tractica believes that most of the new use cases that could emerge will be subsets or branches of the existing use cases that have been included in the model. Tractica also aims to keep track of new emerging use cases and will be publishing updates to the model and forecasts on a regular basis.

Detailed market sizing, segmentation, and forecasting tables are included in the Excel databook that accompanies this report.

6.2 GLOBAL MARKET FORECASTS

Tractica forecasts that annual revenue for enterprise applications of blockchain will increase from roughly $2.5 billion worldwide in 2016 to $19.9 billion in 2025, representing a CAGR of 26.2%. While a relatively lower CAGR than other emerging technology markets, Tractica forecasts that the blockchain market's growth will remain conservative for some time. Although the blockchain market has seen significant investment over the last 18 months, areas of growth will remain fragmented and contingent upon numerous macro forces far beyond the control of any single country, government, enterprise, or technology. Blockchain is unique among emerging technologies in that its growth is compounded by the "network effect." As more constituencies adopt the technology, Tractica anticipates a resulting acceleration in adoption.

Chart 6.1 Blockchain Revenue by Region, World Markets: 2016-2025



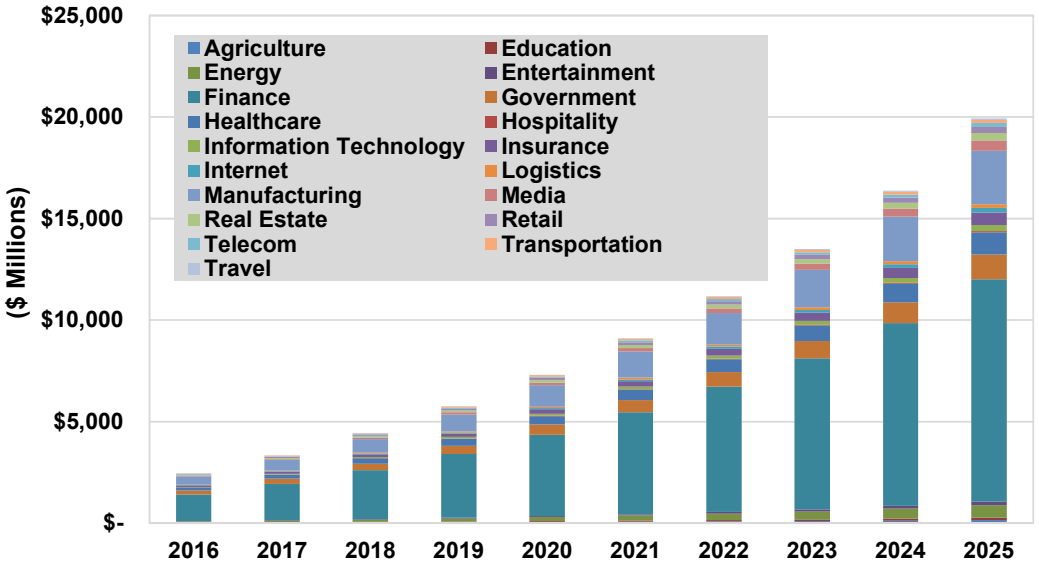
(Source: Tractica)

As with many technologies, the most robust adoption is already underway in North America, Western Europe, and China. Because of its decentralized nature, many of the financial institutions driving adoption to facilitate international currency transfer and post-trade settlement will likely push adoption into the rest of the world, beginning with areas in Eastern Europe, Southeast Asia, and the Middle East, and eventually spreading into India, South America, and Africa.

6.3 ENTERPRISE BLOCKCHAIN REVENUE BY INDUSTRY

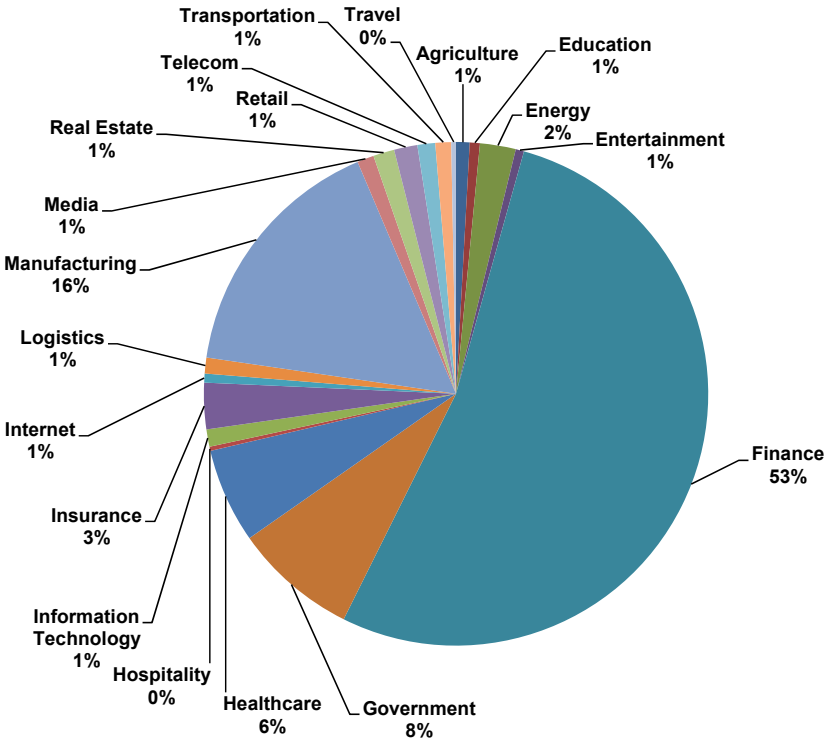
Blockchain technology is currently enjoying the greatest enterprise activity across the financial services industry. Yet the potential for this technology is widely applicable across a range of industries, particularly those with numerous counterparties involved to complete a transaction; those conducting a high frequency and volume of transactions; and those with low trust and a high potential for tampering, error, or fraud. Blockchain's transcendence from currency-only transactions into event-based transactions has extended its potential application into myriad industries. Tractica anticipates significant revenue opportunity in financial services, but also identifies healthcare, government, logistics, transportation, manufacturing, and energy as potentially ripe for efficiency, visibility, and security gains enabled by blockchain technologies. Indeed, adoption in one industry could also accelerate other industries' adoption as well, such as transportation's adoption impacting the media, travel, telecom, and even hospitality industries.

Chart 6.2 Blockchain Revenue by Industry, World Markets: 2016-2025



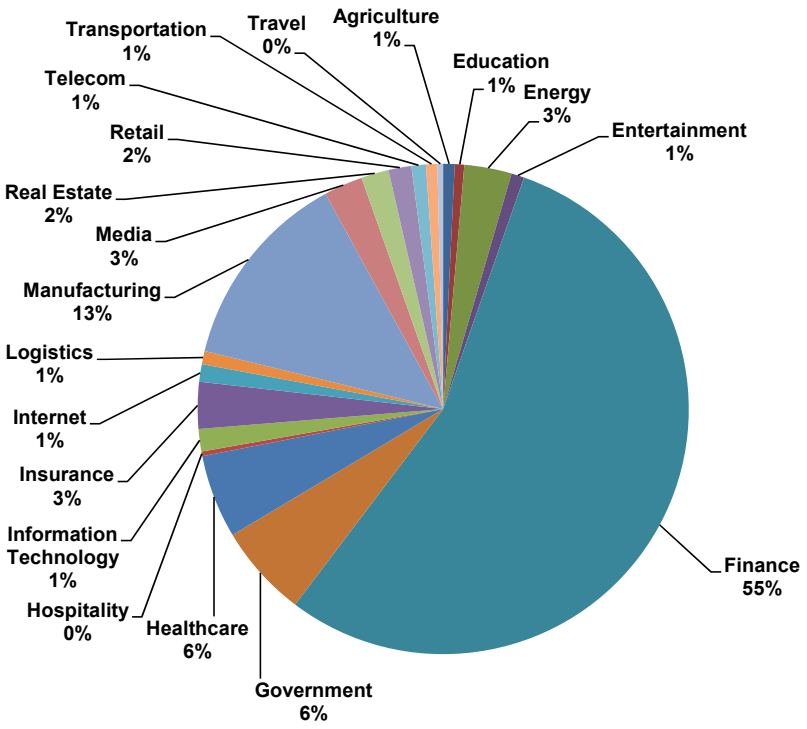
(Source: Tractica)

Chart 6.3 Blockchain Revenue Share by Industry, World Markets: 2016



(Source: Tractica)

