Internet/Financial Technology

The Blockchain Report: Welcome to the Internet of Value

Blockchain technology is a radical innovation that enables direct value exchange over the internet. This is a powerful departure from the status quo, where digital value exchange has always necessitated a middleman and, consequently, incurred their inherent friction in the form of cost, delays, and risk. In this respect, **blockchain is a disintermediating technology that is removing friction in the exchange of value over the internet.** In this report we examine the essence of blockchain technology, identify eleven use cases and applications, highlight drivers and hurdles for mainstream adoption, and profile some of the leading companies in the space.

As a result of several structural advantages such as durability, transparency, and immutability we believe that blockchain technology will have a significant impact on many industries including Payments, Exchanges, Cybersecurity, IoT, and Smart Contracts. Emerging trends in the industry such as early enterprise adoption, usage trends, R&D expenditure, and venture capital activity, suggest that blockchain technology is approaching an inflection point toward greater mainstream and enterprise adoption.

A major factor for realizing the full potential of blockchain technology—and a critical portion of our thesis and expectations—is the permissionless innovation that is enabled by public blockchains. In the same way the openness of the internet and the freedom to build upon it enabled a rich ecosystem of innovative information applications and services, so too do we expect an open value exchange network to develop into a rich ecosystem with previously impossible and hard-to-imagine money/value applications and services. We believe this is happening and the innovative use cases described throughout this report are early evidence of the potential ahead.

We see blockchain technology as a disruptive innovation whose impact will ultimately be profound. Similar to how the proliferation of internet accessibility created the opportunity for new business models for information exchange in the likes of Facebook, Twitter and LinkedIn, so too will the rise of blockchain technology present new business opportunities of similar scale for value exchange.

Venture capital invested in blockchain-related companies has accelerated considerably over the past three years and is on track to top $600 million in 2015. We expect venture capital flows to accelerate in 2016 and lead to further development of the foundational and infrastructure services necessary to create a fertile "plug and play" ecosystem for entrepreneurs and innovation that will ultimately escalate enterprise adoption from a trickle in 2016 to a multi-year boom starting in 2017.

Topic of Discussion:

Blockchain Technology

Contributing Analysts

Spencer Bogart, CFA
(415) 262-4877
sbogart@needhamco.com

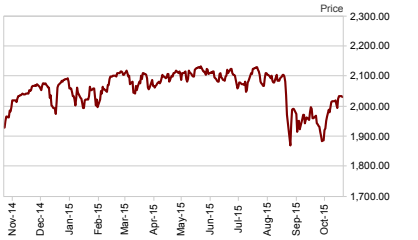
Kerry Rice
(415) 262-4890
krice@needhamco.com

Companies Mentioned in Report:

- **Amazon.com, Inc. (AMZN: $560.88, PT: NA)**
- **eBay Inc. (EBAY: $24.42, PT: NA)**
- **Alphabet Inc. (GOOG: $650.28, PT: $740.00)**
- **Seagate Technology (STX: $38.52, PT: $50.00)**
- **Cisco Systems, Inc. (CSCO: $28.50, PT: NA)**
- **Facebook, Inc. (FB: $97.00, PT: $115.00)**
- **LinkedIn Corporation (LNKD: $197.60, PT: $260.00)**

Sector Chart

S&P 500 10/21/15



Relevant disclosures begin on page 56 of this report.

The Blockchain Report:

Welcome to the Internet of Value

Introduction

Blockchain technology first emerged as the backbone of Bitcoin in 2009 and lived a relatively quiet existence in its early years. As the new technology established a formidable track record, its true potential began to emerge and gain wider recognition beyond a core group of passionate followers. Since then, there has been a flurry of advancements, new use cases, and applications of blockchain technology.

Emerging trends such as early enterprise adoption, usage trends, R&D expenditure, and venture capital activity suggest that blockchain technology is approaching an inflection point toward greater mainstream and enterprise adoption. While public investment opportunities for pure-play blockchain opportunities are minimal today, the technology has potentially far-reaching implications for public companies across a broad swath of sectors and industries.

The pace and magnitude of venture capital flowing to blockchain-related companies is rapidly accelerating, and there are dozens of private companies at the very early stages of disrupting massive markets.

Currently, the foundational layer and infrastructure necessary to support a rich ecosystem of blockchain-based applications and services is being established. As they mature, we expect to see blockchain-enabled companies flourish and bring new economic efficiencies and possibilities into the mainstream.

As with any new technology that fosters a rapidly developing market, there's significant confusion regarding blockchain technology, its advantages, and the significance of potential applications. **We hope to clear the muddied waters by providing a useful explanation of the technology, by highlighting its structural advantages, and by outlining how those advantages manifest in applications.**

In this report, we provide our interpretation of the current blockchain landscape, highlight emerging themes, provide an analysis of blockchain capital formation and, finally, profile some of the leading private companies in the industry. The overarching purpose of the report is to explore the disruptive impact of blockchain technology across a range of applications and use cases.

What is Blockchain Technology?

Blockchains come in many shapes and sizes with vast structural differences. Our comments and analysis here pertain largely to public blockchains and, specifically, the Bitcoin blockchain because it has a proven track record and an established network effect with a rapidly expanding and diversifying ecosystem. However, we also address the uses, advantages, and disadvantages of private, permissioned, and federated blockchains throughout this report. While private, permissioned, and federated blockchains do not have an extensive track record, they have garnered an increasing amount of enterprise attention and venture capital activity.

What Is a Blockchain?

Generically, a blockchain is a distributed ledger: a chronological chain of "blocks" where each "block" contains a record of valid network activity since the last block was added to the chain.

More Specifically…

The Bitcoin blockchain is a distributed chronological ledger of valid network transactions that anyone can review, anyone can add to (by transacting on the network), but nobody can change. As a result, it is a complete and immutable history of activity (transactions) within the network.

Which Is Significant Because…

This complete and immutable history is used to obviate trust and middlemen. It enables two or more entities that don't necessarily know or trust each other to securely exchange value over the internet without involving a third party.

This is a significant departure from the status quo where secure value exchange over the internet has always required an intermediary, a trusted third party. Removing these intermediaries also removes the inherent friction of middlemen that come in the form of costs, delays, and risk. In this respect, blockchain is a disintermediating technology that eliminates friction in value exchange over the internet.

Network Effect

An important characteristic of most blockchains is that they thrive on the network effect and become increasingly robust, secure, valuable and attractive with greater adoption—a critical factor in analyzing the future viability of the vast array of blockchains in existence.

Decentralized

Among the most important qualities of a blockchain is that it is decentralized—meaning that no single entity is in control of the record. Instead of a central authority holding and maintaining the record—where concentrated power can be abused, hacked, or simply neglected—it is distributed among a network of independent computers and constantly validated by network participants.

Distributed Consensus

Therefore, among the greatest achievements of blockchain technology is the ability to reach *distributed consensus*. That is, the ability to get a distributed network to come to agreement/consensus regarding the state of data without involving a central authority. By removing the need for a trusted third party or central authority to monitor and retain control, blockchain facilitates peer-to-peer, consensus-based exchange and record-keeping.

Relative to Status Quo

This is a profound difference from the status quo of how centralized systems operate today. In centralized systems, access is based on trust: Access is heavily restricted for people, businesses, and administrators that want to connect to the system—anything less could compromise its integrity. Under this model, the more people that have access to the network, the greater the risk to the network.

In contrast, **the Bitcoin blockchain uses an alternative model for access: It trusts no one but is open everyone**. That's because blockchains are built with the goal that the only feasible way to gain is to play by the rules—nefarious behavior costs more than it's worth. Moreover, not only does the Bitcoin blockchain welcome everyone but it relies on the pursuit of self-interest to secure the network. So rather than self-interest being the primary threat, it is the basis of security.

Permissionless Innovation

Perhaps the single greatest catalyst for the growth and development of public blockchains and their relative ecosystems is that they enable permissionless innovation: Anyone can connect to the network and build products, services, and applications off the open network.

From the Internet of Information to the Internet of Value

In the same way that the internet enabled permissionless innovation for all things regarding information exchange, so too do public blockchains enable permissionless innovation for all things regarding value exchange. Just as TCP/IP became the foundational standard for an open network of information exchange (what we know as the internet today), so too will the Internet of Value rely on a common foundational standard which will likely be a public blockchain—Bitcoin being the current forerunner.

"The same way TCP-IP imposed itself as the main protocol in the early days of the creation of internet, and no other (even better) protocol could develop enough network effect to overcome it ever since, so Bitcoin is the first and the most important of "Internet of Value" protocols, and there are high chances that it can establish itself as a global standard, as it leverages at least four powerful network effects: Bitcoin network has by far the largest hashing power (and so the greatest security), the higher capitalization, the largest user (and merchant) adoption, the best and largest developing and maintenance effort around it."

Intessa Sanpaolo in response to ESMA Call for Evidence)

"Bitcoin protocol and network today is that foundational layer. It is value transfer network. Beyond that, it is a core, backbone security service securing contracts, physical and digital property, equities, bonds, robot A.I. and an enormous wave of applications which have not yet been conceived. Inventing bitcoin-the-currency, securing bitcoin-the-token, was the Minimum Viable Product, the necessary first step towards building a universe of secure, decentralized services."

Jeff Garzik, Bitcoin Core Developer

Blockchain Beyond Currency

While the Bitcoin blockchain was built to be a payment network, blockchain technology is now being applied for many other use cases. For example, Nasdaq Private Market is working with the company Chain to leverage blockchain technology for the issuance, trading, and settlement of private market securities, and Guardtime uses blockchain technology as a cybersecurity tool to verify systems integrity. To address these and the other uses highlighted throughout this report, there are many different blockchain strategies being pursued.

The Bitcoin Blockchain, Alternative Blockchains, and Other Strategies

There are many blockchains in existence—some competing and some complementary with one another. The most famous of these and the most widely used is the Bitcoin blockchain. This was the original implementation of blockchain technology, and Bitcoin was the first application of blockchain technology. Far from being currency-specific, the Bitcoin blockchain is now being used for many applications beyond currency.

However, perceived weaknesses of the Bitcoin blockchain have led to the creation of alternative blockchains that are entirely independent of the Bitcoin blockchain and that seek to remedy real or perceived shortcomings of the Bitcoin blockchain. These alternative blockchains tout features such as even faster settlement times, larger transaction sizes, different consensus methods, varying degrees of anonymity/pseudonymity, more advanced functionality, permissioning features, etc.

Seeing as how the Bitcoin blockchain was built to facilitate the exchange of a digital currency, the question that arises isn't whether blockchain technology will be used for other uses (it already is) but what the best approach is for facilitating other applications.

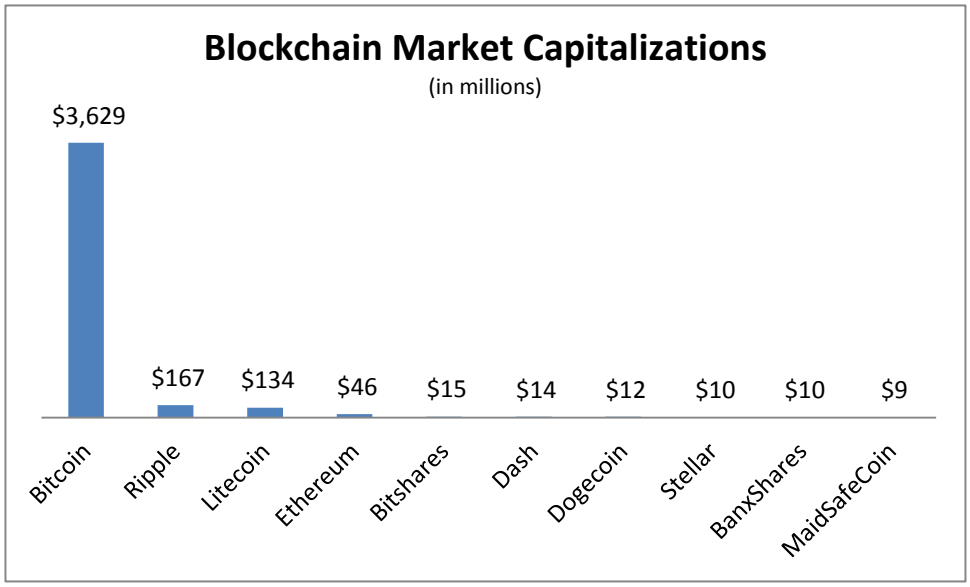
We note three main approaches currently being pursued in the industry: 1) **alternative blockchains**—which seek to create new blockchains independent of the Bitcoin blockchain; 2) **colored coins**—which use the Bitcoin blockchain and Bitcoins themselves to represent assets other than digital currency; and 3) **sidechains**—which use a two-way peg between the Bitcoin blockchain and alternative blockchains in order to get the best of both worlds (the network effect and security of the Bitcoin blockchain and the opportunity to build/try new capabilities and functions that comes with an independent blockchain).

Each of these approaches is worthy of a research paper of its own, so here we will suffice with a brief description of the three.

Alternative Blockchains

Alternative blockchains ("alt chains") is one approach to leveraging blockchain technology for applications beyond Bitcoin the digital currency. In this case, "alternative blockchains" refers to any blockchain other than the most popular one—the Bitcoin blockchain. They come in a wide variety of forms—each designed to either improve on a real or perceived weakness of the Bitcoin blockchain (e.g., transaction size/speed) or to facilitate functionality that isn't natively supported by the Bitcoin blockchain. The question is whether the advantages of these blockchains will be sufficient to overcome the huge network effect advantage of the Bitcoin blockchain. Furthermore, the Bitcoin blockchain protocol is not static and could incorporate the features of alternative blockchains and potentially render them obsolete. To date, no alternative blockchain has come close to the value/size of the Bitcoin blockchain. While we see it as highly unlikely that an alternatively blockchain will supplant the Bitcoin blockchain as an open payment network, we recognize that, for certain use cases, the advantages of an alternative blockchain (public or private) could be sufficient to justify an alternative independent blockchain.

Figure 1 Comparing Blockchains



Source: Coinmarketcap.com, 10/11/2015.

While none of these alternative blockchains comes close to the value of the Bitcoin blockchain, a direct comparison isn't appropriate for all. For example, Litecoin competes directly and is designed to be a better Bitcoin, but Ripple and Ethereum address different use cases altogether: private blockchains and smart contracts, respectively.

Alternative blockchains is a broad term that encompasses many different blockchain strategies. One subset of alternative blockchains is private, permissioned or federated blockchains. In contrast to the completely open and permissionless nature of public blockchains (where anyone can participate in the network and/or validate transactions), this strategy restricts transparency, access, and/or transaction validators on the network. The basic concept is to leverage blockchain technology for use cases where the perceived risk of complete openness and accessibility outweighs the risk of trusting one entity or a group of entities. As transaction validation is restricted from an unlimited number (as on the Bitcoin blockchain) to a group of validators (as on a federated blockchain) to a single validator (as on completely private blockchains) network participants place an increasing amount of trust on the validators: from none in the case of the Bitcoin blockchain to a very high level of trust in the case of a completely private blockchain. For some use cases, particularly where the counterparties on the network know each other, this introduction of trust may not be problematic. This partly explains why there has been heavy exploration of private blockchains as a means for banks to conduct business with each other.

Colored Coins

Colored coins is another approach to extending blockchain technology beyond the transacting of digital currency. In contrast to "alt chains," the colored coins approach uses the Bitcoin blockchain. Colored coins are miniscule, cryptographically unique fractions of a Bitcoin that have been explicitly demarcated to represent another asset (other than the trivial amount of Bitcoin that it is tied to) such as shares of a company, bonds, currencies, or another asset.

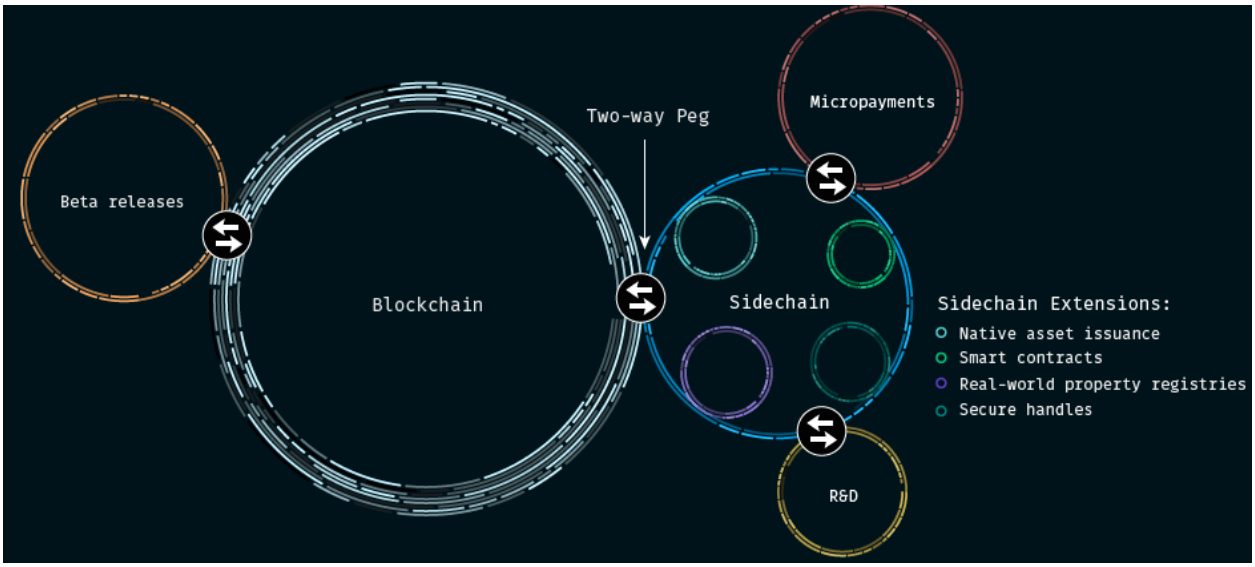
The advantage of the colored coins approach is that it captures the network effect of the Bitcoin blockchain, uses regular Bitcoin transactions, and will inherently leverage

future advances of the Bitcoin protocol. The downside is that transacting directly on the Bitcoin blockchain limits the features and functionality of colored coins to that of the Bitcoin protocol. Additionally, there's concern that widespread adoption of such an approach could "bloat" the Bitcoin blockchain (a concern that revolves around the current size limit and transaction speed of blocks on the Bitcoin blockchain). Nasdaq is using the colored coins approach as part of an enterprise-wide blockchain initiative whose first goal is to leverage colored coins and the Bitcoin blockchain to trade private company (pre-IPO) shares.