Chart 6.4 Blockchain Revenue Share by Industry, World Markets: 2025

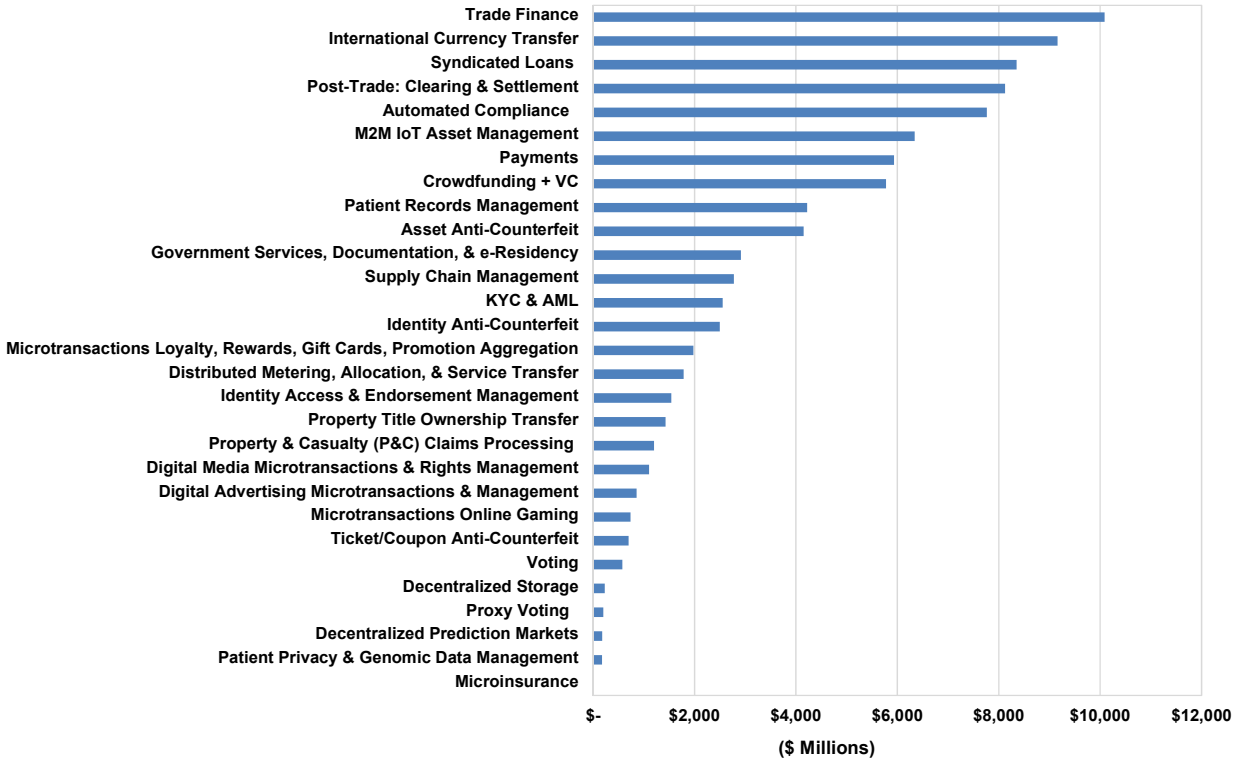


(Source: Tractica)

6.4 BLOCKCHAIN REVENUE BY USE CASE

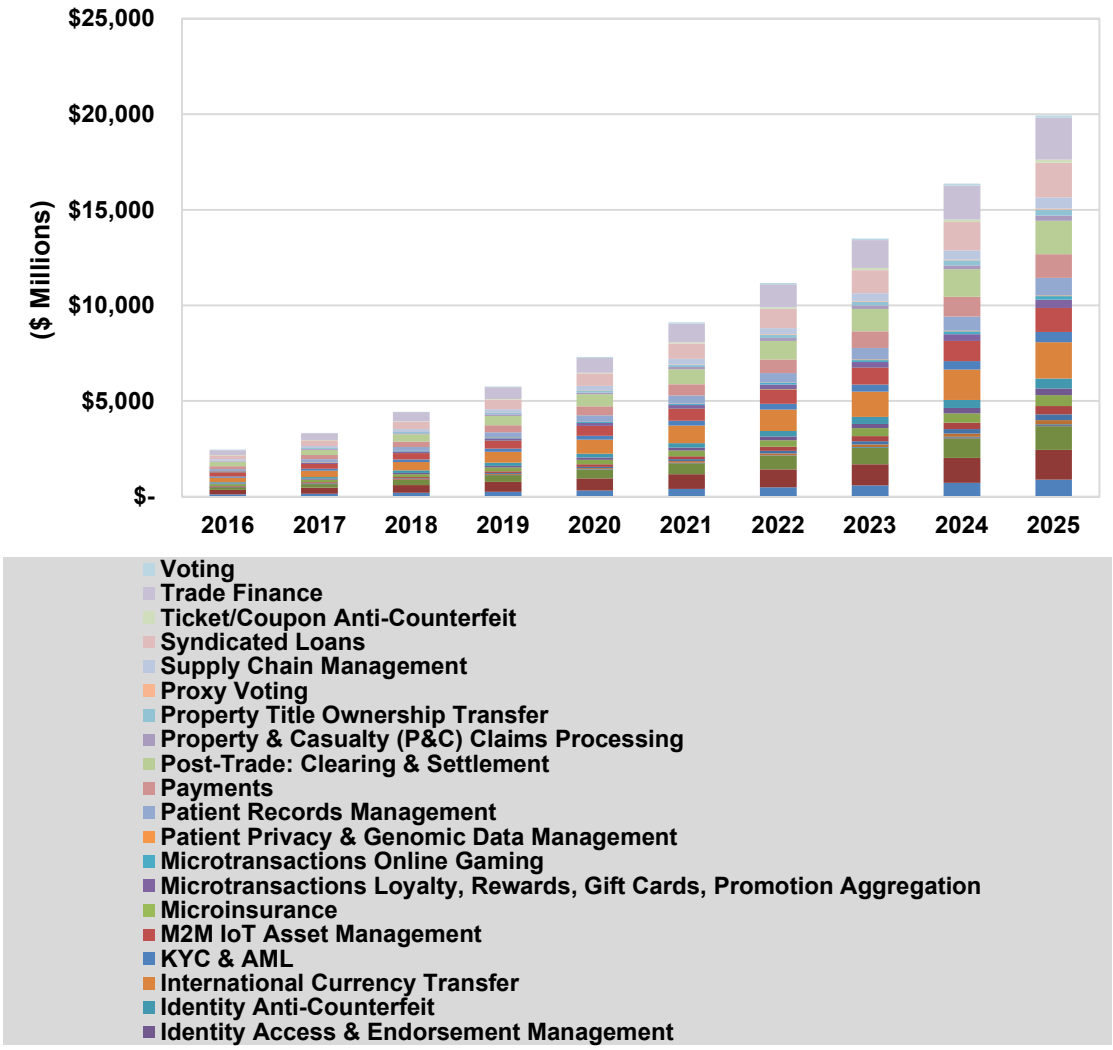
Tractica's research finds blockchain technology may be applicable across a wide range of industries, thus enabling a long list of potential use cases. Distributed database transaction verification technology is inherent to business by nature, and thus applies to most companies conducting transactions at scale. Given current investments and activities underway at the time of this report's publication, Tractica anticipates the bulk of revenue associated with blockchain deployment will be realized in financial services use cases, such as applications supporting trade, finance, international currency transfer, payments, syndicated loans, post-trade clearing & settlement, and other compliance-related use cases. Beyond financial services, Tractica anticipates significant revenue opportunity in use cases associated with asset management, supply chain and provenance tracking, as well as IoT and, eventually, identity authentication and verification.