Sidechains

Sidechains are alternative blockchains that are linked to the Bitcoin blockchain via a two-way peg—thus allowing users to seamlessly transition between the alternative blockchain and the Bitcoin blockchain. If successful, **sidechains could be the Goldilocks approach, as it would allow sidechains the freedom to optimize their respective blockchain for specific features while also allowing them to leverage the network effect of the Bitcoin blockchain.** While this functionality is new to digital currency, it is a centuries-old solution in that the relationship between a sidechain and the Bitcoin blockchain is fundamentally analogous to the relationship between a gold-backed currency and gold itself.

Figure 2 Visual Illustration of Sidechains



Source: Blockstream.

The Show Will Go On

While this is a notable area of uncertainty whose resolution will be determined by the market as businesses select an approach to build toward, the debate will largely go unnoticed by end-users and should not greatly affect the development of applications. Regardless of whether alternative blockchains, sidechains, colored coins, or another development are the way forward for blockchain technology, these competing projects have more in common than they have in difference and whatever differences they have are greatly overshadowed by their common structural advantages.

"I don't know what's going to succeed. What I'm certain of is that we are going to see blockchain solutions, peer-to-peer solutions emerging in our industry and we want to be close to that development."

Simon McNamara, Chief Administrative Officer, RBS

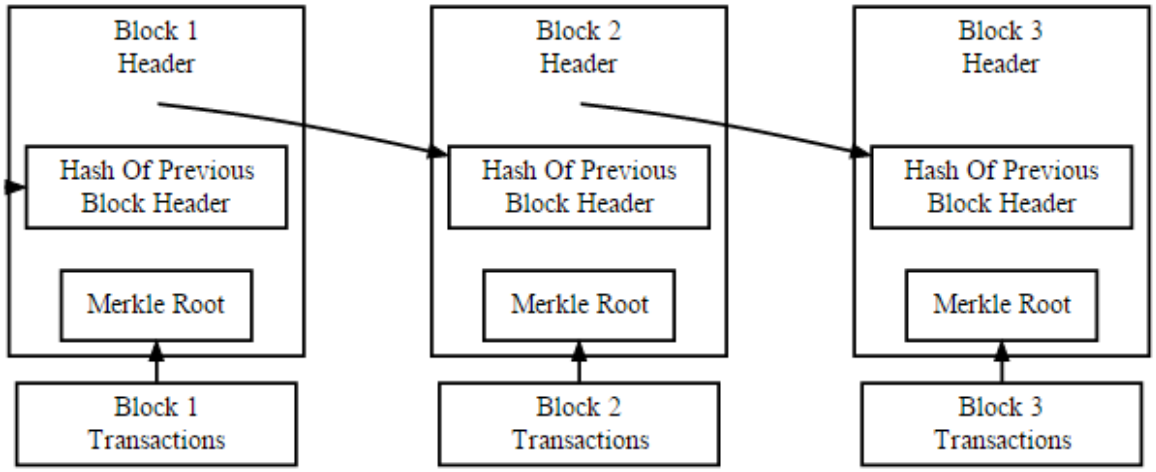
Brief Technical Explanation

We offer a brief step-by-step description of how a Bitcoin transaction is added to the Bitcoin blockchain. For a more detailed technical explanation of how the Bitcoin blockchain works, we recommend the original Bitcoin whitepaper by Satoshi Nakamoto and other resources from Bitcoin.org. While other blockchains function similarly, they each have their own intricacies. We recommend addressing the original whitepapers for each of these blockchains for complete technical explanations.

A Bitcoin transaction:

1. Alice wants to send Bitcoin to Bob. She submits a transaction to the network.
   - Alice is attempting to change the record of ownership of the Bitcoin in question from herself to Bob. To do this, she sends a message to the network and uses her public and private key (public key cryptography) to prove that she is the current valid owner of the Bitcoin in question. Alice identifies the receiver by including Bob's public key in the transaction. Once the transaction is processed, Bob will use his private key to prove he is the owner of the public key to which Alice has ascribed ownership.
2. This transaction information is broadcast out to the nodes on the network.
3. Nodes receive information about this transaction and all other transactions occurring around the same time and verify that for each transaction the person who is sending Bitcoin is the rightful owner and has not already spent it.
4. Nodes work to incorporate the transaction into the ledger of all valid transactions that have ever occurred.
5. Nodes take all the transactions that have occurred recently and aggregate them into a block, which each node will independently try to add to the publicly recognized valid ledger (blockchain).
6. The transaction processors (miners) then try to solve a proof-of-work that is essentially a randomized math problem that requires computing power (and the associated energy consumption) to solve.
7. Once a miner solves the proof of work, they broadcast the solution and group of transactions to all the other nodes who then incorporate the block into their versions of the ledger—thereby adding it to the blockchain and validating the transaction. This block is then a necessary input into the mathematical puzzle for the next block to be added, thus linking the blocks together and creating a "blockchain."

Figure 3 Bitcoin Blockchain Visual Illustration



Source: Bitcoin.org Developer Guide.

Structural Advantages of Blockchain Technology

As we'll see throughout the various applications that follow, there are several recurring advantages of blockchain technology. However, because blockchains differ structurally from one another in several important ways, the advantages that follow manifest to varying degrees (or not at all) in any given blockchain. The broad, frequently recurring advantages that we have identified include durability, process integrity, transparency, immutability, longevity, reliability, and availability. For now, only the Bitcoin blockchain can claim them all.

Durability

Public blockchains operate on decentralized networks as opposed to a central server or network of servers. Without a central point of failure, distributed ledgers are significantly more durable than today's centralized systems and better able to withstand anything from malicious network attacks to power outages. The Bitcoin blockchain, for example, runs on thousands of nodes (over 5K) around the world.

Process Integrity

By nature, distributed open-source protocols execute exactly as their code dictates—removing the need to trust a third party to execute any given transaction (money, data or otherwise). With a robust blockchain like the Bitcoin blockchain, users can be certain that transactions will be executed exactly as the protocol commands. Relative to trusting a third party, this greatly improves process integrity/execution surety. One implication of this process integrity improvement (quicker adoption timelines) is described in the implications section that follows.

Transparency

As distributed publicly viewable ledgers, public blockchains have inherent transparency advantages in that any changes to the ledger are public so, whether the service utilizing the blockchain is a smart contracts platform or a value transfer application, any changes are apparent and traceable. Private blockchains tend to optimize this transparency for their various applications—some being relatively opaque and others being nearly as transparent as a public blockchain.

Immutability

Records that are validated onto a well-distributed public blockchain—such as the Bitcoin blockchain—are practically immutable. This allows processes and applications enabled by blockchains to operate with the highest degree of confidence that they have a complete and unaltered history of activity. This is crucial for many applications enabled by blockchain technology such as payments protocols, securities settlement networks, and systems integrity applications. In these instances, anything less than a complete and unaltered history of transactions/activity on the blockchain creates a huge risk for honest users and a huge opportunity for potentially fraudulent users.

Longevity

Devices, services, and applications that offload their critical transaction processing functionality to a public blockchain that is independent of the device manufacturer, service provider, or application developer, can instill confidence in consumers and users that the device, service, or application will continue to function for a long time—even if the device manufacturer, service provider, or application developer goes out of business, loses interest in it, or subsequently wishes to manipulate the transaction processing function. This is particularly relevant to device manufacturers for the Internet of Things, where the confluence of long lifespan and low-cost products coupled with the burden of centralized operation (such as the maintenance of server-farms) drive a strong incentive to offload critical transaction processing functionality to a blockchain.

Reliability & Availability

A well-distributed blockchain with a high level of redundancy can be considered highly reliable because the failure of any particular node or group of nodes does not compromise the blockchain's transaction processing capabilities. Similarly, because the data and information contained within a well-distributed blockchain is available for access from hundreds or thousands of nodes, it is also highly available.

Implications of Structural Advantages

Disintermediation & "Trustless" Exchange

Among the greatest gains of blockchain technology and perhaps the single greatest contributor to its economic advantage stems from its ability to instill trust between two transacting parties without third-party intermediation. Said simply, blockchain technology allows one entity to confidently transact value directly with another entity without relying on a third party to stand between them and ensure that each honors the transaction agreement. Eliminating the need for third-party intermediation goes a long way toward removing friction and creating efficiency in all types of value exchange.

Empowered Users

A common theme evident in the applications of blockchain technology that are discussed in this report—and a direct effect of disintermediation—is that users are increasingly in the driver seat and in control of all their information and transactions. Examples throughout this report showcase users in control of their own financial data, their money, their personal documents, and their personal identity.

Data Will Be Better than Ever

Blockchain data is high quality in terms of completeness, validity, consistency, timeliness, accuracy and availability. Furthermore, because the data is essentially stored in a giant public data base (the distributed ledger), it is highly accessible.

Aside from data contained within a blockchain, what can be done with proprietary data will also be greatly improved: individuals and businesses will be able to leverage blockchain technology to store data in the cloud without any complete copies in any one place—eliminating the opportunity for the dataset to be compromised by hackers or insiders. Businesses will also be able to run analytics in the cloud without revealing the complete dataset to anyone—thereby eliminating the inherent vulnerability of centralized storage and analytics.

Faster Growth and Adoption Times

Traditionally, businesses grow and attract users by operating honestly and building trust over time. Depending on the business or industry, this can be a long process that hinders the growth and adoption of new businesses and services—particularly at the outset. What would be helpful for these businesses would be the ability to independently prove that they will do what they claim to do, that they've handicapped their own role to prevent interference, and that their device, service, or application will continue to perform its critical function even if the company goes out of business. Blockchain enables businesses to do this. Device manufacturers, service providers, and application developers can offload their critical transaction processing function to a blockchain such that it can be independently reviewed, cannot be interfered with, and will continue to function independent of its original sponsor.

Blockchain Applications & Use Cases

The potential applications of blockchain technology are vast and the most fruitful applications of the technology may yet be developed. We have identified eleven applications of blockchain technology that we think are particularly interesting to explore in greater depth. At the back of this report, we profile some of the leading companies and services in several of these application areas.

As a framework for identifying the most promising applications of blockchain technology, we examined the areas where the advantages of blockchain technology are greatest relative to the status quo—the applications where blockchain best addresses pain points and adds value. **We expect that much of the initial success with blockchain technology will center on applications that improve existing processes and services. That is, applying the disruptive technology (blockchain) to sustaining innovations.**

We believe that the second stage of innovation for blockchain technology will more fully leverage the opportunities of an open and permissionless value layer of the internet to create truly innovative processes, services, and applications that were not previously possible.

Payments

To the payments industry, and the $425 billion in transaction-related revenues generated[1] blockchain technology could bring improvements in security (users fully

[1] *Global Payments 2014*, The Boston Consulting Group (September 2014)

in control of payment info), speed (faster settlement times), access (no bank account required), and cost (reduced/more efficient infrastructure).

In terms of privacy and security, blockchain-based payments are "push" rather than "pull" transactions: Users send defined funds (push) without providing the merchant with their personal bank account information which the merchant otherwise stores and uses to withdraw funds (pull). Consequently, using a blockchain for payments allows a user to isolate their payment information and pay without disclosing and storing their financial or credit card information with the merchant—stored data that creates an attraction for thieves and hackers. In light of recent high-profile breaches at the likes of Home Depot (56 million cards compromised), Target (40 million cards compromised), Michael's (2.6 million affected), and many others, this could be one of the most important features of blockchain technology for the payments industry.

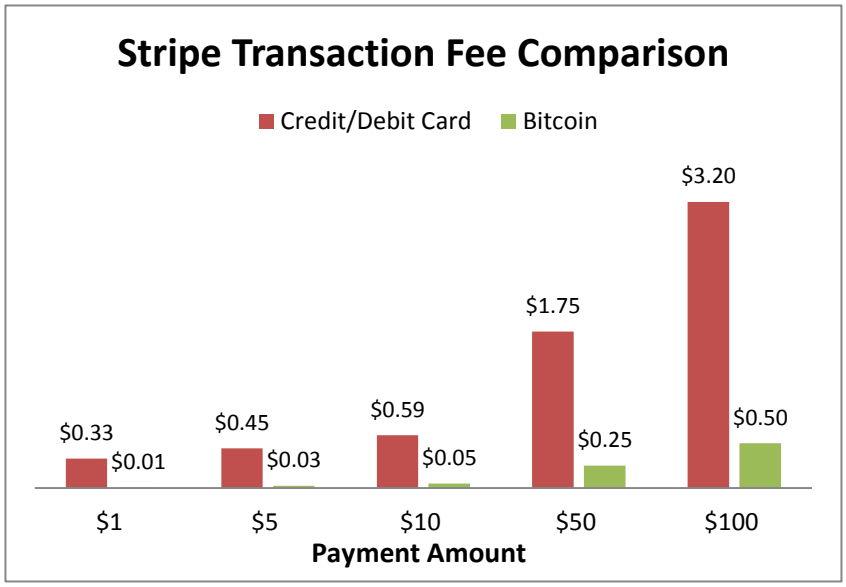
Forward-thinking companies have picked up on this security feature: Apple Pay and Google Pay are "token" systems that allow a user to pay without giving the merchant their financial information. Instead, Apple (or Google or PayPal) stores the information and uses a cryptographic token that represents your financial/credit information. The token is used to charge your card for that transaction but it can't be used again. While this greatly reduces the number of places that a user's payments information is stored (and, consequently, the number of breach opportunities), it still leaves one centralized risk: Apple and Alphabet (GOOG – BUY) themselves.

In contrast, with a blockchain-based payments system, the user stays fully in control of their account information and is never forced to provide it to third parties—which otherwise store the payment information and consequently attract thieves and hackers.

From a merchant point of view, blockchain-based payment networks may be preferred because there's no inherent processing fee (although some services will automatically process digital currency payments and convert to local currency for around 0.50%), they can open their business to users worldwide, avoid chargeback fraud, and circumvent the cost and risk of storing users' payment information.

Delving deeper into the issue of cost: Merchants that rely on payment processors can save 80-90% on transaction fees with Bitcoin payments relative to traditional credit/debit card payments. Merchants are charged an average of roughly 3% to accept a credit/debit card at their business but can accept Bitcoin payments for much less. For example, Stripe normally charges merchants a 2.9% processing fee in addition to a flat $0.30 per transaction, but the company only charges 0.5% to accept Bitcoin payments. Similarly, Braintree (PayPal subsidiary) doesn't charge a fee for the first $1 million that a merchant accepts in Bitcoin and subsequently charges 1% per transaction after the $1 million threshold is passed. Both services leverage Coinbase (private company) to enable this functionality.

Figure 4 Stripe Transaction Fees



Source: Stripe.

The cost advantage manifests in a similar fashion for corporate payments, where blockchain-based networks could become the connective tissue that allows what are otherwise relatively siloed payment systems to communicate and exchange in real-time with complete confidence.

The other big advantage that blockchain technology brings to the payments industry is settlement time. Most credit and debit card transactions don't settle for several days after a payment. However, Bitcoin-based payments settle much faster: anywhere from near-instantly to a couple of hours (depending on the degree of confidence necessary for the transaction).

In turn, this quicker settlement time is the source of another big cost advantage of blockchain technology for the corporate payments market: the cost of float. International payments typically take over two days to settle and during that settlement time companies are forced to let cash sit idle instead of earning a return. Furthermore, foreign exchange costs could be reduced by two factors: 1) quicker settlement times reduce exchange risk; and 2) the introduction of competitive foreign exchange marketplaces (such as Ripple's) could produce more competitive rates for cross-border corporate payments.

Not only can blockchain-based payment systems improve on traditional industry metrics, they are also enabling new functions such as "micropayments" or "nanopayments." Historically, there's been a fixed cost associated with payments that has made it economically impractical to use traditional payment networks for very small transactions (usually a fixed fee of around $0.30 per transaction). However, with blockchain-based payment networks, users could transact very small amounts such as micro- or nanopayments for each page viewed on a website (paid seamlessly in real-time).

For example, blockchain-based payment services present the possibility of paying for access, such as to the *Wall Street Journal*, not on a monthly subscription basis but on a per-article basis or, perhaps even more likely, on a per-page-read basis. From a user standpoint, this is a favorable closer alignment between value received and cost paid

and is a further extension of an ongoing trend in other industries, such as the shift in software from perpetual licenses deals to subscription models.

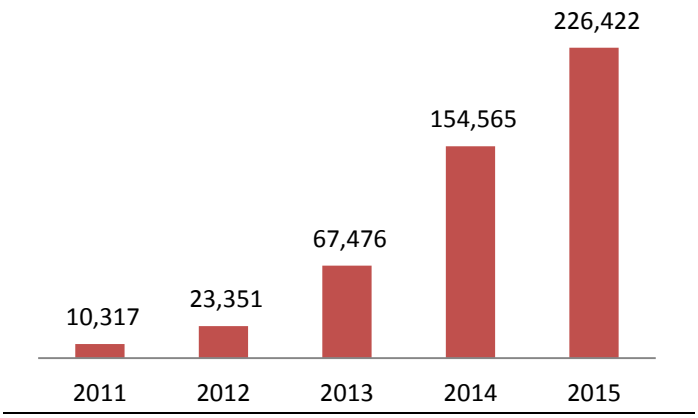
This is just one of the potentially many opportunities that will contribute to a large expansion in digital value exchange as blockchain technology reduces friction and drives down cost significantly.

Trends on the Bitcoin network (as seen in Figure 5) are generally up and to the right—especially in terms of average daily transaction count and the number of unique addresses used. There's a slight slowdown in 2015 for estimated daily transaction volume and in total transaction volume. Because other usage metrics have increased significantly, we attribute the slowdown to the price of Bitcoin which is down more than 50% from an average of $527 in 2014 to an average of $248 in 2015.