Chart 6.5 Blockchain Cumulative Revenue by Use Case, World Markets: 2016-2025



(Source: Tractica)

Chart 6.6 Blockchain Revenue by Use Case, World Markets: 2016-2025



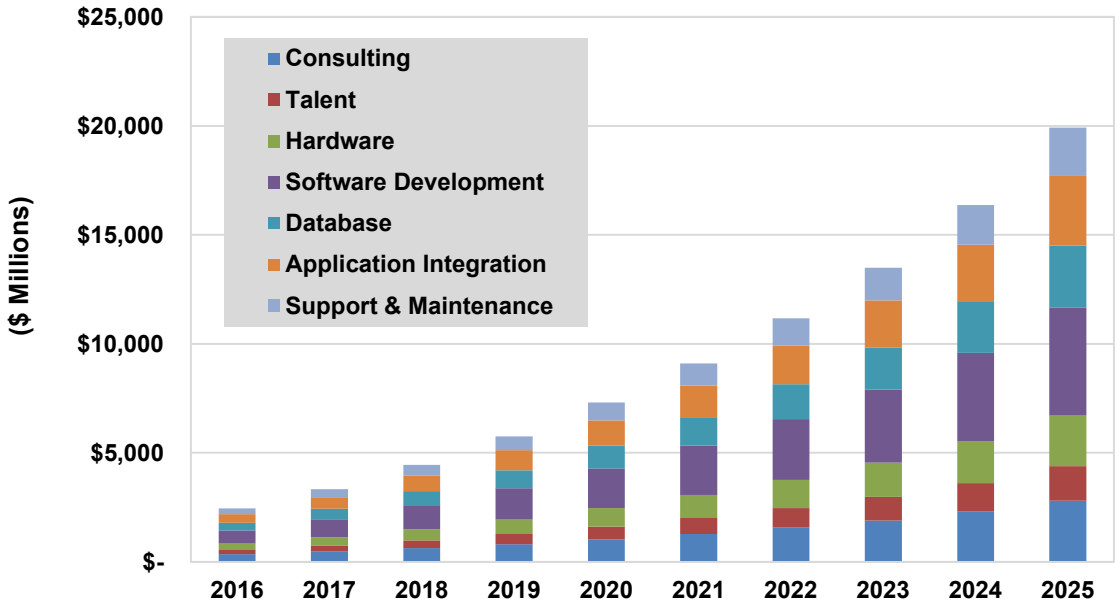
(Source: Tractica)

6.5 BLOCKCHAIN REVENUE BY IMPLEMENTATION CATEGORY

Blockchain technology implementations are far from one-size-fits-all, and vary in nature widely across industries and use cases, and from proprietary "home-grown" pilots to more vendor-enabled "off-the-shelf" experimentations combining pre-configured modules with custom programming. As with many emerging technologies, adopters often find themselves investing in the consulting and guidance needed to "get off the ground," both in educating stakeholders on the value, as well as in scoping priority use cases. It is important to note that at the time of this report's publication, there are very few (if any) at-scale, in-production blockchain deployments running. Nonetheless, Tractica's research finds that costs will vary significantly depending on the extent of internal versus external build, as well as customizations and regulatory requirements reflected in the architecture. Investment allocations into software, hardware, database development, and support will also vary based on integration requirements with existing infrastructure, the number of counterparties

involved, and the scale of hardware associated with transaction execution. As a "single" blockchain-based deployment may involve numerous counterparties, investments may also be divided up across numerous institutions.

Chart 6.7 Blockchain Revenue by Implementation Category, World Markets: 2016-2025



(Source: Tractica)

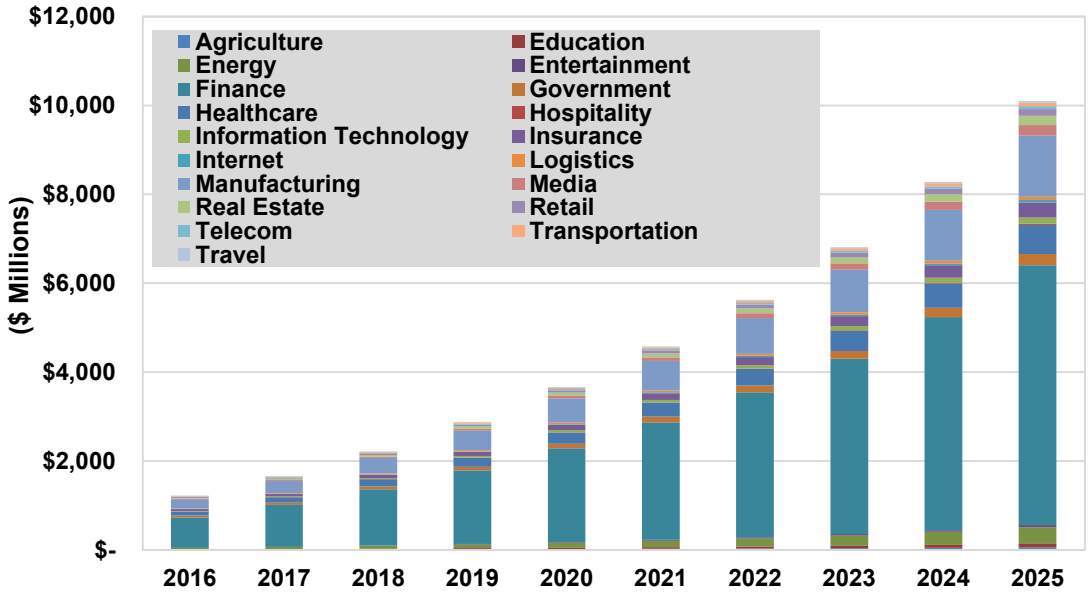
6.6 BLOCKCHAIN REVENUE BY REGION

6.6.1 NORTH AMERICA

Since the inception of Bitcoin, North America has been driving much of the activity in cryptocurrency, and increasingly, in the enterprise blockchain market. Although Europe and Asia are gaining traction in blockchain efforts, the United States has led the supplier side of the market in technology enterprises, startups, VCs, accelerators, and so on. In addition, a great majority of North America's largest banks have either partnered with enterprise blockchain consortia, many of which were founded in the United States, or invested themselves in blockchain development, talent acquisition, and consulting services. Beyond financial services, Tractica forecasts that blockchain technology adoption in North America will grow significantly in a handful of the continent's other economically critical industries, namely manufacturing, healthcare, and agriculture. Like other regions, Canada and particularly the United States are subject to shifting regulatory regimes, which could influence adoption incentives (or disincentives) in unforeseen ways.

Tractica forecasts that annual revenue for enterprise blockchain applications in North America will increase from $1.2 billion worldwide in 2016 to $10.1 billion in 2025.

Chart 6.8 Blockchain Revenue by Industry, North America: 2016-2025



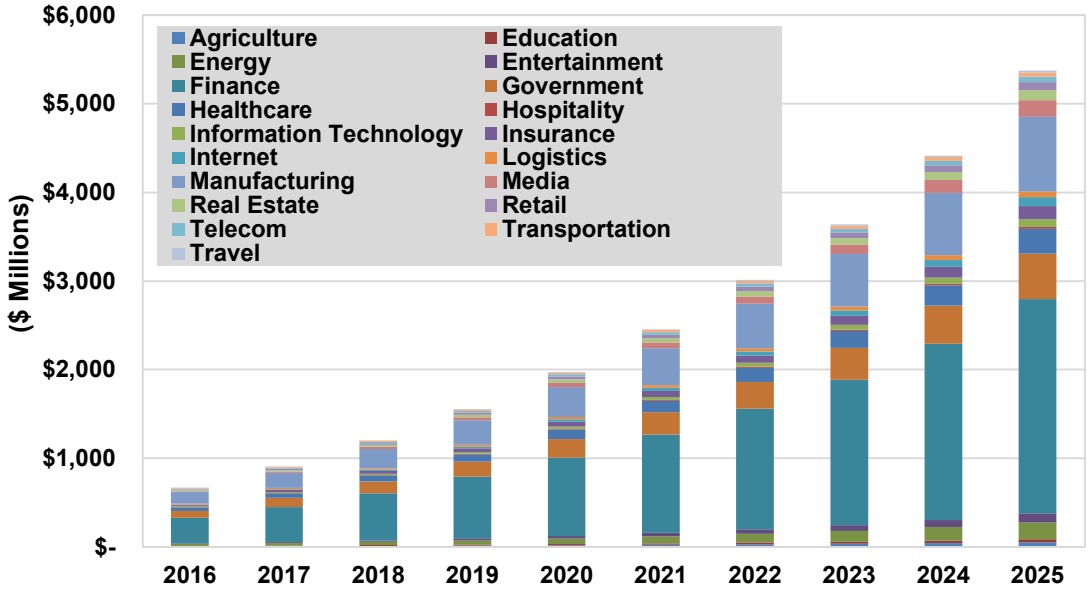
(Source: Tractica)

6.6.2 EUROPE

Europe's role in blockchain development is growing rapidly. Next to China, the volume and range of institutions in Europe are hardly matched the world over. Britain, Germany, France, Spain, and even Estonia are each home to numerous blockchain technology providers, consulting efforts, regulatory studies, and notable pilot programs. Given Europe's current investment in green energy, Tractica expects use cases involving P2P or device-to-device energy distribution and transmission will likely enjoy the greatest adoption relative to other world regions. Shifting energy economies onto blockchain technology would also potentially create demand in adjacent industries such as transportation (autonomous cars, for example), manufacturing, and telecom.

Tractica forecasts that annual revenue for enterprise blockchain applications in Europe will increase from $669.1 million worldwide in 2016 to $5.4 billion in 2025.