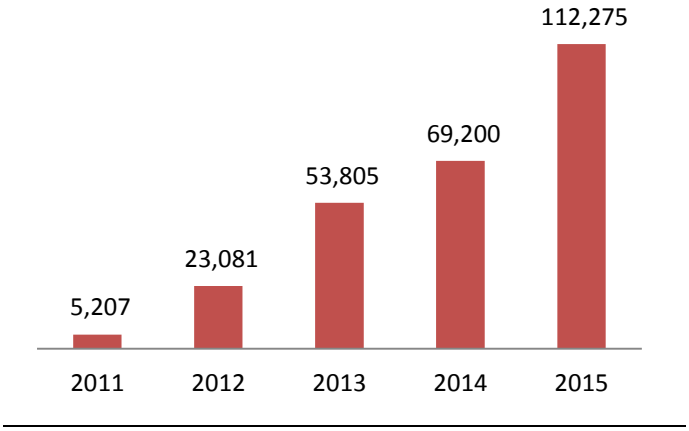
In addition to the cost, speed, and security/privacy advantages, blockchain-based payments have an access advantage and a potential innovation advantage. Permissionless blockchain-based payment networks like Bitcoin have an access advantage because they don't require a bank account—thus opening the networks to the half of the world's population without a bank account. Lastly, as a particular network achieves critical mass, there is an innovation advantage from being an open network on which entrepreneurs and developers are free to build.

Figure 5 Bitcoin Market Data

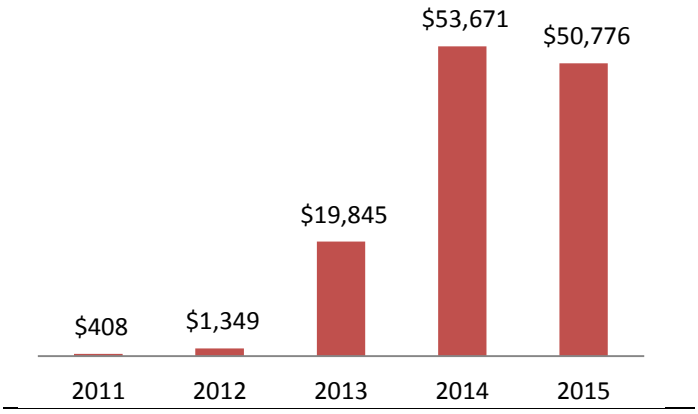
Average Daily Unique Addresses Used



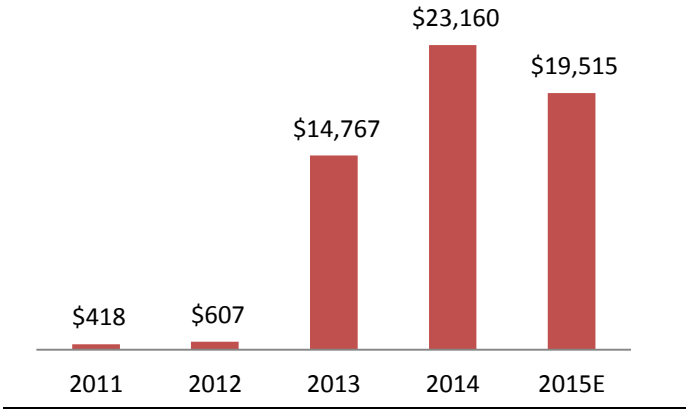
Average Number of Daily Transactions



Median Daily Transaction Volume (thousands)



***Total Transaction Volume** (millions)*



Source: Blockchain.info 10/6/15.

Exchanges

Blockchain technology's most natural application is in digital value exchange, and we believe it will have a profound impact on the structure of financial markets—specifically in regard to clearing and settlement processes. There are two primary types of blockchain-related applications to discuss here. First, there's digital currency exchanges, which facilitate the buying and selling of digital currencies like Bitcoin. Second, there are the companies creating the platforms and software to facilitate the exchange of other digital assets (equity securities, bonds, energy credits, gift cards, mobile minutes, etc.).

"As blockchain technology continues to redefine not only how the exchange sector operates, but the global financial economy as a whole, Nasdaq aims to be at the center of this watershed development. The benefits to the industry are immense and cannot be ignored"

Bob Greifeld, CEO, Nasdaq

Digital currency exchanges—which facilitate the buying and selling of digital currencies such as Bitcoin—are tangentially related to blockchain technology in that they serve as strategically positioned on- and off-ramps to the world of digital currencies. There are only two ways to acquire Bitcoin, for example: mine for it by processing transactions and collecting the associated Bitcoin rewards or buy it with another currency. However, considering that transaction processing is confined largely to specialists with highly optimized equipment, the vast majority of digital currency acquisition ultimately takes place through an exchange. Some of the most popular digital currency exchanges in the world include Coinbase, itBit, Kraken, Bitstamp and Bitfinex.

These digital currency exchanges are well positioned in the emerging blockchain ecosystem where, regardless of the use case, digital currency serves largely as the lifeblood of blockchain applications.

In terms of disruptive impact, however, blockchain technology's biggest contribution is likely in the exchange of assets beyond digital currencies. Blockchain technology will likely have a drastic impact on post-trade processes such as clearing and settlement for a broad array of digital assets, including equity securities (private and public), debt securities, energy credits, gift cards, and mobile minutes.

When applied to digital asset exchange, blockchain technology could bring significant improvements in speed and cost. In stark contrast to the traditional three-day settlement timeframe that dominates modern financial markets, a clearing and settlement network built on blockchain technology could facilitate near instant settlement. The U.S. moved to a three-day framework in 1996 (from a five-day process) and considering the advancements in speed, connectivity, and technology since then, a major upgrade is in order.

"While the technology to exchange messages for trade is fast, the technology to actually move the asset and settle them is slow and very expensive. The opportunity here is to bring asset transfer into the 21st century and that's something we couldn't do easily before the blockchain."

Adam Ludwin, CEO, Chain

As it stands, trading a digital security such as a stock requires a series of intermediaries that add cost, delays, points of failure, and vulnerability to the exchange process. Consultancy Oliver Wyman estimates that globally these processes add $65-80 billion in costs each year[2]. Fundamentally, blockchain technology was built to cut through these intermediaries and allow counterparties to confidently transact directly with one another.

The post-trade process consists largely of distributing and duplicating data across relevant counterparties to transfer the title of an asset in a way that protects counterparties from each other. However, this results in costly and time-consuming reconciliation processes across intermediaries. In contrast, blockchains are shared infrastructure that solve the data synchronization and trust problem by replicating data throughout a network. This shared blockchain infrastructure performs the function of many intermediaries, facilitates real-time information exchange and drastically minimizes error rates—all of which should reduce settlement times (to nearly instant) and bring significant cost savings to the exchange of digital assets.

Beyond the exchange of securities, blockchains are also being used to register digital asset ownership and to issue digital assets—which are necessary first steps before these assets can be exchanged on a blockchain. For example, Digital Asset Holdings recently helped Pivit (a live-odds and prediction platform) issue a portion of its latest funding round directly on a blockchain. Similarly, Nasdaq private markets is working with Chain to leverage blockchain solutions for the exchange of private market securities—Chain also plans to issue its own pre-IPO shares directly on this blockchain. Lastly, Overstock.com leveraged its own cryptosecurities trading platform, tØ, to issue a $5 million "cryptobond" via blockchain technology.

Among the companies creating the software, platform and networks to facilitate blockchain-enabled clearing and settlement processes, we note leading companies Chain, Digital Asset Holdings, itBit (Bankchain), Ripple Labs, and tØ.

Smart Contracts

Blockchain-enabled smart contracts could bring tremendous advantages and innovation to the digital world. The basic premise of smart contracts is to reduce mutual agreements between businesses, individuals, or machines to software code that self-executes and self-enforces. This functionality could greatly reduce costs and risks for businesses and individuals.

Smart contracts can be viewed as a software protocol that performs a function when certain conditions are met. In his 1997 paper, "Smart Contracts: Building Blocks for Digital Markets,"[3] the pioneering thought leader behind smart contracts, Nick Szabo, described vending machines as operating via a basic smart contract mechanism in that they deterministically release an item when the correct value is submitted and the selection is made.

Outlining the future potential of embedded smart contracts, Szabo highlighted (in 1997) an example that today may not be far from reality: A smart contract between a bank and a car buyer which specifies that the customer has rights to the car so long as they make their payments and, if they fail to do, the contract returns control of the car's digital keys to the bank. This process happens automatically, transparently, and at a lower cost than alternative measures.

Blockchain-based smart contracts can add this same functionality to a broad array of daily tasks and applications. The idea of smart contracts is relatively straightforward: A software protocol performs an action (releases funds, sends information, makes a

[2] *The Capital Markets Industry,* Oliver Wyman (2014)
[3] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets,* (1996)

purchase, etc.) when certain conditions are met (a payment is received, the outcome of an event is determined, etc.).The advantage of blockchain-based smart contracts is that they reduce the amount of human involvement (billable hours from attorneys and accountants) required to create, execute and enforce a contract—thereby lowering its cost while raising the surety of execution and enforcement.

One of the challenges of smart contracts is how to ingest the trigger event to fire up the engine of the smart contract. For digital events and transactions, the solution is relatively simple: For example, a record of payment can easily be recorded and ingested with little dispute. The task becomes more challenging as we move to events in the physical world to trigger the contract. Solutions for this functionality include multi-signature transactions, prediction markets, and oracles.

- *Multi-signature transactions* simply require some subset of the parties to agree that the terms have been met, thereby triggering execution of the contract. An example is a digital transaction between a buyer and seller that may also involve a third party "trust/escrow agent." In this instance, the payment will be transferred to the seller if two of the three parties agree that the terms have been met: First, it will be between the buyer and seller and if they both agree there's no need to involve a third party but, in the case of a dispute, a third party can step in to cast a tie-breaking vote as to whether or not the terms of the contract have been honored. In the marketplaces section that follows we highlight how an open marketplace of escrow or trust agents could provide this service reliably at low cost.
- *Prediction markets*: The basic premise behind prediction markets is that the wisdom of the crowd is more accurate at predicting events than any expert. Prediction markets take this premise and add an economic incentive for genuine participation: Individuals can take the "yes" or "no" side of any event occurring and receive a payout according to the probability of the event occurring relative to its ultimate outcome. Traditional prediction markets are dogged by securities regulation in the U.S. but some decentralized alternatives, such as Augur (which is enabled by smart contracts platform Ethereum) aim to provide the same service and avoid regulatory burden by being strictly peer-to-peer.
- *Oracle services* are another potential solution as to how events from the physical world could reliably be registered in the digital realm. Oracle services are third-parties that verify the outcome of events and feed the data to smart contracts data services.

In short, smart contracts automate an exchange of value based on pre-specified conditions. They have a vast array of use cases in ecommerce, funding, gambling, legal services, digital property, machine-to-machine (M2M) communications, and access/admission control, among others. We've included a brief explanation of a few use cases below:

- **Ecommerce**: Smart contracts help facilitate trade and business between consumers on the internet by reducing counterparty risk (self-executing contracts that boil down to transparent logic) and reducing the costs of transacting by minimizing the amount of human involvement in the process.
- **Internet of Things** (IoT): Smart contracts could also be instrumental to machine-to-machine communications, where devices transact with each other autonomously according to predefined criteria. For example, an autonomous vehicle could pay for its own parking spot after it has dropped off a passenger. (We explore this further in the "Internet of Things" section.)
- **Access/admission control**: An AirBnB host could automatically provide digital keys to their smart-home after receiving payment and build

conditions such that the digital keys become inoperable after the paid length of stay.

- **Funding** (scholarship funds, unemployment, etc.) could be released according to conditions such as classroom attendance or anything else that can be verified digitally.
- **Gambling**: Blockchain-based gambling inherently uses smart contracts to release funds to winning parties according to the outcome of the game.
- **Estate planning**: Smart contracts could be used to release a will to the appropriate parties, or to disperse assets, upon death.
- **Digital property (such as digital art):** Smart contracts could be used to facilitate the transfer and licensing of proprietary content.

There are several different companies, groups and organizations forming platforms to facilitate smart contracts—the most prominent being Ethereum. Aside from the platform for smart contracts, leading companies such as IBM, Samsung and UBS are exploring how to integrate smart contracts into their products and services.

Internet of Things

"[Blockchain is] a completely novel architecture for business—a foundation for building a new generation of transactional applications that establish trust and transparency while streamlining business processes. We believe blockchain is an extraordinarily important phenomenon, which is why IBM is deeply engaged in moving it forward."

Arvind Krishna, Sr., Vice President and Director of IBM Research

As we move from billions of connected devices to hundreds of billions of connected devices, the mode of governance and operation of these devices' smart functionality and connectivity will be increasingly important. Traditional centralized computing models (cloud or otherwise) are sub-optimal for the Internet of Things in many regards, including security, privacy, scalability, longevity, and interconnectivity.

At the forefront of this problem is the issue of privacy and security. As consumers connect everything from their cars to their thermostats, they simultaneously produce a rich data history that includes intimate details of their daily life. Used correctly, this rich data is very valuable but the challenge is preventing its abuse. The best way to prevent the abuse of smart devices and the data that they generate is to avoid collecting it on and processing it through centralized systems. The centralization itself inherently enables governments, insiders, and other intruders to use and abuse the devices and generated data—with or without consent of the centralized entity itself.

There are many other significant drawbacks of a centralized model for the Internet of Things, including the fact that centralized systems inherently create points of failure, have a tendency to create walled gardens (which could limit interconnectivity between devices from different manufacturers), a lack of transparent and independently verifiable operational integrity, and a longevity challenge.

The points of failure inherent in centralized systems and the tendency to create walled gardens that limit interconnectivity are relatively straightforward and well-

understood, but the other challenges of verifiable operational integrity and longevity warrant further discussion.

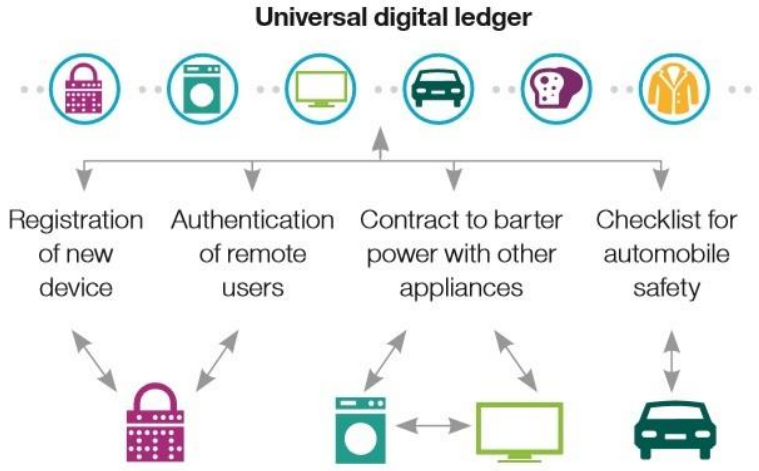
In regards to operational integrity, the problem lies in verifying that a smart, connected device has not been altered to operate outside its proper function. For example, it is important for the passenger of an autonomous vehicle to be able to independently verify that the vehicle's systems have not been altered to operate differently than intended—such as an alteration to drive at unsafe speeds or to deliver the passenger to the wrong location. Given that anything "connected" is potentially vulnerable to manipulation, the solution here is not security through obscurity, but instead, security through transparency, which then allows the state or integrity of a device to be independently verified against a history of previously valid states. Companies like Guardtime are already using blockchain technology to do this for customers and partners such as Lockheed Martin and Raytheon, which need to be absolutely certain of the operational integrity of their defense systems. While defense systems are an extremely high-value-add use case and, consequently, the first implementation, we expect that this same type of systems integrity solution will be critical for consumers and businesses in the Internet of Things.

In regards to the longevity challenge, the problem lies in the ongoing operational costs associated with maintaining connected devices in a centralized fashion. Consumers of smart products want to be sure that their device's smart functionality will continue to operate properly far into the future. In a centralized model, it will be difficult for all but the world's largest device manufacturers to convince consumers that the company will still be operational and able to maintain the device's functionality for the next 3, 5, or 10 years (aside from the question of whether this is economically feasible or desirable for the manufacturer). Furthermore, this is particularly concerning in that it creates a very high barrier to entry and, consequently, limits the speed on innovation in the industry.

To address the longevity challenge, device manufacturers are arguably better off discharging some of this burden to a distributed blockchain in a way that consumers can be confident that their device's smart functionality will continue to operate regardless of whether the original manufacturer is around (not out of business) or retains an interest (economic incentive) to do so.

Figure 6 Blockchain and the IoT

The blockchain functions as a universal digital ledger facilitating various types of IoT transactions between devices



Source: Veena Pureswaran and Paul Brody, Device Democracy, IBM Institute for Business Value.

The operation of connected devices and all computing ultimately boils down to data transaction processing. That is, with input X, perform action Y. That data transaction could be anything from sending and posting a Facebook (FB – Buy) update to uploading a file to Dropbox. However, as we move to a world of increasingly connected devices we need a way to eliminate trust from the data transaction in order to remove any uncertainty around processing. In the same way that blockchain technology solved the "trust" challenge of value transactions over the internet (via Bitcoin), blockchain technology can also solve the "trust" problems associated with other transaction over the internet—in this case, the data transactions originating from the Internet of Things.