Chart 6.9 Blockchain Revenue by Industry, Europe: 2016-2025



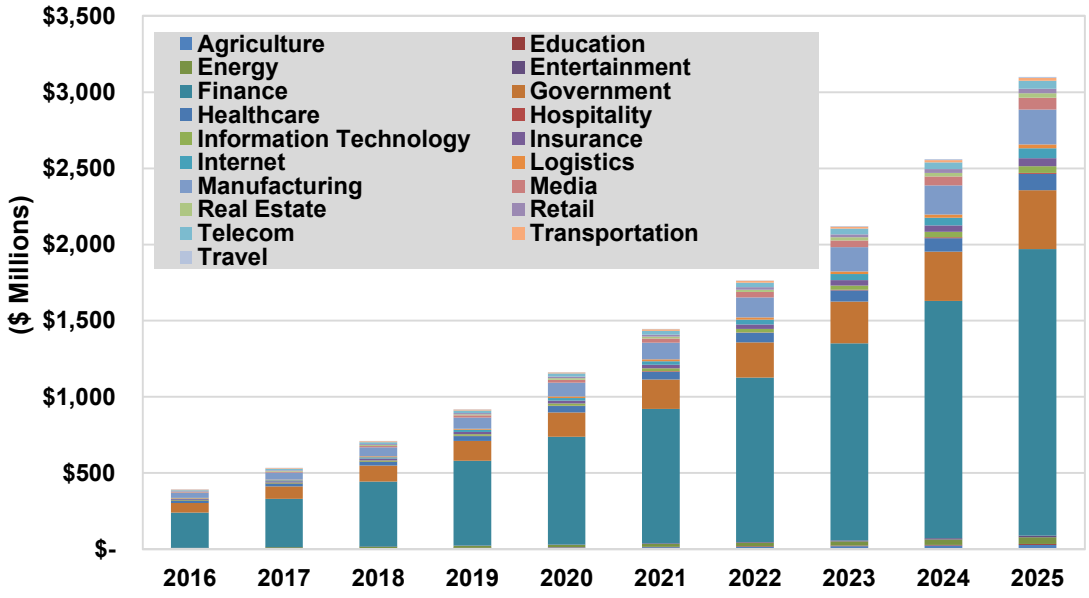
(Source: Tractica)

6.6.3 ASIA PACIFIC

Blockchain adoption is growing rapidly in Asia Pacific, with the bulk of deployments happening in China and Australia, and countless activities brewing in Japan, Singapore, Taiwan, India, and elsewhere. In particular, China's robust economies in finance, manufacturing, and online gaming, in addition to its relatively consolidated political structure, render blockchain financially and strategically attractive. Efforts across Australia and New Zealand point to fewer government and regulatory restrictions, at least when it comes to conducting pilots; both countries are conducting ongoing POCs in agriculture, supply chain, and trade finance. Asia Pacific is, of course, extremely diverse in geography, politics, economics, and beyond, and it is likely that highly fragmented adoption will be sustained far beyond 2025.

Tractica forecasts that annual revenue for enterprise blockchain applications in Asia Pacific will increase from $392.1 million worldwide in 2016 to $3.1 billion in 2025.

Chart 6.10 Blockchain Revenue by Industry, Asia Pacific: 2016-2025



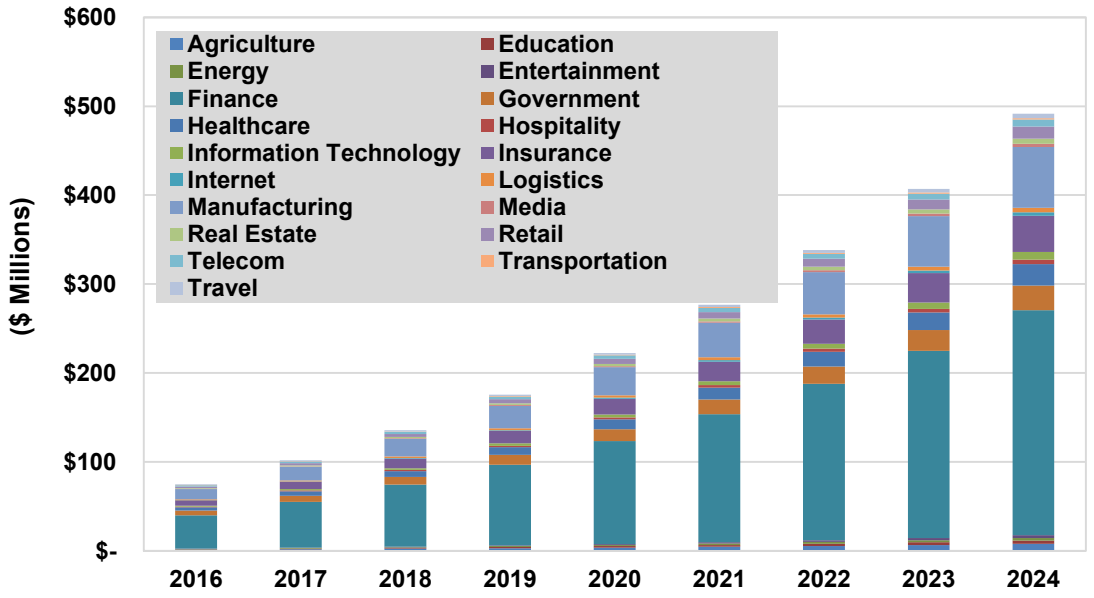
(Source: Tractica)

6.6.4 LATIN AMERICA

Most countries in Latin America, including South America, are embracing blockchain technology at a relatively slower pace than other regions. Mexico and Brazil have shown some interest, particularly around international payments and microinsurance. Honduras expressed interest in a government services-related blockchain application in its partnership with Factom, but the project was stalled due to political tensions. The combination of economic and political tensions, plus a huge and diverse set of countries, as is the case in Latin and South America, will challenge its adoption. But, in certain areas, like international payments and microinsurance, less developed regions may leapfrog over more mature markets.

Tractica forecasts that annual revenue for enterprise blockchain applications in Latin America will increase from $74.8 million worldwide in 2016 to $596 million in 2025.

Chart 6.11 Blockchain Revenue by Industry, Latin America: 2016-2025



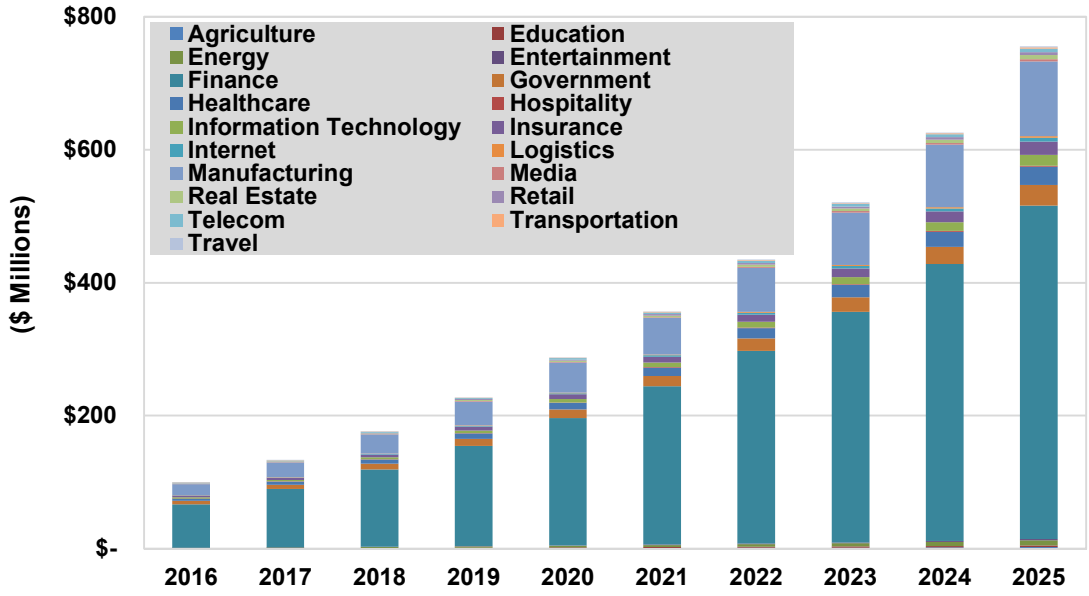
(Source: Tractica)

6.6.5 MIDDLE EAST & AFRICA

Blockchain applications across Africa remain few, although there are a handful of crypto-currency and payment-related startups. In the Middle East, activity is picking up, particularly in the financial sector. Dubai's du Telecom recently announced the formulation of a working group to address the blockchain opportunity around healthcare, government, regulation, and finance. Extreme diversity in political, economic, and business conditions will likely hinder rapid blockchain adoption, although less developed regions sometimes leapfrog more mature markets, as Africa did with mobile commerce.