In a research paper, IBM highlights this possible future for the Internet of Things: "In our vision of a decentralized IoT, the blockchain is the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an 'Internet of Decentralized, Autonomous Things' – and thus the democratization of the digital world".[4]

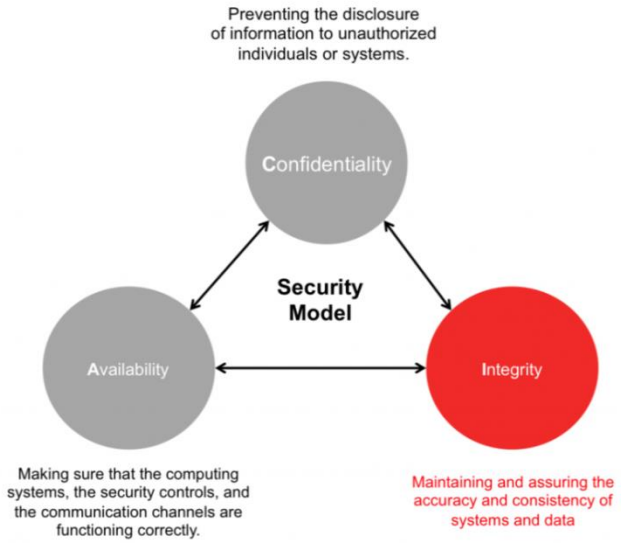
The blockchain could ultimately play three critical roles for connected devices: 1) immutable record of device identity; 2) the foundation for smart contracts; and 3) the exchange of value between devices.

For a more detailed evaluation of the benefits of a decentralized foundation for the Internet of Things, we recommend IBM research paper "Device Democracy: Saving the Future of the Internet of Things" and Filament's "Declaration of Device Independence."

Cybersecurity

In the same way that the integrity of a Bitcoin transaction is confirmed by an audit of the blockchain before it is processed, so too can the integrity of data, systems, and networks be verified with a blockchain. This powerful verification ability enables real-time detection of data manipulation and real-time verification of systems integrity.

Figure 7 CIA Triad of Cybersecurity



Source: Guardtime.com.

[4] Veena Pureswaran and Paul Brody, *Device Democracy,* IBM Institute for Business Value (2015).

Within the CIA triad (confidentiality, integrity, availability) of data security, blockchain technology is particularly well suited to address the integrity aspect. This is done by verifying the state of data, systems or networks against their previous states (which are recorded on a blockchain) and against the record of valid "transactions" (data actions such as transportation, processing, etc.) that has happened since (also recorded on a blockchain).

We note Guardtime as the leader in this space with its KSI blockchain and solutions.

Documentation

Record keeping is the very essence of blockchain technology and, consequently, it has tremendous potential value as an immutable and chronological documentation tool. We touch on this feature of blockchain technology in other sections of this report but are dedicating a section here in order to more explicitly detail the value of blockchain technology in this respect.

First, a point of clarification: Immutability is the primary advantage that blockchain technology brings to documentation. However, any given blockchain can only be described as immutable if its records are secured and cannot be changed. At this point in time, only the Bitcoin blockchain can be described as immutable. This is because the Bitcoin blockchain is secured by "proof of work" calculations which are performed dynamically by thousands of high performance computers around the world.

Using the immutable chronological record that is the Bitcoin blockchain, a time-stamped record of existence can be created in such a way that the creator of the record can later prove irrefutably that a particular document (or image, video, etc.) was in existence at that point in time. This is done by creating a hash of the document which is then stored in the memo field of a deminimis Bitcoin transaction. When that transaction is recorded into the Bitcoin blockchain, so too is the hash of the document. That hash (not the document itself) is now essentially written in stone—a stone that anyone can see and verify. At any later point in time, the user can produce the document and prove that it existed at the time of the transaction by matching the hash of the document they've produced to the one stored in the blockchain. The hashes will only match if the document has not been changed and is in exactly the same state as when it was hashed onto the blockchain, thus verifying and ensuring the document's integrity.

This immutable record-keeping functionality could be particularly appealing for a wide variety of legal documents, for verifying intellectual property and, more broadly, for any time-sensitive documents that require verification and time-stamping (traditionally served by notaries). It could also be used as a measure to counter corruption and retain better records for internal purposes within an enterprise or government body.

For example, the Honduran government has explored, via a proof-of-concept, whether Factom's blockchain-based record-keeping service could help counter corruption in the country's land registry—where some officials with access to the land registry awarded themselves premium property unjustly.

Digital Identity

Blockchain technology could provide the infrastructure to scale digital identity at extremely low costs with significant improvements in security. Think of it as next-generation passwords. Given that consumers rely on passwords to access everything from social media to smart-homes to payment verification, the potential use cases for

blockchain-based digital identity services are vast and of increasing importance as digital identity verification becomes a several-times-a-day task.

The technology also has repercussions for businesses and individuals. Previously, reputation and identity systems have been maintained on a site-by-site basis. A seller on Amazon must build up a good reputation by being honest and serving their customers. Unfortunately, that reputation isn't portable. If they want to start selling their goods on eBay, they have to start from scratch to build their reputation. Now, several blockchain-based identity services are providing this service in a highly portable way so that reputation can be established through all honest dealings on the internet.

The advantage for users is that a blockchain-based digital identity service could enable consumers to retain better control of their information (both their payment and identity information), as well as enabling seamless payments (for digital identity services that are tied to a digital wallet). In terms of information control, users will better be able to isolate the personal information they're willing to share with a website by using an independent blockchain-based identity service as opposed to social media accounts. Further, because blockchain-based identity verification services can operate at a fraction of the cost of traditional providers (discussed below), merchants and credit card companies are likely to verify identities more frequently—which consequently reduces the risk of fraud for all honest people that transact on the internet.

For businesses, a blockchain-based digital identity service could facilitate more seamless payments and lower the costs of identity verification. In terms of payments, if a user logs in with a blockchain-based identity service that's tied to a payment method, it eliminates a step (entering payment info) in the transaction process relative to existing identity verification tools (i.e., login with Facebook, LinkedIn (LNKD – Buy), or Twitter), which subsequently require the user to input their payment information and, consequently, increase the probability of cart abandonment. Using a blockchain-based payments service also has the other advantages for merchants (lower processing fees, no chargeback fraud, global access, etc.) that we highlighted in the preceding "payments" section. In terms of cost, blockchain-based identity services can perform the same verification at a lower cost because of the speed, automation, and security provided by blockchain-based providers relative to existing time consuming, and largely manual fraud prevention measures.

To imagine the privacy benefits to consumers, think of the number of times and places that you're asked to provide your social security number—potentially your single most important personal identifier. As the saying goes, the security of your identity is only as strong as the weakest leak, and the more places your social security and other identity information is provided, the more likely hackers or others will be able to access it for nefarious purposes.

A Javelin Strategy & Research report[5] estimates there were 13.1 million fraud victims in 2013. The report estimates that one in three people who received a data breach notification (from a retailer, for example) became an identity fraud victim. The problem is known and being addressed on one side: damage control. While the number of fraud victims rose to 13.1 million (from 12.6 million in 2012), the amount of damage fell by $3 billion to $18 billion, "reflecting more aggressive actions from financial institutions identity theft protection providers and consumers." This data suggests that the industry is successfully tackling the symptoms—but the real challenge is to address the cause. In order to do that, users need to have better control over access to their personal information. Blockchain is one solution that enables users to retain better control of their personal identifying information (PII).

[5] *2014 Identity Fraud Study,* Javelin Strategy & Research (February 2014).

Delivery & Consumption of Media and Professional Services

Blockchain technology brings new possibilities to streaming and the broader media industry in the form of direct-to-consumer, real-time, pay-as-you-go services. This new possibility stems from the peer-to-peer functionality of blockchain technology coupled with the low cost of transacting on a blockchain. The former could disrupt media distribution channels by connecting creators direct to consumers while the latter could enable micropayments and a closer alignment between media consumed and price paid.

In fact, content delivery platforms such as Apple Music and Amazon Kindle are already paying their content creators in this fashion: Apple pays artists based on the number of times users listen to their song and Amazon pays some Kindle authors based on the number of pages that users read. Again, blockchain technology is another extension of the present trend: Users paying according to actual usage metrics. As discussed in the preceding "Payments" section, these fees would be funded via a series of micropayments that are aggregated into a larger payment at the conclusion of a session.

Aside from connecting media creators more directly to consumers, this blockchain functionality could usher in a new era for services offered over the internet. Instead of booking a 30-minute or 60-minute appointment with the doctor (or lawyer or developer or a tutor), which the patient pays for entirely regardless of the amount of the professional's time actually consumed (let alone the opportunity cost of commuting and wait-time), the patient could digitally conference their doctor and pay them directly, but only for the time they actually consume—all via a series of micropayments.

Decentralized Cloud Storage & Data Analysis

To cloud storage, blockchain technology could help facilitate new advantages in efficiency, price, durability security, and longevity. Decentralized, blockchain-based storage companies can leverage existing hardware storage to more securely store data with greater availability at a significantly lower cost. Instead of paying Amazon Web Services (AMZN - Hold), DropBox, or Google Drive to construct and maintain multi-million-dollar data centers, what if you could securely store your files on your neighbor's hard drive? That's the opportunity that decentralized, blockchain-based cloud storage presents.

This model has obvious efficiency and cost-advantages: Leveraging free capacity on hard drives already in existence is naturally more cost effective than building massive new data centers from the ground up. In the same way that RelayRides helps car owners generate income by granting others use of their vehicles, so too can decentralized, blockchain-based cloud storage services help computer owners generate income (however minimal) by allowing others to store files on their excess hard drive space.

Not only could a decentralized, blockchain-based storage service be more cost-effective than existing models, they're likely more secure than existing services as well. That's because mainstream cloud storage services maintain centralized servers where anyone who gets through external security (an admittedly difficult task) has access to complete versions of the documents stored within. In contrast, decentralized, blockchain-based storage services turn this model upside down by replacing expensive security measures with a software protocol. Instead of storing your document in one place, such as your own computer or on Dropbox servers, decentralized, blockchain-based storage providers shred your document into

thousands of pieces then spread those pieces across time zones and continents on hard drive space available to the network.

Your documents are safe on these hard drives too. If the person "renting" their hard drive space tries to access your file, the network identifies them as a "bad" node, shuts them out of the network, and moves your thousandth of a file elsewhere. Each thousandth of a piece is stored with adjustable levels of redundancy—meaning that users can pay more for higher levels of redundancy (for their highest value documents) and lower levels for less-important documents. There's also a speed advantage from such a decentralized system in that data can be simultaneously downloaded from a multitude of redundant locations.

Lastly, decentralized, blockchain-based cloud storage presents longevity advantages. Your files will continue to be stored on the network even as users enlist and delist their hard drive space—the pieces of your document are intelligently moved to other available space. In contrast, if a centralized cloud storage provider went out of business or had all their servers attacked, the documents stored would be lost.

In a way, such decentralized storage systems platforms could induce the unbundling of cloud storage by allowing users to optimize their hosting for the factors that are most important to them: A user that valued speed above all else can pay more to host on providers with faster connections and closer proximity. Alternatively, a user could optimize for cost or security, respectively, by hosting with the lowest cost providers or with higher levels of redundancy and geographic distribution.

Decentralized cloud storage providers estimate they will be able to cut the costs of today's major providers by at least 50%.

Using the same technique as decentralized data storage, so too can businesses leverage blockchain technology to share and analyze data in the cloud without ever revealing the actual data—greatly improving the security, efficiency, and privacy of cloud data analysis. To perform this function, a data set is shredded into thousands of pieces which are encrypted and intelligently distributed across a decentralized network. Analysis is performed on each discrete piece of the overall data set and only the owner can re-aggregate the data and results.

This process keeps the data out of the reach of hackers or surveillance. Another implication is that people and businesses might be more willing to share their data (in light of the fact that they have guaranteed privacy)—a feature which could have profound impact for all data-intensive industries, including pharmaceuticals, healthcare, and advertising. This helps solve a big problem: The ability to leverage the exponentially increasing amounts of data that we generate without sacrificing privacy.

Marketplaces

"The Internet has decentralized communications, and Bitcoin has decentralized money, but online commerce still relies on numerous intermediaries. OpenBazaar removes the intermediaries and gives everyone—individuals to large companies—the ability to directly engage in trade with anyone in the world, for free"

Brian Hoffman, Project Lead, OpenBazaar

Blockchain technology or, more broadly, decentralization could also bring lower costs to digital marketplaces and reduce friction in peer-to-peer exchange. Three main

advantages for sellers and buyers on centralized digital marketplaces like Amazon and eBay (EBAY – Hold) are: 1) reputation establishment; 2) dispute resolution; and 3) payment processing. These are undoubtedly valuable services and, faced with limited alternatives, users have generally been safer and better-off transacting on these platforms. Initially, these centralized platforms compete heavily against one another and race to charge the lowest fees and establish a network effect. However, once established, network effects are inherently difficult to disrupt, allowing the platform to exert leverage over buyers and/or sellers in the form of transaction fees.

However, the three main value-adds of these centralized marketplaces (reputation establishment, dispute resolution, and payment processing) are being challenged by blockchain-based services. We've already outlined the advantages of blockchain-based payments and digital identity services in preceding sections, so here we add the potential advantages of decentralized, blockchain-based dispute resolution services.

Dispute resolution is a fairly simple process: When a dispute arises between buyer and seller, a third party casts a tie-breaking vote between the seller and the buyer as to whether the terms and conditions of the sale were met. Blockchain-based services help lower the cost of this function by creating a global marketplace where anyone can serve as an "escrow agent" and can build and establish their reputation as an escrow agent only by being 'fair.' By removing barriers to entry and creating an open marketplace for escrow agents, blockchain-based services are lowering the cost of dispute resolution itself. (Again, see the preceding sections "digital identity" and "payments" for explanations as to how blockchain technology presents efficiencies in these areas as well.)

Considering that today's centralized marketplaces charge fees of roughly 15% on most transactions (range of roughly 6-45%)[6][7], the gains to be had from a decentralized blockchain-based marketplace are significant: Splitting the fee down the middle, buyers could get a ~7% discount and, simultaneously, sellers could earn ~7% more simply by transacting away from the centralized platform—and the challenges to doing so are being greatly diminished. These benefits (gains of 6-45%) might be sufficient to overcome the network effect of established marketplace providers—especially considering that the typical seller on these marketplaces earns a profit margin of roughly 20-25%[8]. With the opportunity for sellers to significantly boost profit margins and for buyers to earn significant discounts, the gains may also be sufficient to outweigh any initial friction of moving to a decentralized platform.

We don't think that decentralized, blockchain-based marketplaces are going to supplant Amazon or eBay—we believe that these platforms add significant and difficult to replace value for users—but we do believe that blockchain-based services are challenging some of their value-add and margins and that some of the exchange that would have gone through these corridors or stayed offline will migrate toward decentralized marketplaces.

The business opportunity for a decentralized, blockchain-based marketplace isn't in charging for transactions but rather in premium services offered around the marketplace to support buyers and sellers. OpenBazaar is one such decentralized marketplace and has been funded by Andreessen Horowitz and Union Square Ventures to establish their no-fee marketplace. A separate for-profit entity, OB1, is building solutions for the OpenBazaar marketplace that can be monetized.

[6] Amazon Fees and Pricing, https://www.amazon.com/gp/help/customer/display.html?nodeId=1161240.
[7] eBay Selling Fees: http://pages.ebay.com/help/sell/fees.html.
[8] http://www.webretailer.com/lean-commerce/statistics-marketplace-seller-survey/ (August 2014).

Gambling & Gaming

The advantages of blockchain technology for gambling include transparency and disintermediation—meaning that participants can better trust the service they're using and can play with better odds. In terms of transparency, a concern with any gambler is that the game or bets are handled fairly. A decentralized gaming service can be "provably fair" by using a blockchain to execute or publish its logic—thereby enabling anybody (including third-party verification services) to authenticate its fairness. Second, with a minimized role for "the house," all participants can play with better odds which, in turn, induces greater participation.

Growth Drivers and Hurdles

There are a number of important drivers and hurdles that will affect the pace of adoption of blockchain technology. We believe that the current hurdles to growth will be resolved or, at least, will not prevent the proliferation of blockchain technology.

Drivers

Major Enterprise Adoptions

Further enterprise adoptions of blockchain technology, such as Nasdaq's blockchain initiative, are important both for establishing a network effect for blockchain platforms and for public psyche surrounding the technology. As major mainstream businesses launch initiatives to explore and adopt blockchain for their operations, the potential value increases for other organizations—essentially creating a virtuous cycle of adoption. Similarly, technology adoption by major enterprises serves to solidify confidence in the technology in the minds of the public who look to these companies for thought and technology leadership.

The Internet of Things

As described in the applications and use cases section, blockchain technology could be a critical component of the Internet of Things. As the number of connected devices continues to accelerate, a blockchain underpinning could drive rapid blockchain adoption throughout the IoT ecosystem.

Broken Trust

Security breaches have been an increasingly important pain point for businesses and consumers in recent years. High-profile incidents like the breach of Apple's iCloud, which released personal and intimate photos, credit card breaches at Target, Michaels and Neiman Marcus, which released the personal financial information of millions, and even a breach at the IRS that saw the theft of at least 100K social security numbers, birth dates and addresses have permanently affected the trust and perceived security of these organizations. These breaches alone have compromised people's personal and intimate photos, their personal financial information, and their identity information. With this information evidently vulnerable, businesses and consumers alike are seeking solutions to better protect information.

Users in the Driver Seat

Increasingly, and partially in response to data breaches, users are increasingly seeking control of their own data and information. Fundamentally, blockchain technology helps put users in control. For example, in regards to payments, rather than storing payment information with an online merchant (a pull payment), blockchain companies allow users to retain control of their information and allow only one-off access to a specified payment amount (a push payment). In this way, a

user's financial information is never stored with the merchant and not subject to a hacker breach. Other current and potential blockchain-based applications apply this trend to other areas such as digital identity and healthcare records.

A Closer Alignment Between Usage and Cost

Aside from other advantages, part of what has helped propel SaaS (software-as-a-service) companies to new heights is their subscription-based model that more closely ties user costs to usage and value attained. Rather than making massive upfront investments in on-premise software with unproven internal value, SaaS companies allowed businesses to pay for their software on a monthly or yearly basis—essentially de-risking software implementation. Blockchain-based applications are facilitating the natural extension of this trend. Businesses and users can pay in real-time according to usage and value attained. For example, users can pay online publishers according to the number of pages of a news article read, seconds of a song listened to, or minutes of a movie viewed. Blockchain technology facilitates this extension because of its transparency, degree of documentation accuracy and the significantly lower cost of transmitting digital currency (even miniscule amounts) with a blockchain.