Tractica forecasts that annual revenue for enterprise blockchain applications in the Middle East & Africa will increase from $99.7 million worldwide in 2016 to $755.5 million in 2025.

Chart 6.12 Blockchain Revenue by Industry, Middle East & Africa: 2016-2025



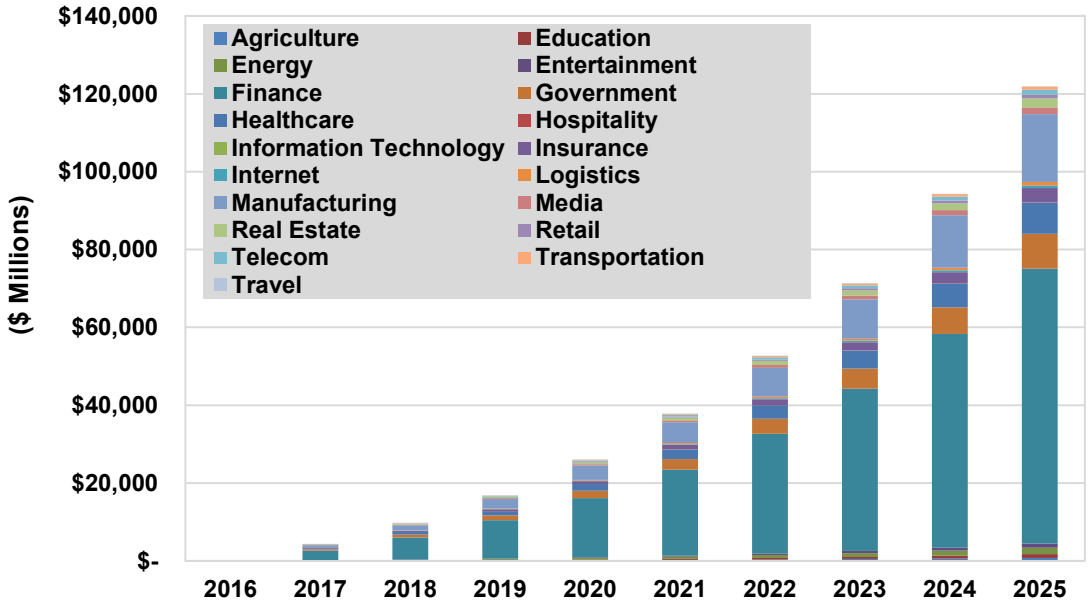
(Source: Tractica)

6.7 BLOCKCHAIN'S COST SAVINGS AND SERVICE REVENUE

Blockchain technology is fundamentally about using code to handle intermediation and secure transaction processing. It is typically understood as a means of cost savings. The types of cost savings vary widely based on the industries, use cases, regulatory environments, number of counterparties, and system integration requirements involved. Tractica's research finds that certain industries, such as finance and healthcare could potentially trim significant sums from the current ways of doing things. For example, in post-trade processing and settlement, entire industries exist worldwide for the sole purpose of verifying documents, credit, identities, shipments, etc.; these processes are largely conducted manually, which can take anywhere from a few days to 3 weeks to complete. "Digitizing" parts (or all) of these reconciliation workflows has the potential to reduce costs associated with headcount, time, technology, data integrity, fraud/counterfeit, security, regulatory non-compliance, etc. The decentralized nature of this technology also means that its cost-saving impacts potentially compound as more counterparties participate in the network.

Although the vast majority of enterprise blockchain deployments today are mere POCs (and not running at-scale or at high-volume), it is not difficult to extrapolate how such an architecture could enable numerous simultaneous efficiencies. Tractica expects financial services-related use cases to hold the greatest cost-savings potential in terms of volume of cost savings, but industries such as healthcare, logistics, and energy hold longer-term potential. Reference Section 2.2.5 for a deeper assessment of potential cost savings.

Chart 6.13 Blockchain Cost Savings by Industry, World Markets: 2016-2025



(Source: Tractica)

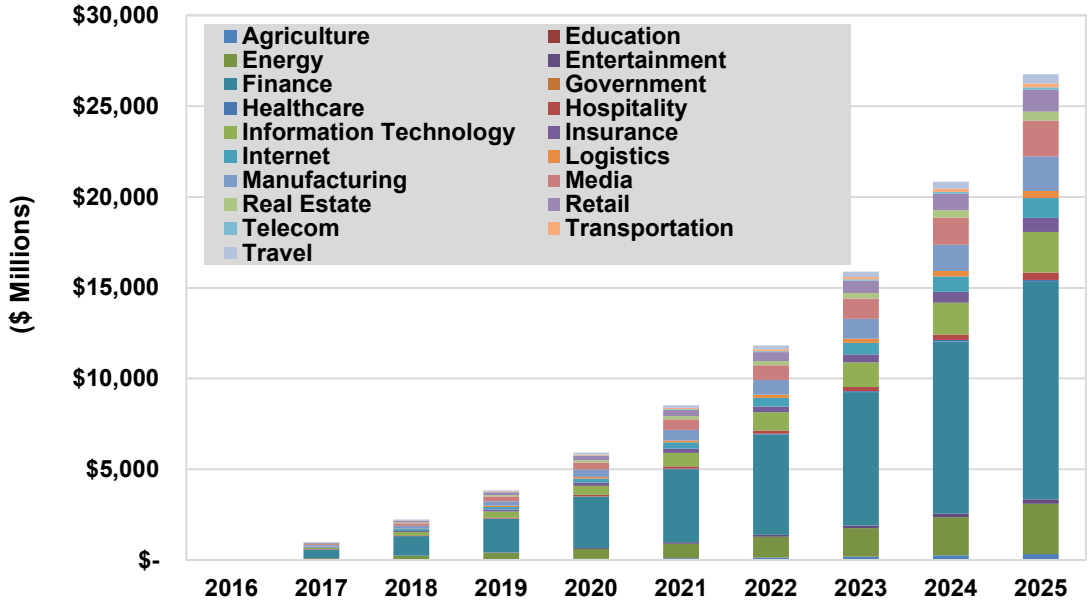
Meanwhile, many institutions are asking if blockchain-based services will generate altogether new revenue. While cost savings may be the more obvious benefits of blockchain technology, Tractica research finds incremental and net new revenue could emerge as blockchain makes possible the following innovations:

- New modes of interactions and transactions (e.g., companies have visibility into processes previously blind to them; devices negotiate for themselves; P2P transactions may be leveraged while maintaining security/privacy)
- New modes work in conjunction with other emerging technology trends (e.g., shared economy, AI, IoT, autonomous vehicles, 3D printing, etc.)
- Third-party services (e.g., payment, microinsurance) using blockchain
- Increased liquidity enabled through the automation of transactions and reduction of latency can be used to support new business models

For example, if a network of companies uses a distributed architecture to monitor, negotiate, distribute, track, and generally manage the provenance of products, visibility into these previously fragmented or invisible steps of the supply chain could open up new means of providing value to each other or to end customers. Contextual data sourced along the chain

could become an asset supporting new revenue streams by securely procuring and selling insights around soil, livestock, weather, traffic, retail, recycling, and beyond.

Chart 6.14 Blockchain-Based Services Revenue by Industry, World Markets: 2016-2025



(Source: Tractica)

SECTION 7
KEY FINDINGS, RECOMMENDATIONS, AND CONCLUSIONS

7.1 KEY FINDINGS

1. **Amid the fog of hype lies a nascent market:** While the blockchain market has generated massive interest and investment from just about every type of institution, the market remains extremely nascent, with very few deployments in production outside of Bitcoin.

2. **Bitcoin is the tip of the blockchain iceberg:** The potential for blockchain technology is far greater than Bitcoin, yet both cryptocurrency and blockchain suffer reputational hurdles to enterprise acceptance.

3. **Tractica identified more than 30 distinct use cases categories:** Beyond Bitcoin and other currency-centric use cases, blockchain could be a promising architecture solution for institutional transformations in identity management, asset management, and compliance automation, among others.

4. **Blockchain will redefine competitive structures:** Blockchain has the potential to disrupt numerous market structures in which transactions currently require numerous stakeholders and intermediaries, and in which trust is limited or lacking.

5. **Blockchain technology is not a panacea or a solution to all IT inefficiency:** Rather, businesses should view this technology as a series of technological modules and concepts that may be selectively chosen and applied, and/or will complement other emerging technology trends.