Natural Pursuit of Efficiency and Profit

Blockchain technology is radical and disruptive in the efficiencies that can be unleashed from a distributed ledger. Companies seeking to reduce costs and create new functionality will find natural applications in blockchain technology by applying it to their supply chain, to payments, and to other disintermediating operational purposes.

"The blockchain could be an Occam's razor, the most efficient, direct, and natural means of coordinating all human and machine activity; it is a natural efficiency process."

Melanie Swan, Institute for Blockchain Studies

Regulatory Clarity

Regulatory clarity is a significant driver for the industry, as it allows large businesses to formally embrace the technology and for investors to confidently fund the next wave of use cases and applications. Even less-than-ideal regulation such as New York's Bitlicense are (arguably) still good for the industry.

A Rich Ecosystem

A rich ecosystem enables businesses and developers to create new products and services using an array of off-the-shelf, plug-and-play technologies from industry vendors, which significantly reduces the barrier to innovation within the industry. As this ecosystem develops and matures, mainstream adoption will increase as businesses and individuals are more fully able to leverage the security, durability, autonomy, and cost efficiencies of blockchain technology. Based on current investment trends, we believe that this foundational level is being developed rapidly.

Sidechains

Sidechains could be an important catalyst for the broader adoption of blockchain technology because, if successful, sidechains would allow businesses and developers to explore new functionality and blockchain innovation while still leveraging the network effect of the Bitcoin blockchain. This could be an important development for optimizing blockchain technology across many use cases and industries. The leader in

sidechains development, Blockstream recently announced its first production sidechain that will be used by a consortium of exchanges and brokerages to improve capital efficiency and market liquidity in the Bitcoin ecosystem.

Robust & Mature Smart Contracts

While basic smart contract functionality already exists, what is available today only scratches the surface of what will be possible with smart contracts. A robust and mature smart contracts platform would be valuable across many industries and the opportunity to easily code business logic into regular operations could greatly reduce errors and costs in basic operations and, as a byproduct, rapidly accelerate blockchain adoption.

Emerging Markets

There are three critical factors that could drive blockchain adoption in emerging markets businesses: 1) a lack of alternatives; 2) mobile phone access; and 3) a marginal cost advantage.

A lack of alternatives: While blockchain technology presents significant advantages for a broad range of applications, there's a classic problem with technological improvements that they can't just be better—they have to be sufficiently better to get end-users to actually care enough to make a switch. In emerging markets, many of these end-users (individuals and businesses) have fewer, if any, alternatives, for many of the applications that can be efficiently built on blockchain technology and profitably deployed in low-income countries.

Mobile phone access: As with other important technology trends in emerging markets, access to mobile phones could be critical. The majority of people residing in emerging markets are unbanked, but among this unbanked subset, a majority have access to a mobile phone—which could be a critical link to accessing blockchain-based services such as money storage/transfer, and other blockchain-based services.

Marginal cost advantage: Lastly, and most importantly, because of the efficiencies that can be unleashed from blockchain technology, the largely unbanked and more price sensitive populations in the developing world may well be one of the most important growth drivers of blockchain technology. In this respect, we see blockchain technology as important to emerging markets because of the low marginal cost associated with blockchain-based services. The marginal cost is important because it represents a minimum threshold whereby businesses (rationally) elect to avoid countries, markets, and people that are unlikely to meet that minimum threshold. Ultimately, we think that removing or greatly reducing this minimum threshold will have magnanimous implications for bringing the next billion people into ecommerce, digital banking, and other vectors of the digital world.

"The very powerful thing about Bitcoin in general and specially the technologies behind it, is they are essentially leapfrogging all the technology and providing a new system for processing these huge amounts of transactions for very small costs."

Kosta Peric, Deputy Director of Financial Services for the Poor, Bill & Melinda Gates Foundation

Hurdles

The Politics of Bitcoin & Government Regulation

As the first, most popular and most widely referenced application of blockchain technology, Bitcoin is inextricably associated with blockchain technology itself. Because modern currencies have always been created and regulated by national governments, currency itself is an intensely political issue. While it wouldn't be feasible or even possible to completely "shut down" Bitcoin, government regulation could make it prohibitively onerous to access or use. While we think that currency is an interesting application of blockchain technology—and potentially one of the most important—the future of blockchain technology itself does not depend upon Bitcoin. The vast array of apolitical applications of the technology means that we will very likely see the proliferation of use cases independent of the success or absence of Bitcoin.

Broken Trust

We also cited broken trust as a driver of adoption, but blockchain-related companies have not been exempt from data breaches either. Several high-profile cases such as the implosion of the largest Bitcoin exchange (and subsequently revealed historical insolvency), Mt. Gox, have rattled the confidence of Bitcoin and blockchain users. Considering that avoiding these events was what drove a significant number of users to Bitcoin and Blockchain in the first place, these are serious issues and future high-profile incidents could temper broader blockchain adoption. While we recognize this as a risk, we believe that speed bumps such as these are natural to new technologies, that the broader industry is responding to the lessons learned, and that new businesses are being created to avoid these incidents moving forward. Ultimately, we believe that decentralized systems are not systematically vulnerable in the way that centralized services and databases have historically been.

Resolution of Technical Debates

There are a number of issues being actively debated in the developer community of potential shortcomings of the original Bitcoin blockchain, ranging from debates around block size to latency to security and throughput. There is also an ongoing debate as to whether the solution to any of these real or perceived issues is to create new blockchains (and forgo the existing network effect of the Bitcoin blockchain) or to continue developing a way to build adaptable blockchains that are linked to the Bitcoin blockchain (sidechains)—both approaches are being actively pursued in the market today. Only time will tell exactly what the resolutions to these issues will be, but we certainly don't view them as insurmountable or as a blockade to broader blockchain adoption.

Capital Formation

Three Years of Acceleration

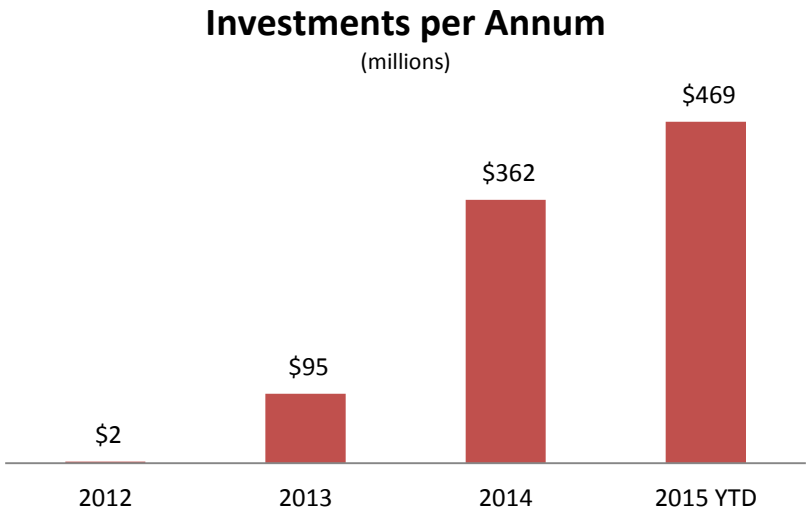
Investment in blockchain-related companies gained initial momentum in 2013 and has accelerated sharply since. The analysis that follows is based on this relatively short timeframe and shows that across all metrics, investments in blockchain-related companies are accelerating. To date, investment has been largely concentrated in companies that we consider to be the first-order benefactors of any mainstream adoption of blockchain technology and digital currencies in particular: These are the companies that have based their businesses around digital currency "wallets,"

payment processing, exchanges, and transaction processing companies. We expect continued investment in this area, and we believe the next leg will see investments in the second-order benefactors of broader blockchain adoption, which we believe includes developer platforms and commercial APIs, among others.

Overall Capital: Small But Growing Rapidly

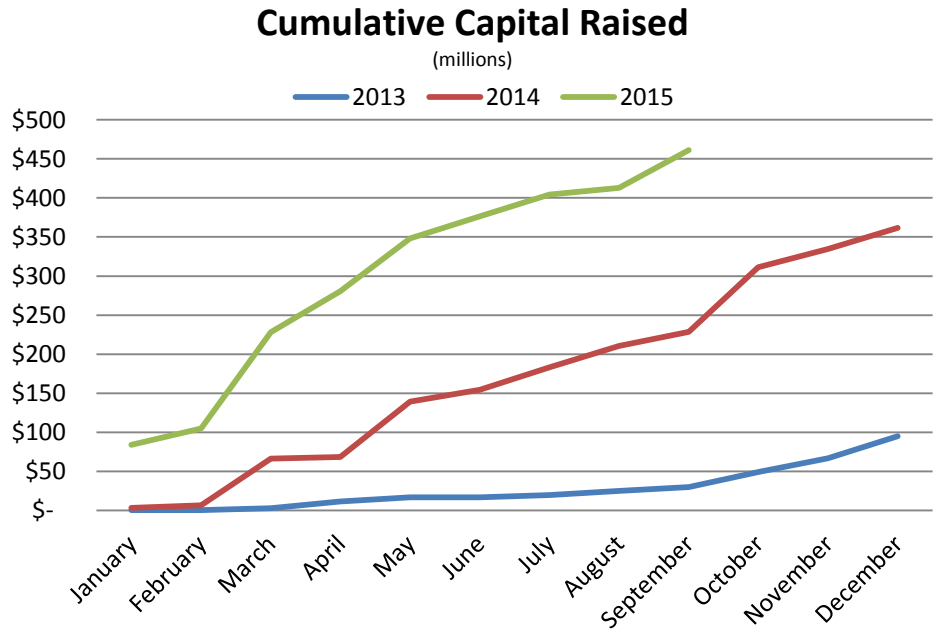
Investments in blockchain-related companies have been growing at a rapid clip over recent years, including year-over-year growth of more than 250% in 2014. With three months left in 2015, blockchain-related companies have already raised $469 million, including the three largest rounds to date from 21, Inc., Coinbase and Circle Internet Financial, which have cumulatively raised more than $240 million in 2015.

Figure 8 Total Capital Raised by Year



Source: CoinDesk, as accessed on 10/12/15.

Figure 9 Capital Raised Over Past Three Years

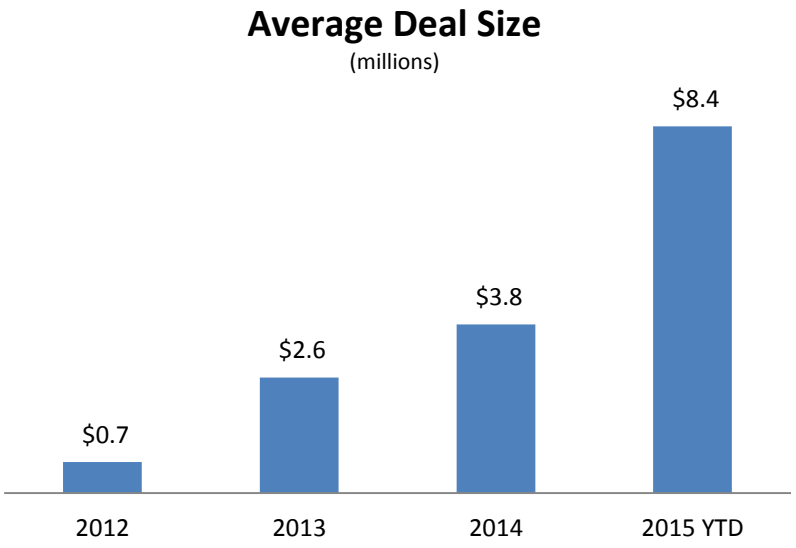


Source: CoinDesk, as accessed on 10/12/15.

Average Deal Size

The average deal size has increased notably over recent years with a particularly sharp uptick thus far in 2015, as 21 Inc. ($116 million round), Coinbase ($75 million round), and Circle ($50 million round) have raised the three largest rounds ever for blockchain-related companies.

Figure 10 Average Deal Size



Source: CoinDesk, as accessed on 10/12/15.

To date, the majority of invested capital has flowed to the companies involved in transaction processing, storage (wallets), exchange, and transmission (payments) of digital assets—the first-order benefactors of broader digital currency and blockchain adoption. We expect continued investments in these types of companies, as this will be valuable real estate to own in the course of any mainstream adoption: All capital will necessarily flow through multiple, if not all, these channels. We believe the next big wave of investments will be focused around the second-order benefactors of broader adoption: The companies that are building developer platforms, commercial APIs, and those that are specifically tackling the clearing and settlement space. Finally, we expect the third big wave of investment capital to be squarely focused on a rich array of end-user applications.

"In as fluid an environment as this one, the value lies in the strategic high ground. We believe that in the Bitcoin ecosystem, the wallet is the strategic high ground. Wallets own the relationship with the consumer and every transaction begins and ends with a wallet."

Lightspeed Venture Partners

"It is naive to assume that the blockchain will make the most impact where it is to be adopted early. Rather, it will make the most impact where change is hardest to achieve, and that might take a little longer, realistically."

William Mougayar, Venture Advisor and Entrepreneur

Investment Opportunities

Given the nascence of the blockchain industry, the investment opportunities that exist today are almost entirely in private markets. The closest pure-play in public markets today is Vogogo (VGO, Not Rated), a risk management and payments services company that works with the many of the world's major Bitcoin exchanges. There are many large publicly traded companies, such as Nasdaq and Overstock, that are implementing, exploring, or investing in blockchain or blockchain-related companies but these initiatives and investments are likely negligible factors for their stock performance in the short term.

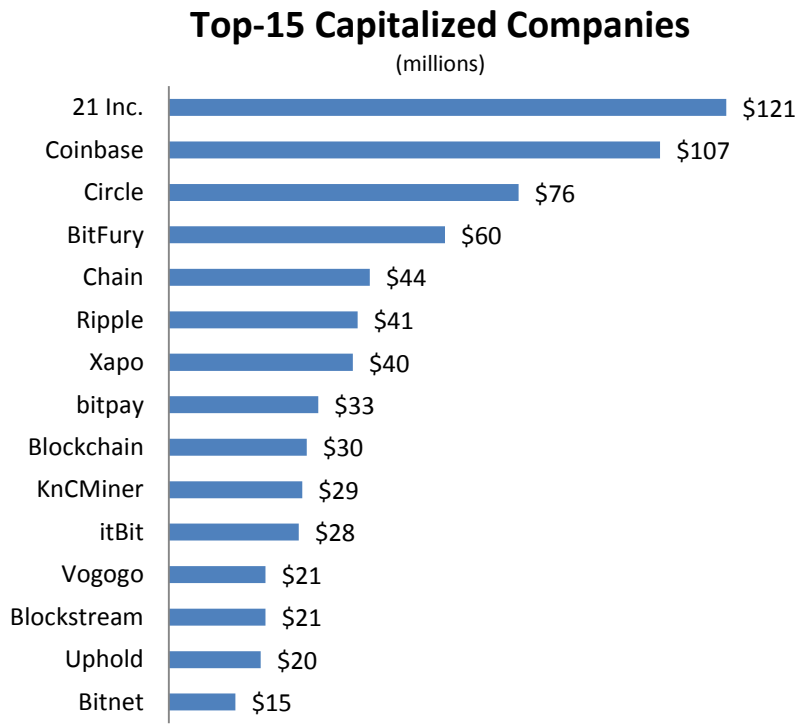
For now, the best way to get direct exposure to blockchain companies is to be an angel investor or to invest alongside venture capital firms that specialize in the industry, such as Blockchain Capital or Pantera Capital. The easiest way to get direct exposure to Bitcoin, in particular, is to simply buy Bitcoin, which can be done through a number of online exchanges—a few of which are profiled in the back of this report.

Best-Capitalized Blockchain-Related Companies

As mentioned before, the bulk of investment capital to date has been focused on the "highways" that will be critical in the event of broader adoption of blockchain technology: Transaction processing, wallets, payments, and exchanges. For more information regarding many of these companies, refer to the profiles at the end of this report.

One notable outlier in this list, and potentially indicative of the oncoming second-wave of blockchain investments, is Blockstream, which, in contrast to the other companies in the top 10, is focused on building "sidechains," which could be an important catalyst for further blockchain development as they allow the freedom to innovate on new blockchains while still leveraging the network effect of the Bitcoin blockchain by using a two-way peg to Bitcoin.

Figure 11 Blockchain Capital Formation



Source: CoinDesk, as accessed on 10/12/15 and Needham & Company, LLC estimates.

Big Names Making Waves in Blockchain

The blockchain industry has attracted legions of the world's foremost entrepreneurs and technology investors, including Peter Thiel, Eric Schmidt, Reid Hoffman, Marc Benioff, Halsey Minor, Richard Branson, Blythe Masters, Larry Summers, Vikram Pandit, John Reed, Marc Andreessen and Tim Draper—among many others. Funding development, at least 7 of the top 10 venture capital firms of 2014 (as ranked by Entrepreneur.com) have invested in the space.

Large financial institutions from traditional banks to exchanges to central banks have taken notice as well. Nasdaq has launched an enterprise-wide blockchain initiative and is working with Chain to implement blockchain technology in their private markets practice to streamline operations and create efficiencies in the documentation, exchange and transfer of pre-IPO shares. Meanwhile, Goldman Sachs, Barclays, RBS, UBS, Visa, Capital One, Citigroup, BNY Mellon, NYSE, USAA, BBVA, Santander and Fiserv have each either made investments in the space or are actively exploring proof of concepts with blockchain service providers. Central banks aren't on the sidelines either: The Bank of England, Monetary Authority of Singapore (Central Bank), and the Federal Reserve are all funding development or fielding inquiries in the industry.

Businesses outside the financial sphere are taking notice too. IBM sees blockchain as an ideal technology for the Internet of Things with advantages in cost, longevity, privacy, and security, and, in partnership with Samsung, is actively building out a blockchain-based platform for the IoT called ADEPT. Separately, IBM is also using blockchain technology to build an open-source smart contracts protocol. Other large corporations such as Qualcomm, Cisco Systems, Samsung, Overstock.com and Seagate Technology have all made investments in the industry as well.

Companies Under Coverage by Needham Mentioned in This Report:
Amazon.com
Cisco Systems
eBay
Facebook
Alphabet/Google
LinkedIn
Seagate Technology

Abra

Status: Private/Venture Backed

HQ: Mountain View, CA

Sub-space(s): Payments

Management Team

Bill Barhydt
CEO

Pete Kelly
VP, Business Development

Financing History

Total Funding: $14MM

Seed: $2MM (March 2015)
Silicon Badia

Series A: $12MM (September 2015)
Arbor Ventures, Carthona Capital
First Round, RRE Ventures

Abra Overview

Abra's mission is to make cash mobile. The company's peer-to-peer money transfer network enables convenient, instant, secure, money movement without transfer fees. While Abra uses Bitcoin on the backend as a payment rail, the user experience is entirely fiat based, so users can take advantage of the efficiencies of Bitcoin without the volatility or complexity.

Just as Uber utilizes a network of drivers for access to transportation, Abra utilizes on a network of human ATMs—Abra Tellers—to provide access to cash. The tellers earn money by buying and selling digital money to Abra users so, for example, someone with $200 in their pocket can instantly make cash available to their cousin on the other side of the country. They do this by using an Abra teller to convert their hard cash to digital money, which they send to their cousin who then finds a nearby Abra teller to pull the cash out—all without involving a bank or intermediary.

While Abra's functionality is particularly appealing to the world's unbanked population and in cash-based economies, it's also potentially helpful for anyone who uses cash. For example, while on a cruise, Abra could help a user easily acquire local currency each time they step off the boat. Teller supply consists of individuals that earn income as mobile ATMs and local businesses that leverage their storefronts to generate extra income by becoming tellers on the Abra network.

While transfer on the Abra network is fee, the company monetizes its peer-to-peer money transfer network by charging tellers a fee for facilitating the transaction. The company also charges a convenience fee for exchanging from one currency to another and a merchant fee for businesses that execute a purchase through the Abra API.

Abra is focused on building a deep network of tellers in each market that it is entering and on building awareness for the application. The company will first be focused on North America, Southeast Asia, and Latin America.

BitFury

Status: Private/Venture Backed

HQ: San Francisco, CA

Sub-space: Transaction Processing

Management Team

Valery Vavilov
Founder & CEO

Valery Nebesny
Founder & CTO

Steven Eliscu
Sr. Director of Finance & IR

Financing History

Total Funding: $60MM

Series A: $20MM
Bill Tai, Binary Financial, Blockchain Capital, Jonathan Teo, Queensbridge Venture Partners, ZAD Investments

Series A: $20MM
Bill Tai, Bob Dykes, Georgian Co-Investment Fund, Lars Rasmussen

Series B: $20MM
DRW Trading Group, Georgian Co-Investment Fund, iTech Capital

BitFury Overview

BitFury is the world's largest private Bitcoin transaction processor, as the company processes roughly 15% of total Bitcoin transactions. BitFury is analogous to the Visa of Bitcoin and is going after what could eventually be a similarly sized market.

As a transaction processor, BitFury is unique among blockchain-related companies in that in order to generate revenue, the company simply manufactures compute power, points that compute power at the Bitcoin network through one of its data centers, processes transactions, and collects the associated revenue (coinbase reward and transaction fees)—without the hassle of extensive sales, marketing, and other customer acquisition efforts. As the most-funded Bitcoin transaction processor, BitFury is particularly well-positioned in the transaction-processing space, where success depends heavily upon capital-intensive research efforts to develop the most efficient technology and the most efficient data centers.

BitFury's business strategy is relatively straightforward: Develop the most efficient technology, build efficient data centers, and process transactions. We estimate that over the past six months, BitFury has been trending toward an annual revenue run-rate of roughly $35-45 million. BitFury is in the process of building out and manufacturing their latest advancement: a 16nm chip that will achieve efficiency of 0.06 joules per gigahash—which should be live in some data centers around the middle of 2016. The new chips, coupled with a new 100mw data center in the country Georgia and another new data center in North America, could help boost BitFury's relative share of compute power on the Bitcoin network—the single most important factor for increasing the company's share of transaction processing revenue.

At a price of $250 per Bitcoin, transaction processing is worth roughly $335MM in annual revenue; therefore, if BitFury were to increase its share of the global Bitcoin network hash rate from 14% to 20%, for example, the company would generate roughly $20MM of incremental revenue per year.

BitGo

Status: Private/Venture Backed

HQ: Palo Alto, CA

Sub-space(s): Wallet, Platform

Management Team

Mike Belshe
CEO & Co-Founder

Ben Davenport
CTO & Co-Founder

Financing History

Total Funding: $14MM

Series A: $14MM (June 2014)
Redpoint Ventures, A-Grade Investments, Bill Lee, Blockchain Capital, Bridgescale Partners, Digital Currency Group, Eric Hahn, Founders Fund, Jeffrey S. Skoll, Liberty City Ventures, Radar Partners

BitGo Overview

BitGo is the world's leading digital asset security platform with a majority share of the P2SH multi-sig wallet market. BitGo's multi-sig wallet eliminates any single point of vulnerability and thereby enables businesses and consumers to transact with confidence. The company has never suffered a breach since its 2013 inception—a particularly impressive statistic considering that the firm recently announced that it transacted over $1 billion in a single quarter. BitGo's platform API makes it easy for anyone developing a Bitcoin application to integrate P2SH multi-sig security.

In the world of Bitcoin wallets, P2SH multi-sig wallets present an alternative to traditional client-side wallets and web-wallets. In a client-side wallet, the user manages their own access information for their Bitcoin address—but if the user's computer is hacked, crashes or the user loses their information, they could lose their funds. In a web wallet, users outsource the management of this information to a web service—but if the web service is hacked or gets shut down, the user could lose their funds. In contrast, a BitGo P2SH multi-sig wallet distributed keys among multiple participants to remove any single point of failure inherent in other wallets.

BitGo also has a transparency-as-a-service offering ('Verified by BitGo') that allows clients to show their customers that they, in fact, have the funds that they say they do. For example, ChangeTip uses this proof-of-solvency service to show their customers that ChangeTip's assets exceed its liabilities at any given time.

For now, BitGo's target market includes any company that is transacting Bitcoin and especially those that allow users to transact with Bitcoin. BitGo's customers include some of the biggest Bitcoin exchanges in the world, such as BitStamp and Bitfinex. The company offers its platform API on a freemium model with stronger service level agreements and support for premium tiers.

Bitnet

Status: Private/Venture Backed

HQ: Belfast, N. Ireland

Sub-space(s): Payments, Platform

Management Team

John McDonnell
Co-Founder & CEO

Stephen McNamara
Co-Founder & CTO

Brendan Smyth
Chief Operating Officer

Financing History

Total Funding: $14.5MM

Series A: $14.5MM (October 2014)
Highland Capital Partners, ARTIS Ventures, Bill McKiernan, Blockchain Capital, Buchanan Investments, Commerce Ventures, Digital Currency Group, James Pallotta, Rakuten, Stephens Investment Management, Stuart Peterson, Webb Investment Network, WSM Capital LLC

Bitnet Overview

Bitnet is a digital commerce platform that is hyper-focused on enabling merchants to confidently and securely accept payments. The company is focused on helping merchants accept Bitcoin payments because of the strong value proposition for merchants, which includes drastically lower transaction fees, guaranteed payment (no chargebacks), the opportunity to open their business to incoming payments from anywhere in the world without cross-border fees, and the decreased security risk that arises from push payment types such as Bitcoin. Much of Bitnet's team came from Visa, where they witnessed the rising complexity, effort, and expenses associated with connecting the world's disparate payment networks. As a result, Bitnet is leveraging the significantly less expensive Bitcoin blockchain payments network and building a service layer that allows merchants to accept Bitcoin and receive payments in their currency of choice without touching Bitcoin or dealing with any of the volatility or other complexities associated with the digital currency.

Bitnet's business is enabled by the fact that their underlying cost, the Bitcoin payment network, is significantly more efficient than traditional payments networks that rely on expensive intermediaries and interconnectivity solutions. Bitnet targets mostly upstream PSPs but has partners and customers across the payments ecosystem, including retailing giant Rakuten (also a strategic investor), platform-as-a-service provider Pay.on, airlines payment network UATP, as well as others such as Zooz and Computop. Bitnet's commerce platform is broadly applicable to all merchants engaged in ecommerce but has particular appeal for merchants whose business is inherently cross-border such as airlines, hospitality, and some marketplaces. Bitnet monetizes their enterprise commerce platform through a revenue-share model with partners.

Moving forward, Bitnet is particularly interested in releasing solutions that extend the benefits of accepting digital currencies to other payment channels and in providing a service layer for adjacent opportunities in the merchant-consumer relationship such as rewards and loyalty services.

BitPay

Status: Private/Venture Backed

HQ: Atlanta, GA

Sub-space(s): Payments, Platform

Management Team

Stephen Pair
Co-Founder, CEO

Tony Gallippi
Co-Founder, Executive Chairman

Bryan Krohn
Chief Financial Officer

Tim Byun
Chief Compliance Officer

Sonny Singh
Chief Commercial Officer

Financing History

Total Funding: $32.7MM

Seed: $2.7MM (May 2013)
Founders Fund

Series A: $30MM (May 2014)
AME Cloud Ventures, Felicis Ventures, Founders Fund, Horizons Ventures, Richard Branson, RRE Ventures, TTV Capital

BitPay Overview

BitPay is a payment processor that helps businesses accept Bitcoin payments. BitPay makes it easy for merchants to add another payment channel to their business and, importantly, merchants get the benefits of this additional channel without the complexity or volatility Bitcoin. BitPay deposits funds directly into the merchant's bank account in the currency of their choice.

Aside from adding an incoming payment option to their channel, merchants reap other benefits from using BitPay. First, BitPay passes along the efficiencies realized by Bitcoin and charges a 1% fee, which is significantly better than the traditional 3% cost of accepting credit cards. Second, by accepting Bitcoin, the merchant immediately opens their business to customers worldwide. Third, merchants avoid shouldering the risk of chargeback fraud that they otherwise bear with traditional credit and debit payment options. Lastly, the nature of Bitcoin payments is such that the merchant doesn't need to store their customer's financial information to receive payment in the way that they ordinarily do with traditional payment channels—thereby alleviating data security costs and the risk of identity theft.

In February 2015, BitPay surpassed 60K merchants that are BitPay-enabled to accept Bitcoin. BitPay's merchant customers include everything from small businesses to enterprise heavyweights, such as Microsoft, Newegg, Gyft, TigerDirect.com, and Virgin Galactic. BitPay partners with some of the most popular e-commerce platforms and point-of-sale systems to make reliable, ready-to-deploy integrations. It has over 40 integrations across open source plugins, point-of-sale systems, billing and accounting systems, donations solutions, and integrated solutions that include Shopify, PayPal, Demandware, Magento, and NationBuilder.

BitPay operates on a three-tier pricing plan: a free Starter plan that has transaction and volume limits, a business plan that has a 1% service fee, and an enterprise tier that comes with premium support and additional settlement options.

Blockchain

Status: Private/Venture Backed

HQ: London, UK

Sub-space(s): Wallet, Data Provider, Payments, Platform

Management Team

Peter Smith
CEO & Co-Founder

Ben Reeves
CTO & Co-Founder

Nicolas Cary
Co-Founder

Financing History

Total Funding: $30MM

Seed: $30MM (October 2014)
Lightspeed Venture Partners, Wicklow Capital, Prudence Holdings, Mosaic Ventures, Amit Jhawar, Future Perfect Ventures, Nat Brown, Rafael Corrales, Sir Richard Branson, and more

Blockchain Overview

Blockchain is one of the oldest and most established companies in the relatively young Bitcoin ecosystem. It builds software that makes using Bitcoin safe, easy and secure for consumers and businesses around the world. The company claims to be the world's most popular Bitcoin wallet, to have the world's most widely used Bitcoin APIs, and has grown from 100,000 users a couple of years ago to over 4.5 million. Blockchain's users cumulatively conduct more than 65,000 transactions daily and can use the Blockchain wallet to locate nearby businesses that accept Bitcoin. The firm is adding over 70,000 new wallets a week.

With their Blockchain Merchant product, the company also makes it easy for businesses to accept Bitcoin payments. In addition to their Blockchain.com domain, the company also operates Blockchain.info, which it claims is the most popular block explorer in service and the most highly trafficked Bitcoin website in general. Leveraging the inherent transparency of the Bitcoin blockchain, the site offers data on recent transactions, mined blocks in the blockchain, and volume statistics, among other datapoints.

Blockchain has made two acquisitions: 1) RTBTC.com, which offered a real-time unified trading platform with access to multiple Bitcoin exchanges; and 2) ZeroBlock, which offers a real-time market data and aggregated news feed for everything Bitcoin.

Blockchain raised $30 million in a Series A round with major investors, including Sir Richard Branson, Lightspeed Venture Partners, and Wicklow Capital.

BlockCypher

Status: Private/Venture Backed

HQ: Redwood City, CA

Sub-space(s): Platform, Software Infrastructure

Management Team

Catheryne Nicholson
Co-Founder & CEO

Matthieu Riou
Co-Founder & CTO

Financing History

Total Funding: $3.1MM

Seed: $3.1MM (January 2014)
500 Startups, AME Cloud Ventures, Blockchain Capital, Boost VC, Fenox Venture Capital, Foundation Capital, Granite Ventures, Jesse Draper, Ken Goldman, Michael Liou, New Enterprise Associates, Queensbridge Venture Partners, Sanjiva Weerawarana, Shawn Byers, Streamlined Ventures TriplePoint Capital, Upside Partnership, Voylet Capital

BlockCypher Overview

BlockCypher is a blockchain software infrastructure company that helps companies easily build applications using simple web APIs. BlockCypher built a blockchain-agnostic infrastructure fabric from the ground up. It supports multiple blockchains, including their own proprietary private blockchain used for sandbox testing. Their cloud-optimized infrastructure is modular and enterprise-grade with 99.99+% uptimes, linear scaling, and no single point of failure.

Key BlockCypher features help developers build complex blockchain applications in as quickly as a few days. Its Confidence Factor helps companies accept and process unconfirmed transactions in less than 10 seconds. Other important web services include an Asset API to handle assets on a blockchain, a Data Endpoint which can be used to embed data or a hash on a blockchain, a Fee Endpoint which adaptively calculates transaction fees, a Microtransaction API that enables micropayments, and other important features such as an Address Wallet API, Multisig API, Payment Forwarding API, Transaction API, WebHooks and WebSockets. All these web services apply to all blockchains that BlockCypher hosts. BlockCypher also offers sandboxes for institutions to build proprietary applications. BlockCypher provides its solutions through service level agreements based on the scope of work, usage volume, and uptime guarantees.

BlockCypher is squarely focused on the developer community building blockchain applications, both currency and non-currency related. That market has been shifting toward large enterprises, especially financial institutions that are increasingly interested in building their own blockchain applications. BlockCypher counts many of the most well-known companies in the blockchain space among its customer base including Coinbase, Xapo, Bitnet, Abra, Gem, ShapeShift and many non-currency related companies such as OneName, Stampery, and ShoCard.

With BlockCypher's considerable traction, the company plans to continue down the path they've laid and work with developers, established blockchain companies, new ventures, and large financial institutions.

Chain

Status: Private/Venture Backed

HQ: San Francisco, CA

Sub-space: Clearing and Settlement, Federated Blockchains, Platform, Software

Management Team

Adam Ludwin
Founder

Devon Gundry
Founder

Financing History

Total Funding: $43.7MM

Seed: $4.2MM
Betaworks, RRE Ventures, SV Angel, Thrive Capital

Series A: $9.5MM
Khosla Ventures, 500 Startups, Barry Silbert, Blockchain Capital, Homebrew, Kevin Ryan, Pantera Capital, RRE Ventures, Scott Banister, SV Angel, Thrive Capital

Series B: $30MM
Capital One, Citi Ventures, Fiserv, Nasdaq, Orange, Visa

Chain Overview

Chain is an enterprise blockchain platform that is helping large financial institutions build the systems and networks to move and exchange assets over the internet without an intermediary. Chain is focused on helping its large financial institution partners revolutionize the way that securities of any kind are traded and settled—potentially taking the clearing and settlement of securities from the T+3 timeframe to nearly instantaneous as large financial institutions and other enterprises move toward a system where they settle and exchange directly with one another.

For example, Chain is currently working with Nasdaq's private markets unit to implement blockchain technology to facilitate the frictionless trading of pre-IPO equity shares. However, private equity shares are only the tip of the iceberg: Chain's solutions can be optimized for issuing and exchanging anything from other financial securities (bonds, derivatives, currencies, etc.) to energy credits to gift cards to mobile minutes. Chain is addressing each of these markets.

In the same way that the APIs of Stripe, Twilio, and Heroku make it easy to accept payments online, communicate through the cloud, and build cloud applications, so too do Chain's APIs make it easy to build blockchain solutions for any number of use-cases. Chain's target market includes most large financial institutions—many of which see blockchain technology as a rare opportunity to reshape and drastically improve financial markets. In general, Chain sees blockchain technology as optimal for markets where there are many (and changing) entities that are regularly exchanging different types of assets. Alongside current engagements with Nasdaq and First Data, Chain is also working with strategic backers, including Visa, Capital One, Fiserv, Orange and others.

Chain plans to work with dozens of large financial institutions to implement blockchain solutions for a variety of use cases as we head toward a world where most or all assets are either issued digitally or have a digital title. Ultimately, the company thinks that we'll see a world with many blockchains with considerable interoperability between them.

ChangeTip

Status: Private/Venture Backed

HQ: San Francisco, CA

Sub-space(s): Micropayments, Platform

Management Team

Nick Sullivan
Founder and CEO

John Q. Smith
COO

Financing History

Total Funding: $4.3MM

Seed: $4.3MM (April, May, Dec 2014)
BOLDstart Ventures, Blockchain Capital, 500 Startups, Galvanize Ventures, Plug & Play Ventures, Transmedia Capital, Patnera Capital

ChangeTip Overview

ChangeTip is a micropayments company that is enabling people to send online tips to their favorite content creators, causes, and friends seamlessly on social media. Microtransacting is a relatively new payments functionality that is enabled by blockchain technology and Bitcoin: Before blockchain-enabled digital currencies like Bitcoin, the fees associated with very small online payments were prohibitively expensive to justify the small amount sent. ChangeTip has created a service that makes it just as easy to tip someone online as it is to tip a musician on the street or a particularly helpful clerk at the store.