6. **The autonomous world requires trust, accountability, and efficiency:** With rigorous proofing and collaborative development, blockchain has long-term potential to be a "missing link" to the secure convergence of emerging technology trends, such as connected and autonomous devices, networked services, cybersecurity, and potentially even AI, among others.

7.2 RECOMMENDATIONS

Blockchain has been coined as the OS for global markets. Will blockchain become for government, banking, law, trade, healthcare, and logistics what the Internet has enabled for media and commerce? As businesses transform digitally, they must consider where to act on the blockchain opportunity. Identifying strategic paths benefits from observing the following parallel disruptive characteristics blockchain has to the Internet.

- Decentralized structure facilitates interaction from new participants
- Disintermediates existing institutions/markets
- Reduces friction for most participants
- Significant cost reductions as a result
- Architecture at the platform level within the stack; supports a range of vertical apps
- Opportunity for new business model creation

Furthermore, blockchain applications will enjoy the augmentation of other advancing technology markets, namely the IoT, AI, advancements in cybersecurity, connectivity, and processing efficiencies, most of which will take form prior to widespread blockchain adoption.

For these reasons, Tractica recommends that almost every business invest in the time, talent, and strategy to understand blockchain technology, and engage with other industry participants to do so. In certain sectors, such as financial, government, logistics, and those within the collaborative economy, blockchain experimentation will become ubiquitous with certain applications gaining unprecedented traction in the next 18 to 24 months. Chief information officers (CIOs) and strategists should be actively pursuing multi-disciplinary collaboration and experimentation with innovators, incumbents, and regulators to explore the economic benefits of blockchain, as well as the risks, lessons learned, and unintended consequences.

Tractica anticipates adoption will move very slowly over the next 2 to 5 years, with limited market adoption in 5 to 7 years, and significant uptick occurring in approximately 7 to 10 years. Blockchain will not replace existing structures and infrastructure overnight; rather, it will evolve alongside incumbent systems, existing standards, complementing, then supporting, and then making certain workflows irrelevant. Technology providers must prioritize integration and interoperability in any platform or application development, particularly so as to not neutralize security protections.

It is critically important to future governance of our society to observe how, when, and why we apply new technology. The gravity of blockchain's potential presents an imperative for research, infrastructural development, testing, and discourse, among other areas. By engaging with the blockchain market today, governments, enterprises, consortia, universities, and even citizens have a role in defining its potential for tomorrow.

7.3 CONCLUSIONS

Can protocol-based trust improve or *even replace* the trust between people, organizations, governments, and devices? Will blockchain serve as the infrastructure for a fully connected autonomous world? Could this technology actually empower millions or billions of individuals to preserve their rights and exercise control over their digital identities?

Blockchain's potential to generate significant value across counterparties depends on the "network effect" and this dynamic could either thwart momentum or accelerate adoption quickly, especially in financial services applications. Viewed through today's lens, one finds it difficult to avoid the conclusion that, while decentralized architectures are technically possible and have truly profound promise, full implementation and adoption cannot and will not come to pass without massive shifts in economic and, in some cases, societal models. The Information Age has already transformed the world, but perhaps we are just getting started.

SECTION 8
COMPANY DIRECTORY

21.co
436 Bryant Street
San Francisco, CA 94107, USA
https://21.co/
+1.415.580.2136

Abra
958 California Street
Mountain View, CA 94041, USA
www.goabra.com

Ascribe.io
Wichertstraße 14A, 10439
Berlin, Germany
www.ascrib.io
+49.30.6482.6092

Blockchain "Blockchain Luxembourg S.A."
www.blockchain.com
+85223575452

BitX
31 Loop St. Cape Town City
Cape Town, 8000, South Africa
www.bitx.co

Blockchain Health Co
2415 Mission Street
San Francisco, CA 94110, USA
https://blockchainhealth.co
+1.650.924.2785

Blockchain Technologies Corporation (BTC)
157 Prince Street
New York, NY 10012, USA
https://blockchaintechcorp.com
+1.917.515.5355

Blockstream
1000 de La Gauchetiere Street West, Suite 2100
Montreal, QC H3B 4W5, Canada
www.blockstream.com

Circle
Dublin, Ireland
https://www.circle.com
+1.617.326.8326

Coinbase
548 Market Street, #23008
San Francisco, CA 94104, USA
www.coinbase.com
+1.800.343.5845

CoinDesk
1460 Broadway, 4th Floor
New York, NY 10036, USA
www.coindesk.com

ConsenSys
49 Wyckoff Avenue
Brooklyn, NY 11201, USA
https://consensys.net
+1.646.598.NERD

Deutsche Bank
Taunusanlage 12
Frankfurt am Main, Hessen 60325, Germany
www.db.com
+1.212.250.2500

Digital Asset Holdings (DAH)
162 5th Avenue, Suite 902
New York, NY 10010, USA
www.digitalasset.com

Ethereum
www.ethereum.org/

Filament
100 N Arlington Avenue, Suite 105
Reno, NE 89501, USA
www.filament.com
+1.775.434.0095

Gem
120 Mildred Avenue
Venice, CA 90291, USA
https://gem.co
+1.323.487.2487

The Hyperledger Project
www.hyperledger.org

HSBC
8 Canada Square
London, E14 5HQ, UK
www.hsbc.com
+1.800.975.4722

IBM
1 New Orchard Road
Armonk, NY 10504, USA
www.ibm.com
+1.914.499.1900

Innogy (Formally RWE)
Opernplatz
45128 Essen, Germany
www.innogy.com
+49.201.12.02

International Blockchain Real Estate Association (IBREA)
www.ibtcrea.org

Loyyal
43 W. 23rd Street, 6F
New York, NY 10010, USA
www.loyyal.com

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052, USA
www.microsoft.com
+1.425.882.8080

NASDAQ
One Liberty Plaza, 165 Broadway
New York, NY 10006, USA
www.nasdaq.com
+1.212.401.8700

Overstock.com
799 West Coliseum Way
Midvale, UT 84047, USA
www.overstock.com
+1.801.947.3100

Royal Philips
Amstelplein 2 Philips Center, P.O. Box 77900
1070 MX Amsterdam, Netherlands
www.philips.com
+31.20.59.77777

PayPal
2211 North First Street
San Jose, CA 95131, USA
www.paypal.com
+1.888.221.1161

Project Provenance
c/o Softwire, Unit #110, Highgate Studios, 53-79 Highgate Road
London, NW51TL, UK
www.provenance.org

R3
1370 Broadway, Suite 1050
New York, NY 10018, USA
https://r3cev.com

Ripple
300 Montgomery Street, 12th Floor
San Francisco, CA 94104, USA
www.ripple.com

Slock.it
Mittweida, GE
https://slock.it

Smart Contract
665 3rd Street, Suite #150
San Francisco, CA 94103, USA
smartcontract.com

Santander
Avenida de Cantabria S/N Boadilla del Monte
Madrid 28660, Spain
www.santander.com
+1.877.768.2265

SolarCoin
www.solarcoin.org

Visa
900 Metro Center Boulevard
Foster City, CA 94404, USA
www.visa.com
+1.640.432.3200

Xapo
Zurich, Switzerland
hwww.xapo.co

SECTION 9

GLOSSARY

Term	Description
Address (a.k.a. cryptocurrency addresses)	Addresses are strings of alphanumerical codes (or QR codes) used to send and receive transactions on the network.
Alternative chains (a.k.a. altchains)	Altchains are blockchain designs based on bitcoin concepts and code that add additional functionality (e.g., performance, anonymity, smart contracts, storage, etc.) to the underlying blockchain or main chain.
Anti-Money Laundering (AML)	This regulation is about understanding patterns of money flow at the transaction level to prevent crime, including facilitating movement of money in support of illegal activity, terrorism, or transfer from so-called "immoral origins."
Asset	Anything that can be owned or controlled to produce value is an asset. Assets can be both tangible (such as a house or car) and intangible (such as a mortgage or lease).
Bitcoin	Created in 2009, bitcoin is a type of digital-only (non-physical) currency that operates independently from governments or centralized banks, and rather by a decentralized authority and encrypted techniques to verify the transfer of funds and regulate the generation of units of currency.
Blockchain	A blockchain is a shared, immutable ledger of transactions. A block is the "current" part of a blockchain that records some or all of the recent transactions, and once completed, goes into the blockchain as a permanent database. Blocks are linked to each other (like a chain) in proper linear, chronological order with every block containing a hash of the previous block.
Blocks	The building blocks; or bundles of valid transactions that combine together with a digital signature and a link to the block before it. A block is a file containing the immutable store of records that, once transacted, cannot be altered or removed. It thus represents the "present truth" on which value transfer is based on the blockchain. When a transaction occurs, it is validated and stored on a block, which is then "complete," and then used to validate the next block in the blockchain.
Cryptocurrency	A cryptocurrency is a digital or virtual currency that uses cryptography for security and is not issued by any central authority, which theoretically prevents government interference or manipulation.
Cryptographic Hashes (a.k.a. Hash Value)	Cryptographic hashes, such as the SHA256 computational algorithm, produce a fixed-size, unique hash value, known as a digest, from variable-sized transaction input. Hashes feature a mathematical property in which a hash can be arrived at uniquely from a given input, but the input cannot be derived from its hash value. A given specific input always results in the same hash value being computed. Any modifications or alterations to transaction input—even the most minuscule change—results in a different hash value being computed, which indicates potentially compromised transaction input. Thus, the hash value can be used to detect the integrity of the transaction input.