The company tries to be everywhere that tip-worthy content would be so that users can tip seamlessly without interrupting the flow of their internet browsing. ChangeTip makes it as easy to tip someone online as it is to hit a "Like" button or to "Share" something. ChangeTip allows users to tip on Facebook, YouTube, Twitter, WordPress, Twitch, Tumblr, Soundcloud, Slack, Reddit, StockTwits, GitHub, and Disqus.

To send a tip to someone on Twitter, for example, a user simply tweets the person's handle, how much they want to send ($0.01-25.00) and includes @ChangeTip in the tweet. ChangeTip's bots automatically recognizes the payment, deducts the amount from the sending account and deposits it in the receiver's account. ChangeTip makes the experience fun to use by offering standard and custom monikers so that instead of a user sending "$1" they can use a moniker such as "a beer" (which represents $3.50), a cookie ($1.50), any other moniker and value that they designate.

More than just an easy way to send small amounts of money online, ChangeTip could change the incentives for content creators online and completely change how users experience and pay for digital content. For creators, rather than focus on maximizing page views to generate income, creators could instead focus on creating the highest quality (and most tippable) content. For users, rather than paying for content by watching an ad, the user could instead leverage micropayments to avoid ads and enjoy a better viewing experience.

Circle

Status: Private/Venture Backed
HQ: Boston, MA
Sub-space(s): Payments, Wallet

Management Team

Jeremy Allaire
Founder, Chairman & CEO

Sean Neville
Co-Founder & President of Product and Operations

John Beccia
General Counsel & CCO

Paul Camp
CFO, Treasurer, EVP Financial Operations

Financing History

Total Funding: $76MM

Series A: $9MM (October 2013)
Accel Partners, General Catalyst Partners, Jim Breyer

Series B: $17MM (March 2014)
Accel Partners, Fenway Summer LLC, General Catalyst Partners, Leonard Schrank, Michele Burns, Oak Investment Partners, Pantera Capital

Series C: $50MM (April 2015)
Accel Partners, General Catalyst Partners, Goldman Sachs, Oak Investment Partners, Pantera Capital

Circle Overview

Circle is an internet-based consumer finance company focused on transforming retail and consumer banking products, and how people store and use money on a day-to-day basis. Circle is building a product with utility value for the average person on the street that uses money. It is embracing a classic consumer internet strategy: Take something that pre-internet was siloed and proprietary and make it open and free with an application that is highly engaging and, in this case, makes money more enjoyable.

In the same way that traditional media was disrupted and had its future in the open protocols that became the internet, Circle sees the future of money and value exchange as based around open protocols for value transfer. In this respect and in contrast to legacy consumer finance services, Circle wants to be plugged into this open network of value exchange rather than create a walled garden that siloes consumers and value. With respect to the core of consumer finance and retail banking—current accounts—which provide two specific functions, storing value and making it easy to use (via debit cards and internet banking, for example), Circle believes that in a world of cloud-based services, mobile applications, and blockchain value transfer protocols, this core service inevitably becomes a free utility on the internet. Circle wants to be the provider of choice for that free utility.

The company's vision is to make sending and receiving value over the internet as easy as sending photos or opinions on the internet. Just as consumers today expect that sending content over the internet is instant (regardless of arbitrary borders) and free, Circle believes that consumers will increasingly have the same expectations for value transfer on the internet. It recently added U.S. Dollars to its platform and will expand to other currencies while continuing to use Bitcoin on the backend for its efficiencies. Circle is one of the best-funded companies in the blockchain ecosystem and includes heavyweight backers such as Goldman Sachs and IDG Capital Partners. Armed with a strong balance sheet and quality backers, Circle is focused on amassing and delighting a large user-base and expanding internationally.

Coinbase

Status: Private/Venture Backed

HQ: San Francisco, CA

Sub-space(s): Exchange, Wallet, Payments, Platform

Management Team

Brian Armstrong
Founder & CEO

Fred Ehrsam
Co-Founder

Adam White
VP, Business Development & Strategy

Financing History

Total Funding: $106.7MM

Series A: $6.1MM
Bobby Goodlatte, FundersClub, Interplay Ventures, Red Swan Ventures, Ribbit Capital, SV Angel, Union Square Ventures

Series B: $25MM
Andreessen Horowitz, Anthony Saleh, QueensBridge Venture Partners, Ribbit Capital, Union Square Ventures

Series C: $75MM
DFJ, Andreessen Horowitz, BBVA Ventures, Blockchain Capital, NYSE, Ribbit Capital, Union Square Ventures, USAA, Valor Capital Group, Vayner/RSE

Coinbase Overview

Coinbase's goal is to make it as easy as possible for users to buy, store, and use Bitcoin. The company has a wallet service for users to store Bitcoin, an exchange for users to acquire Bitcoin, and a developer platform that, among other things, helps merchants accept Bitcoin. More than 40,000 merchants use the Coinbase platform to accept Bitcoin and 2.6 million users have created 4 million wallets with Coinbase. In addition to its retail Bitcoin conversion service, the company launched an institutional exchange in January, which quickly helped Coinbase surpass $2.5 billion in exchange volume.

The company is strategically positioned at an important onramp to the world of blockchain and digital currencies: Whatever innovative use cases may arise in the future, nearly everyone will need to buy, sell, and store Bitcoin (or another digital currency/asset)—and Coinbase is well-positioned to offer these and ancillary services. In addition to the company's 2.5 million users, it has an impressive stable of enterprise customers that use the Coinbase platform to accept Bitcoin in their businesses, including Expedia, Intuit, Wikimedia, Overstock.com, Dish Network, and many others. Coinbase also has several major partnerships with payment processors, such as PayPal and Stripe, as well as with large financial institutions, such as BBVA and USAA.

Coinbase monetizes its platform by charging customers a fee to exchange fiat currency for Bitcoin. Depending on volume, fees are between 0.10% and 0.25% on the Coinbase exchange and 1% for retail conversion. As more companies use the Coinbase platform to develop other Bitcoin and blockchain-based applications, the company could have several potential sources of revenue.

Coinbase plans to continue expanding internationally (from 30 countries to ~40 by year end, including Latin America and parts of Southeast Asia), to continue maintaining and improving their robust compliance and AML/KYC management, and to develop more strategic partnerships with key stakeholders in the digital currency and payments ecosystems.

Digital Asset Holdings

Digital Asset Holdings

Status: Private

Sub-space(s): Clearing and Settlement, Software, Private & Public Blockchains

Management Team

Blythe Masters
CEO

Donald Wilson
Co-Founder & Board Member

Sunil Hirani
Co-Founder & Board Member

Yuval Rooz
COO

Shaul Kfir
CTO

Dan O'Prey
CMO

Eric Saraniecki
Head of Product

Digital Asset Holdings Overview

Digital Asset Holdings is a software company that utilizes modern cryptographic techniques and blockchain technology to provide enhanced asset settlement and cognizance solutions to financial institutions. The problem that Digital Asset solves is that legacy financial infrastructure is expensive, inefficient, and subject to operational failure. Digital Asset helps solve these problems by using blockchain technology to upgrade existing market infrastructure and bring significant reductions in settlement time. Digital Asset is helmed by a veteran team of Wall Street and technology experts with significant insight into resolving the critical challenges of implementing a blockchain solution for clearing and settlement.

Digital Asset aims to partner with and help incumbent financial intermediaries gain efficiency by leveraging Digital Asset's software. The company's solutions are built to tackle difficult real-world problems of implementing and using a blockchain for clearing and settlement such as on- and off-ramps to a particular blockchain for digital assets that were issued and may be traded off-blockchain. Digital Asset's software is designed to keep transactions private and, when required, to facilitate net settlement.

As a company, Digital Asset is blockchain-agnostic in that its solutions can be used to record transactions on different types of blockchains, including the Bitcoin blockchain and the company's open-source permissioned Hyperledger blockchain. However, due to current limitations of the Bitcoin blockchain and the needs of the company's target market, the majority of Digital Asset's solutions use private permissioned blockchains where participants are known.

Digital Asset's target market and customers encompass all the major stakeholders for clearing and settlement, including banks, dealers, exchanges, central securities depositories, custodians, and central clearing counterparties. The company's solutions are applicable across many use cases, including loans, securities, derivatives, and FX.

Factom

Status: Private

HQ: Austin, TX

Sub-space(s): Data Management

Management Team

Paul Snow
CEO & Lead Developer

Peter Kirby
Founder & President

David Johnston
Chairman of the Board

Jack Lu
Chief Technology Officer

Brian Deery
Chief Scientist

Abhi Dobhal
VP of Business Development

Financing History

Total Funding: $1.1MM

Seed: $1.1MM (July 2015)
David Cohen, First Step Fund, Resonant Venture Partners, VegasTechFund

Factom Overview

Factom's solutions can be used to secure the world's data. The company offers businesses a blockchain-based data layer to record and store information. Factom's software solutions are appealing because they facilitate tamper-proof record keeping by storing small amounts of information or hashes of information onto the Bitcoin blockchain, thereby creating immutable audit trails—functionality that is particularly ideal for companies with strict compliance requirements. By storing hashes of a document onto the blockchain, a customer can later prove that a document existed in a particular state at a point in time. Later versions of the document can be linked to the original to provide a verifiable record of changes to the document. This process can be used beyond documents for other types of media, such as photos and videos.

The government of Honduras, for example, has engaged Factom for a proof-of-concept to see if the company's immutable data layer could help resolve issues with centralized government record-keeping—namely that officials with access to land title records have awarded themselves premium property unjustly.

To circumvent throughput and processing time constraints, Factom first uses its own blockchain to aggregate incoming data hashes then ultimately secures them on the Bitcoin blockchain, which provides the highest level of blockchain immutability and security. This process allows Factom to immutably record millions of documents in a single hash roughly every 10 minutes.

Factom operates on a SaaS model, where pricing is based on the amount of records written to the blockchain. Factom's blockchain-based immutable data layer could be appealing to a broad range of industry verticals, including financial, medical, and legal records.

Filament

Status: Private/Venture Backed

HQ: Reno, NV

Sub-space(s): Internet of Things, Industrial Mesh Networking

Management Team

Eric Jennings
Co-Founder & CEO

Jeremie Miller
CTO

Jake Ingman
Head of Product

Bud Raymor
Head of Finance

Nora Laitinen
Head of Operations

Nate Ashley
Business Development

Financing History

Total Funding: $6MM

Seed: $1MM (August 2014)
David Cohen, First Step Fund, Resonant Venture Partners, VegasTechFund

Series A: $5MM (August 2015)
Bullpen Capital, Crosslink Capital, Digital Currency Group, Haystack, Samsung Ventures, Techstars, Verizon Ventures, Working Lab Capital

Filament Overview

Filament is an industrial mesh networking company that helps companies across verticals connect their legacy infrastructure without a cell or WiFi connection. Filament's customers have a common problem: They want to embrace the Internet of Things and realize the safety and efficiency benefits of connected devices but are stuck with "dumb" legacy industrial infrastructure that wasn't manufactured for connectivity. Filament helps those companies connect that infrastructure. Filament's products are enabling a decentralized Internet of Things, whereby devices are fully autonomous in that they can find and interact with each other and transact value directly machine-to-machine without any intermediary.

Filament has two main products: Taps and Patch. Taps are standalone devices with a battery life of up to 20 years that enable a piece of industrial infrastructure to communicate with another device at a range of up to 10 miles (without cell or WiFi). Taps are designed to be deployable on any given piece of infrastructure in around two minutes. Patch is the brain of Tap without all the hardware and is designed so third-party companies can embed Patch directly in their products—such as a tractor, for example. Filament uses blockchain technology for three main purposes in their products: device identity, smart contract functionality, and micropayments.

Filament is horizontally focused across all verticals that have legacy industrial infrastructure. Sectors like utilities, mining, and oil and gas, which have significant industrial infrastructure that would benefit significantly from connectivity, are particularly prime markets for Filament's solutions.

Filament sells its products via a subscription, sensor-as-a-service model. The devices have smart contract functionality built-in which causes the device to enter a reduced service mode (similar to a cell phone) if the subscription is not paid. This functionality also allows Tap users to monetize their sensor with their own customers paying a subscription for access to data generated. The BLE-enabled devices allow anyone with a Bluetooth capable phone to pay the device directly.

Guardtime

Status: Private
HQ: Tallinn, Estonia
Sub-space(s): Data Security
Competitors: Factom

Management Team

Mike Gault
CEO

Matthew Johnson
CTO

David Hamilton
President, Guardtime Federal

Herb Kelsey
Chief Architect

Minerva Rodriguez
SVP Engineering

Tony Kenyon
CTO EMEA

Martin Ruubel
VP Alliances

Jamie Steiner
Director, Business Development

Guardtime Overview

Guardtime is a systems engineering company that is using blockchain technology to build cryptographic applications that guarantee the integrity of systems. Founded seven years ago, the company counts Ericsson, Lockheed Martin, and Raytheon among its growing list of channel partners.

Within the CIA triad (confidentiality, integrity, availability) of data security, Guardtime focuses explicitly on the integrity aspect. Guardtime verifies integrity by registering components of the software supply chain into the blockchain giving companies resolution and verification of their networks, systems, and data down to the second. For example, in a typical breach, the attention quickly focuses on what data was accessed or stolen—but rarely can anyone answer the equally important question: What if something was added or changed? What if a new person with high-level authorization was added to a personnel database? Guardtime's solutions make it easy to answer these questions in real-time. Far from immature, Guardtime's solutions have been battle-tested for more than five years by government and financial institutions that use the solutions as an early detection system for breaches. The company has also produced a quantum-immune alternative to RSA called BLT that could become the new underpinning of internet security.

In addition to the defense and communications industries, Guardtime's solutions are also ideal for financial services, the internet of things software supply chain, and for AML/KYC purposes. Guardtime is scaling up its operations to address this massive market opportunity. Its business model is to work with channel partners to license their full-stack infrastructure and integrate Guardtime technology directly into third-party products.

Over the next year or two, Guardtime will be working with channel partners to further adoption of current solutions and will continue working with partners to develop new solutions and exploring other blockchain-based opportunities.

itBit

Status: Private/Venture Backed

HQ: New York, NY

Sub-space(s): Exchange, Clearing & Settlement, Private Blockchain, Software, Platform

Management Team

Charles Cascarilla
CEO & Co-Founder

Andrew Chang
COO

Richmond Teo
CEO of Asia & Co-Founder

Kim Petry
CFO

Financing History

Total Funding: $32.5MM

Seed: $3.3MM (November 2013)
Canaan Partners, RRE Ventures, Ben Davenport, Jay W. Jordan II, Liberty City Ventures

Series A: $25MM (May 2015)
Blockchain Capital, James Pallotta, Jay W. Jordan II, Liberty City Ventures, Raptor Capital Management, RRE Ventures, Solon Mack Capital

itBit Overview

itBit's vision is for people to be able to trade any asset, anytime, from anywhere. itBit launched its international Bitcoin exchange in November 2013, and launched domestically in May 2015 after being awarded their Trust Company charter. More recently, the company has been particularly focused on the clearing and settlement space with their Bankchain solution.

Despite only launching domestically this year, itBit's Bitcoin exchange is among the most popular in the world. While Bitcoin trading fees are currently waived, itBit otherwise charges between 35 and 50 bps in fees for Bitcoin trading depending on volume.

Bankchain is targeted at financial institutions as a quicker, cheaper and all-around more efficient avenue for clearing and settling securities transactions. Bankchain is a private blockchain and decentralized network that is governed by the financial institutions that elect to join the platform. For every asset class that itBit is targeting, the company believes it will be able to deliver a 75-90% cost advantage in clearing and settlement.

In the clouded and often grey area of Bitcoin regulation, itBit's Trust Company Charter could prove to be an important differentiator moving forward—it is basically the same legal status as well-known entities such as The Depository Trust Company, Northern Trust, and BNY Mellon. Their status as a Trust Company is beneficial because it exempts itBit from New York's Bitlicense and from the burdensome process of registering as a money transmitter in numerous states. It could also be an important differentiator as the company lures banking partners for its Bankchain product.

In the months and years to come, itBit will, as always, be focused on improving their exchange but will also be heavily focused on adding other digital assets to the Bankchain solution and exchange (gold and unregistered securities are up next).

Ripple

Status: Private/Venture Backed

HQ: San Francisco, CA

Sub-space(s): Payments, Clearing & Settlement, Private Blockchain, Software, FX, Platform

Management Team

Chris Larsen
Co-Founder & CEO

Brad Garlinghouse
Chief Operating Officer

Bret Allenbach
Chief Financial Officer

Financing History

Total Funding: $38.4MM

Angel: $2.9MM (Apr & May 2013)
Andreessen Horowitz, Digital Currency Group, FF Angel LLC, Lightspeed Venture Partners, Vast Ventures, Camp One Ventures, Google Ventures, IDG Capital Partners, Pantera Capital

Seed: $3.5MM (Nov 2013)
Camp One Ventures, Core Innovation Capital, IDG Capital Partners, Venture51

Series A: $32MM (May 2015)
AME Cloud Ventures, Blockchain Capital, China Rock Capital, CME Group, Core Innovation Capital, Digital Currency Group, IDG Capital Partners, Route 66 Ventures, RRE Ventures, Santander, Seagate

Ripple Overview

Ripple is a distributed financial technology company with licensable technology solutions that connect the world's disparate payment systems and power real-time settlement. Ripple developed two full-stack technology solutions for cross-currency settlement and FX market, making that financial institutions can leverage to transact with one another for instant, certain and low-cost payments.

With its settlement technology, Ripple is creating a new infrastructure layer for moving value around the world—thus directly connecting the entities within the world's otherwise disparate payment systems. The problem with disparate payment systems is that they require intermediaries—correspondent banks—which add points of failure, costs, and delays to the movement of money. Instead, Ripple facilitates real-time, certain and direct settlement of payments.