Term	Description
Cryptographic Signatures	Cryptographic signatures determine which transactions are valid. Signatures are generated from a hash of data to be signed, and a private key. Digital signatures ensure that the receiver receives the transactions without middle parties modifying or forging the contents of transactions, while also ensuring that the transactions originated from senders (signed with private keys) and not imposters.
Encryption	Encryption refers to the operation of disguising and concealing plaintext information through a set of rules called the encryption algorithm. The operation of an algorithm depends on the encryption key, or an input to the algorithm with the message. For a user to obtain a message from the output of an algorithm, there must be a decryption algorithm that, when used with a decryption key, reproduces the plaintext.
Hard Fork	A hard fork is a radical divergence from the original blockchain protocol, rendering previously valid blocks/transactions invalid (or vice versa). It requires that all nodes or users upgrade to the latest version of the protocol software in order to add new functionality, correct security flaws, or, as in the case of the recent DAO hack, reverse or relocate transactions by creating new smart contracts.
Hash	A hash is an identifier of data (e.g., blocks, transactions, and addresses) in a transaction. On the blockchain, transactions are referred to by their hash, not the details of the transaction itself. Transactions occurring on the blockchain are stored as hashes because hashes are more lightweight than the full detail of the transaction.
Hash Functions	Hash functions take an alphanumeric input, perform some computations, and spit out another alphanumeric value of a predetermined length. A given input has a predictable output of a specified length, usually, but not necessarily much shorter than the input. Hash functions are important to the mathematical integrity of blockchain architectures because if the input is only slightly changed, the output differs dramatically. Inversely, it is very difficult, if not practically impossible, to infer the original input, given only the output if the hash functions cryptographically.
Hash rates	Hash rate is the measuring unit of processing power to complete operation in blockchain code. Specifically, it measures the number of times a hash function can be computed per second.
Hashing	One way of reducing data that creates links to previous blocks so that it is impossible to modify transactions in historical sets of transaction data.
Know Your Customer (KYC)	KYC is a process and regulation in financial services markets wherein the institution (bank) must verify with whom they are providing services. This applies to both individual/consumer customers and to business customers (sometimes known in this circumstance as Know Your Business (KYB)). Typical information required to verify individuals include proof of identification, personal information, proof of income and/or equity, potential business interests, and sometimes a background check; and, for companies, business structure, leadership, shareholders, revenue, and business models. Given centralized relationships, banks are not able to trust verification from another entity and streamline their own verification process, thus costs and friction ensue with each customer acquisition.

Term	Description
Main Chains	The original chain is normally referred to as the “main chain.” Other blockchains and sidechains may extend the functionality of the main chain.
Miners	The nodes or groups of nodes that compete to achieve computational verification and broadcast the result across the network.
Mining	The process in which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies as miners are incentivized by earning rewards in cryptocurrency.
Multi-Signature Transactions (a.k.a. multisigs)	Multi-signature addresses require multiple parties and thus more than one key to authorize a transaction. The terms and number of signatures are designed during the creation of the addresses.
Nodes	Devices attached to a distributed network.
Oracle	One or more trusted parties, contracts, or code required to create transaction embedding data into the chain. Whereas smart contracts pull data from the blockchain, oracles push data onto the blockchain.
Participant	Any actor that can access the ledger, read records, and add new records.
Permissions	Ability to access any aspect of or visibility into a record or transaction.
Private Blockchain	Public blockchains allow for distributed identical copies of a ledger, but only to a limited number of trusted participants only.
Private Key	A private key might be thought of as a unique password; it is a string of unique data allowing a single individual to access and spend their tokens through a cryptographic signature.
Proof-of-Activity	A dual approach in which each block is a product of combined proof-of work and proof-of-stake mining.
Proof-of-Stake	Rather than requiring the prover to perform a certain amount of computational work (proof-of-work), a proof-of-stake system requires the prover to show ownership (“stake”) of a certain amount of money. Proof-of-stake is commonly used in private or hybrid blockchain development to mitigate bandwidth, storage, and energy costs
Proof-of-Work	A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof-of-work. Proof-of-work is a number, called a nonce, which when combined with other data and hashed, produces a value smaller than a specified target.
Public Blockchain (a.k.a. Permissionless Ledgers)	Public blockchains allow anyone to contribute data to the ledger with all participants possessing an identical copy of the ledger.
Public Key	Part of a cryptographic system used to control encryption and decryption of records. A public key is known to everyone; public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.
Sidechains	Sidechains are mechanisms that make it possible to move cryptocurrency bidirectionally, from the main chain to the sidechain and then back to the

Term	Description
	original main chain securely and efficiently. They are decentralized, P2P networks that run in parallel and extend functionality and interoperability from the main chain to transfer or synchronize tokens between public to private to public networks.
Smart Contract	Smart contracts are custom-developed, self-executing programs/applications that run on a blockchain and are triggered by some external data or event that instructs them to modify some other data, thereby enacting, executing, and enforcing the validity of a transaction.
Tokens	Tokens are cryptocurrency, a type of digital asset that works by cryptographically secured transactions and creations of new units. There are two types of tokens: intrinsic/built-in tokens and asset-backed tokens. Intrinsic tokens are made-up resources that have some utility. Common examples include: BTC on the Bitcoin blockchain, XRP on the Ripple network, NXT on the NXT platform, ETH on Ethereum, LSK on Lisk. Asset-backed tokens are claims on an underlying asset, from a specific issuer. Popular assets for these schemes are currency (US$, EUR, etc.) and precious metals, as well as other assets, such as diamonds, art, music, etc.
Transaction	A transaction is an asset transfer onto, within, or off of the ledger.

SECTION 10
ACRONYM AND ABBREVIATION LIST

Anti-Money Laundering (Regulation) ..... AML

Artificial Intelligence ..... AI

Application Program Interface ..... API

Autonomous Decentralized Peer-to-Peer Telemetry ..... ADEPT

Automated Teller Machine ..... ATM

Bitcoin (Bitcoin currency metric) ..... BTC

Blockchain-as-a-Service ..... BaaS

Brent, Forties, Ekofisk, and Oseberg ..... BFOE

Central Counterparty ..... CCP

Central Processing Unit ..... CPU

Chief Information Officer ..... CIO

Compound Annual Growth Rate ..... CAGR

Cost-per-Click ..... CPC

Cost-per-Impression ..... CPM

Customer Due Diligence ..... CDD

Customer Relationship Management ..... CRM

Customer-to-Customer C2C

Digital Asset Transfer Authority ..... DATA

Decentralized Applications ..... Dapps

Decentralized Autonomous Company ..... DAC

Decentralized Autonomous Organization ..... DAO

Distributed Concurrence Ledger ..... DCL

Distributed Ledger Technology ..... DLT

Evaluation Assurance Levels ..... EAL

Electronic Medical Records ..... EMR

Electronic Settlement Platform ..... ESP

Enterprise Resource Planning ..... ERP

Ether (Ethereum-based currency metric) ..... ETH

European Union ..... EU

Ethereum Virtual Machine ..... EVM

Federal Information Processing Standards ..... FIPS

Foreign Account Tax Compliance Act ..... FATCA

Foreign Exchange ..... FX

Genetically Modified Organism ..... GMO

Global Data Protection Regulation ..... GDPR

Global Positioning System ..... GPS

Graphics Performance Analyzers ..... GPA

Graphics Processing Unit ..... GPU

Gross Domestic Product ..... GDP

Health Information Technology for Economic & Clinical Health ..... HITECH

Health Insurance Portability & Accountability Act ..... HIPAA

Hypertext Transfer Protocol ..... HTTP

Identification ..... ID

International Chamber of Commerce ICC

Information Technology ..... IT

Initial Coin Offering ..... ICO

Initial Public Offering ..... IPO

Intellectual Property ..... IP

International Standards Organization ..... ISO

Internet of Things ..... IoT

Know Your Business ..... KYB

Know Your Customer (Regulation) ..... KYC

Low-Power Wide Area (Networks) ..... LPWA

Machine-to-Machine M2M

Massachusetts Institute of Technology ..... MIT

Minimum Viable Project ..... MVP

Multi-Party Computation ..... MPC

New York Department of Financial Services ..... NYDFS

National Settlement Depository ..... NSD

Operating System ..... OS

Original Equipment Manufacturer ..... OEM

Over-the-Counter ..... OTC

Peer-to-Peer P2P

Personal Identification Number ..... PIN

Property and Casualty ..... P&C

Proof-of-Concept ..... POC

Quick Response ..... QR

Radio Frequency Identification ..... RFID

Search Engine Optimization ..... SEO

Securities and Exchange Commission ..... SEC

Settlement Date Coordination ..... SDC

Society for Worldwide Interbank Financial Telecommunications ..... SWIFT

System of Record ..... SoR

United Arab Emirates ..... UAE

User Experience ..... UX

Venture Capital VC

Virtual Power Plant ..... VPP

Zero-Knowledge Proof ..... ZKP

SECTION 11

TABLE OF CONTENTS

SECTION 12
TABLE OF CHARTS AND FIGURES

SECTION 13
SCOPE OF STUDY

This report examines the enterprise opportunity for blockchain. The report is distinct in its identification, description, and categorization of more than 30 unique use cases wherein blockchain technologies may be applied across a wide range of industries. In the Market Issues and Technology Issues sections, Tractica explores the most important drivers, barriers, and constituencies influencing blockchain market development. Tractica identifies the core characteristics of blockchain architecture in public (permissionless), private (permissioned), as well as hybrid configurations. In addressing technology issues surrounding the blockchain market, Tractica identifies distinct modules of blockchain configurations, including transaction distribution, consensus, rules of validity & linkage, immutability, identity authentication & private keys, supervisory or regulatory nodes, anti-double spend, and built-in assets or smart contracts. Most of the market and technology issues addressed in this report apply to enterprise and/or government and institutional applications. Although mentioned, purely citizen-to-citizen/P2P blockchain applications are beyond the scope of this report.

The nascence of this market cannot be understated. To the best of its abilities, Tractica's assessment of the blockchain market seeks to convey both immaturity and limitations in market definition, consensus, and activity, while thoroughly illustrating its radical and disruptive potential. One of the challenges of developing a forecast in a market as ephemeral, yet innovative as blockchain is the allowance for unforeseen emerging technologies and/or geopolitical forces that could play a significant role during the forecast period (2016 to 2025) covered in this study.

Within that scope, this report considers the potential for blockchain applications across 19 industries and more than 30 unique use case categories. The report also assesses both qualitatively and quantitatively the investment/implementation categories, cost-savings versus new services revenue, and overarching business model implications of distributed ledger technologies. The accompanying Excel databook forecasts revenue for blockchain applications across world regions, industries, use cases, implementation categories, and business model impacts during the period from 2016 through 2025.

SOURCES AND METHODOLOGY

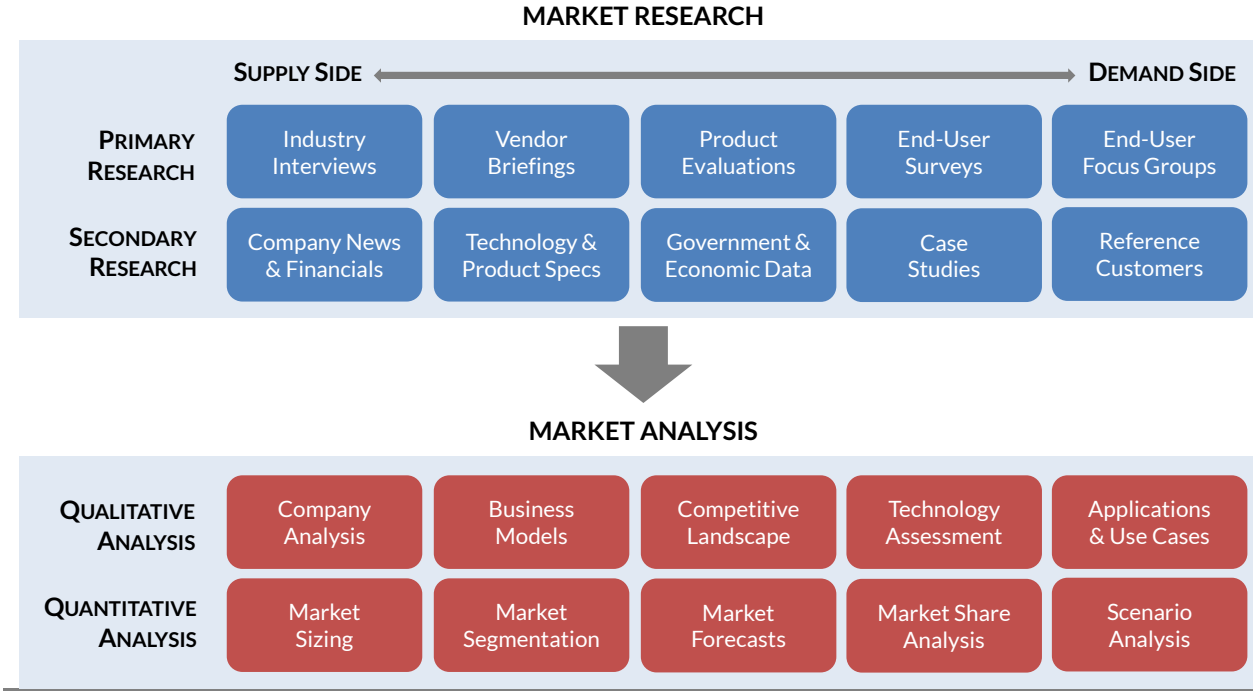
Tractica is an independent market research firm that provides industry participants and stakeholders with an objective, unbiased view of market dynamics and business opportunities within its coverage areas. The firm's industry analysts are dedicated to presenting clear and actionable analysis to support business planning initiatives and go-to-market strategies, utilizing rigorous market research methodologies and without regard for technology hype or special interests including Tractica's own client relationships. Within its market analysis, Tractica strives to offer conclusions and recommendations that reflect the most likely path of industry development, even when those views may be contrarian.

The basis of Tractica's analysis is primary research collected from a variety of sources including industry interviews, vendor briefings, product demonstrations, and quantitative and qualitative market research focused on consumer and business end-users. Industry analysts conduct interviews with representative groups of executives, technology practitioners, sales and marketing professionals, industry association personnel, government representatives, investors, consultants, and other industry stakeholders. Analysts are diligent in pursuing interviews with representatives from every part of the value chain in an effort to gain a comprehensive view of current market activity and future plans. Within the firm's surveys and focus groups, respondent samples are carefully selected to ensure that they provide the most accurate possible view of demand dynamics within consumer and business markets, utilizing balanced and representative samples where appropriate and careful screening and qualification criteria in cases where the research topic requires a more targeted group of respondents.

Tractica's primary research is supplemented by the review and analysis of all secondary information available on the topic being studied, including company news and financial information, technology specifications, product attributes, government and economic data, industry reports and databases from third-party sources, case studies, and reference customers. As applicable, all secondary research sources are appropriately cited within the firm's publications.

All of Tractica's research reports and other publications are carefully reviewed and scrutinized by the firm's senior management team in an effort to ensure that research methodology is sound, all information provided is accurate, analyst assumptions are carefully documented, and conclusions are well-supported by facts. Tractica is highly responsive to feedback from industry participants and, in the event errors in the firm's research are identified and verified, such errors are corrected promptly.

Chart 13.1 Tractica Research Methodology



(Source: Tractica)

NOTES

CAGR refers to compound average annual growth rate, using the formula:

CAGR = (End Year Value ÷ Start Year Value)$^{(1/steps)}$ – 1.

CAGRs presented in the tables are for the entire timeframe in the title. Where data for fewer years are given, the CAGR is for the range presented. Where relevant, CAGRs for shorter timeframes may be given as well.

Figures are based on the best estimates available at the time of calculation. Annual revenue, shipments, and sales are based on end-of-year figures unless otherwise noted. All values are expressed in year 2016 U.S. dollars unless otherwise noted. Percentages may not add up to 100 due to rounding.

Published 4Q 2016

1111 Pearl Street, Suite 201
Boulder, CO 80302
Tel: +1.303.248.3000
Email: info@tractica.com
www.tractica.com