Not only does Ripple help eliminate the points of failure, costs and delays associated with intermediaries, it also allows corporations and financial institutions to be more efficient with their capital: Companies can't put their capital to use during the time that it takes transactions to settle, but as Ripple moves settlement times to nearly instant, enterprises can be more efficient with their capital. Ripple's FX marketplace makes liquidity more competitive and minimizes FX exposure, lowering the volatility and counterparty risk of cross-currency trades.

Ripple is targeting the institutional payments market—which comprises 93% of the total value of cross-border payments. There's a good first-mover advantage for banks and other financial institutions to adopt Ripple, as Ripple provides access to new cross-border payment corridors and a global network of banks and market makers. Ripple has several financial institution customers, including Accenture, Earthport, Fidor Bank, CBW Bank, and Cross River Bank. The company ultimately sees payments settlement as the first and most important step toward building an Internet of Value, enabling money to move as easily as information moves today.

Storj

Status: Private

Sub-space(s): Decentralized Cloud Storage

Management Team

Shawn Wilkinson
Founder & Lead Developer

Tome Boshevski
Founder & Lead Designer

John Quinn
Founder & Chief Development Officer

James Prestwich
Founder & Business Development

Storj Overview

Storj is a decentralized cloud storage platform that is based on blockchain technology and peer-to-peer protocols. Storj leverages blockchain technology to add a critical piece to the decentralized storage puzzle: incentives. Storj's cloud storage platform is a marketplace for cloud storage. People or businesses can leverage excess storage capacity by offering it for "rent" on Storj's marketplace. The company is in its second test group and the network already includes 1.4 petabytes of storage across roughly 350 users in the test group.

When a document is added to Storj, it is digitally shredded into pieces, encrypted then spread across the decentralized network with adjustable redundancy. Storj's decentralized cloud storage platform offers several advantages over traditional cloud storage providers, including cost, privacy, resiliency, and performance.

Storj estimates it will undercut the cost of cloud storage from major providers by at least 50% and deliver faster speeds across its decentralized network. The platform could also offer enhanced privacy for users in that the encrypted data stored across the network is only accessible with the owner's key—no third party can access the encrypted data or reassemble the "shredded" pieces.

Storj uses blockchain technology for three main purposes: payments, auditing, and proof. Blockchain technology facilitates the direct payment from "renters" to "providers" and provides a transparent record that users can audit to verify that their data is safe and has not been accessed or changed.

As a marketplace, the company will be focused on attracting more supply and demand to the network, and hopes to attract data-intensive applications, such as virtual reality, where the cost advantage is of most benefit. Storj monetizes their offering by retaining a portion of the storage payment.

Uphold

Status: Private/Venture Backed

HQ: San Francisco, CA

Sub-space(s): Payments, FX, Wallet, Platform

Management Team

Anthony Watson
President & CEO

Halsey Minor
Founder, Chairman, Chief Visionary

J.P. Thieriot
Vice-Chairman, Head of The Reserve and Investor Relations

Tim Parsa
Chief Compliance & Transparency Officer

Financing History

Total Funding: $20MM

Equity Crowdfunding: $9.9MM (December 2014)

Uphold Overview

Uphold strives to be the central hub for people to store, send and convert value in the cloud. From the outset, Uphold has been focused on helping people leverage the efficiencies of digital money and the Bitcoin payment rail without its drawbacks. Namely, Uphold enables people to securely send, receive, hold, and convert money instantly for free without any of the costs or delays of traditional banking and without any of the confusion or volatility associated with digital currencies, such as Bitcoin. The company aims to be a central hub for value storage, conversion and transmission in a blockchain-enabled world, where value moves as freely as information moves through the internet today.

On the Uphold platform, users can store value in the currency or precious metal of their choice. Uphold also enables users to send and convert between forms of value—such as between fiat currencies and digital currencies for free and into or out of precious metals for a fee. The company's platform is less than a year old but has already seen nearly $400MM of transactions and hosts roughly $3MM in deposits—a number which could increase significantly as the company expands its onramps beyond Bitcoin.

Aside from the free services that Uphold offers, its most radical difference from the traditional banking system is the level of transparency offered on the platform. The company operates on the basic premise that transparency trumps trust: Uphold uses a blockchain to provide a real-time audit showing that their reserves exceed their obligations to customers, instilling confidence for customers that their money is present and available at any time.

Uphold's API platform is facilitating the unbundling and optimization of traditional banking services. While Uphold serves the basic function of storing and converting value, developers and entrepreneurs can leverage the Uphold API platform to create new financial services and inject choice into an otherwise heavily siloed financial system—furthering Uphold's goal to be the central hub of cloud money.

Vogogo

Status: Public (TSXV: VGO)

HQ: Calgary, AB

Sub-space(s): Risk Management and Payment Services.

Management Team

Geoff Gordon
Chief Executive Officer

Tom Wenz
Chief Operating Officer

Rodney Thompson
Chief Revenue Officer

Financing History

Total Funding: $21MM

Series A: $8.5MM (August 2014)
Cormark Securities, Beacon Securities, Canaccord Genuity Corp, Clarus Securities, Salman Partners

Series B: $12.5MM (June 2015)
Beacon Securities, Clarus Securities, Salman Partners

Vogogo Overview

Vogogo is a risk management and payment services company with significant experience in fraud mitigation and compliance requirements for high-risk verticals. Vogogo got its start processing payments for online gaming (poker) sites servicing the U.S. market; experience that gave the company significant insight as to how to effectively combat and mitigate online payment fraud. Vogogo noticed the same challenges that faced the online poker industry were happening in the emerging cryptocurrency-space and other high-risk verticals, and late last year raised money to dial-up and optimize their platform for these rapidly emerging opportunities.

Fast forward a few months and Vogogo now counts many of the major U.S. and European Bitcoin exchanges among its customer base, including Coinbase, Kraken, and BitStamp. In particular, the tough regulatory environment in the U.S. with multiple overlapping jurisdictions between federal and state regulatory agencies helps create demand for Vogogo's solutions. While the company remains focused on the Bitcoin, Blockchain and cryptocurrency space, its solutions can be used for other high-risk verticals, and the company counts payment processors, banks and other financial service providers among its partners and customers.

Ultimately, Vogogo's deep experience in real-time fraud mitigation has helped the company build proprietary software solutions that allow clients to conduct automated fraud mitigation without slowing down or adding bottlenecks to the payment process—all while helping to collect the necessary KYC/AML info.

In the coming months, Vogogo will be heavily focused on international expansion. The company is in the process of registering with the U.K.'s Financial Conduct Authority as an Electronic Money Institution, which will allow Vogogo to better operate across the European Union. It also has its sight set on Asia—another hotbed for Bitcoin and cryptocurrency activity—and is hoping to begin operations there within the year. The U.S., South America and eventually Africa remain on the international expansion agenda.

Xapo

Status: Private/Venture Backed

HQ: Palo Alto, CA

Sub-space(s): Wallet, Payments, Platform

Management Team

Wences Casares
Founder & CEO

Ted Rogers
President

Federico Murrone
Founder and COO

Carlos Rienzi
Head of Security

Financing History

Total Funding: $40M

Series A: $20MM (March 2014)
Benchmark, Fortress Investment Group, Pantera Capital, Ribbit Capital, Slow Ventures

Series A: $20MM (July 2014)
Greylock Partners, Index Ventus, AME Cloud Ventures, Blockchain Capital, David Marcus, Emergence Capital Partners, Max Levchin, Winklevoss Capital, Yuri Milner

Xapo Overview

Xapo is likely the world's largest custodian of Bitcoin in the world. It offers easy-to-use solutions for storing and spending Bitcoin. Xapo's Vaults are one of—if not *the*—most secure way to store Bitcoin in the world: Bitcoin stored in Xapo Vaults is held offline on encrypted servers stored in Faraday cages deep underground in decommissioned military bunkers in the Swiss Alps. Xapo also offers solutions for people in cash-based economies to convert cash into digital money that they can spend online without a bank account.

Xapo straddles two disparate markets: high-net worth consumers, enterprises, hedge funds, and family offices that want to use Xapo Vaults to securely store their Bitcoin and emerging market consumers that are largely unbanked but have a smartphone and use Xapo solutions to convert hard cash into digital money that they can spend online for things like shopping, games, and topping-up mobile minutes. While the former group comprises the majority of Bitcoin that Xapo has under custody, the latter emerging markets group is the high-growth area for the company. Xapo users can turn their physical cash into digital money through one of the mobile top-up companies that Xapo partners with and then spend their digital cash with a Xapo Visa debit card—functionality that is useful for everyone but particularly for the un banked or underbanked.

Xapo offers its wallet and vaults free of charge then makes 1% for transactions in and out of Bitcoin. Xapo earns interchange fees when customers use their Xapo debit card for purchases.

Looking forward, the company is heavily focused on growth in emerging markets, where consumers aren't particularly drawn to Bitcoin but want a convenient way to spend money online. In this respect, Xapo is focused on building out the infrastructure to fully capture this opportunity—which requires forming partnerships with local banks, integrating with the sites that people most want to spend at, and getting the appropriate approval to move money locally and mitigate risk.

ANALYST CERTIFICATION

I, Spencer Bogart hereby certify that the views expressed in this research report accurately reflect my personal views about the subject company (ies) and its (their) securities. I, also certify that I, have not been, and will not be receiving direct or indirect compensation in exchange for expressing the specific recommendation(s) in this report.

RATINGS DISTRIBUTIONS FOR NEEDHAM & COMPANY, LLC

	% of companies under coverage with this rating	% for which investment banking services have been provided for in the past 12 months
Strong Buy	5	24
Buy	64	22
Hold	29	3
Underperform	0	0
Rating Suspended	< 1	0
Restricted	2	0

Needham & Company, LLC employs a rating system based on the following:

Strong Buy: A security, which at the time the rating is instituted, we expect to outperform the average total return of the broader market as well as the securities in the analyst's coverage universe over the next 12 months.

Buy: A security, which at the time the rating is instituted, we expect to outperform the average total return of the broader market over the next 12 months.

Hold: A security, which at the time the rating is instituted, we expect to perform approximately in line with the average total return of the broader market over the next 12 months.

Underperform: A security, which at the time the rating is instituted, we expect to underperform the average total return of the broader market over the next 12 months.

Rating Suspended: We have suspended the rating and/or price target, if any, for this security, because there is not a sufficient fundamental basis for determining a rating or price target. The previous rating and price target, if any, are no longer in effect and should not be relied upon. This rating also includes the previous designation of "Under Review".

Restricted: Needham & Company, LLC policy and/or applicable law and regulations preclude certain types of communications, including an investment recommendation, during the course of Needham & Company, LLC's engagement in an investment banking transaction and in certain other circumstances.

For disclosure purposes, in accordance with FINRA requirements, please note that our Strong Buy and Buy ratings most closely correspond to a "Buy" recommendation. When combined, 69% of companies under coverage would have a "Buy" rating and 22% have had investment banking services provided within the past 12 months. Hold ratings mostly correspond to a "Hold/Neutral" recommendation; while our Underperform rating closely corresponds to the "Sell" recommendation required by the FINRA.

Our rating system attempts to incorporate industry, company and/or overall market risk and volatility. Consequently, at any given point in time, our investment rating on a security and its implied price appreciation may not correspond to the stated 12-month price target. For valuation methods used to determine our price targets and risks related to our price targets, please contact your Needham & Company, LLC salesperson for a copy of the most recent research report.

Price charts and rating histories for companies under coverage and discussed in this report are available at http://www.needhamco.com/. You may also request this information by writing to: Needham & Company, LLC, Attn: Compliance/Research, 445 Park Ave., 3rd Floor, New York, NY 10022

By issuing this research report, each Needham & Company, LLC analyst and associate whose name appears within this report hereby certifies that (i) the recommendations and opinions expressed in the research report accurately reflect the research analyst's and associate's personal views about any and all of the subject securities or issuers discussed herein and (ii) no part of the research analyst's or associate's compensation was, is or will be directly or indirectly related to the specific recommendations or views expressed by the research analyst or associate in the research report.

Disclosures

The research analyst and research associate have received compensation based upon various factors, including quality of research, investor client feedback, and the Firm's overall revenues, which includes investment banking revenues for the following: Amazon.com, Inc., Cisco Systems, Inc., eBay Inc., Facebook, Inc., Alphabet Inc., LinkedIn Corporation and Seagate Technology

The Firm, at the time of publication, makes a market in the subject companies Amazon.com, Inc., Cisco Systems, Inc., eBay Inc., Facebook, Inc., Alphabet Inc. and Seagate Technology .

Equity Options Disclosure

Any Equity Options or Technical Strategy Opinions ("Opinions") contained within this report was prepared by the Equity Options Sales and Trading Desk of Needham & Company, LLC ("Needham" or the "Firm") for distribution to Needham's clients. This Opinion consists of market information and general market commentary only. It is not intended to be an analysis of any security or to provide any information sufficient upon which to base an investment decision.

THIS EQUITY OPTIONS OR TECHNICAL STRATEGY OPINION IS NOT A PRODUCT OF NEEDHAM'S RESEARCH DEPARTMENT AND IS NOT A RESEARCH REPORT. Unless otherwise specifically stated, the information and commentary expressed herein are solely those of the author and may differ from the information, views and analysis expressed by Needham's Research Department or other departments of the Firm or its affiliates.

Needham and its affiliates may have positions (long or short), effect transactions or make a market in the securities or financial instruments referenced in this Opinion. Needham or its affiliates may engage in securities transactions that are not consistent with the information and commentary expressed in this Opinion. Needham may have provided investment banking or other services to the issuers mentioned herein and may solicit such services in the future.

If this Opinion includes extracts or summary material derived from research reports produced by Needham's Research Department, you are directed to the most recent research report for further details, including analyst certifications and other important disclosures. Copies of such reports may be obtained from your Needham sales representative or at www.needhamco.com

This material is provided for informational purposes only and is not intended as a recommendation or an offer or solicitation for the purchase or sale of any security or financial instrument. Any investment decision by you should be based on your specific investment objectives and financial situation. Please contact your Needham sales representative for specific guidance.

The information contained in this Opinion has been obtained from or is based upon sources believed to be reliable, but neither Needham nor the author makes any representation or warranty as to its accuracy or completeness. The information contained in this Opinion is as of the date specified herein. Needham does not undertake any obligation to monitor or update the information. Past performance is not indicative of future results and no representation or warranty, express or implied, is made with respect to future performance. Needham disclaims all liability for any loss that may arise (whether direct or consequential) from any use of the information contained in this Opinion.

Structured securities, options, futures and other derivatives are complex instruments, may involve a high degree of risk, and may be appropriate investments only for sophisticated investors who are capable of understanding and assuming the risks involved. Because of the importance of tax considerations to many options transactions, any investor considering the purchase or sale of any options contract should consult with his or her tax advisor as to how taxes affect the outcome of contemplated transactions. Needham and its affiliates do not provide tax advice.

OPTIONS ARE NOT SUITABLE FOR ALL INVESTORS. For further information on the risks associated therewith, please consult the Options Clearing Corporation's options risk disclosure document available at the following web address: http://www.optionsclearing.com/about/publications/character-risks.jsp

Clients should call the Equity Options Sales and Trading Desk (212-705-0369) for additional information.

Additional Disclosures for Israeli Clients

All information presented in this document is, unless otherwise specified, under copyright of Needham & Company, LLC ("Needham"). No part of this publication may be copied or redistributed to other persons or companies without the prior written consent of Needham. These reports have been prepared by Needham and distributed by Clal Finance Batucha Brokerage, Ltd. ("Clal"), which accepts sole responsibility for its content subject to the terms set forth below.

Neither Clal or its affiliates (and any director, officer or employee thereof) nor Needham is liable for any incomplete or improper transmission of these reports or for any delay in transmission. Any unauthorized use, disclosure, copying, distribution, or taking of any action in reliance on these reports is strictly prohibited. The views and expressions in the reports are expressions of opinion and are given in good faith, but are subject to change without notice. These reports may not be reproduced in whole or in part or passed to third parties without permission. Clal or its affiliates (and any director, officer or employee thereof) and Needham do not guarantee their accuracy or completeness, and neither Clal or its affiliates (and any director, officer or employee thereof) nor Needham shall be liable in respect of any errors or omissions or for any losses or consequential losses arising from such errors or omissions.

Neither the information contained in these reports nor any opinion expressed constitutes an offer, or an invitation to make an offer, to buy or sell any securities or any options, futures or other derivatives related to such securities ("related investments"). Clal or its affiliates (and any director, officer or employee thereof) and Needham may trade for their own accounts as odd-lot dealer, market maker, block positioner, specialist and/or arbitrageur in any securities of the issuer or in related investments, and may be on the opposite side of public orders. Clal or its affiliates (and any director, officer or employee thereof) and/or Needham may have a long or short position in any securities of the issuer or in related investments. Clal or its affiliates (and any director, officer or employee thereof) and/or Needham may from time to time perform investment banking or other services for, or solicit investment banking or other business from, any entity mentioned in these reports.

These reports are prepared in general for the Israeli clients of Clal who are qualified institutional customers as defined by reference to the First Schedule to the Securities Law, 1968, of the State of Israel. They do not have regard to the specific investment objectives, financial situation and the particular needs of any specific person who may receive any of these reports. Investors should seek financial advice regarding the appropriateness of investing in any securities or investment strategies discussed or recommended in these reports and should understand that statements regarding future prospects may not be realized. Investors should note that income from such securities, if any, may fluctuate and that each security's price or value may rise or fall. Accordingly, investors may receive back less than originally invested. Past performance is not necessarily an indication of future performance.

Foreign currency rates of exchange may adversely affect the value, price or income of any security or related investment mentioned in these reports. In addition, investors in securities such as ADRs, whose value are influenced by the currency of the underlying security, effectively assume currency risk. Unless agreed in writing with Clal, this research is intended solely for use internally by the recipient.

Needham is not an authorized broker, dealer or investment adviser outside the United States. The research does not constitute an offer to provide financial services to anyone outside the United States. Any investor in Israel wishing to buy or sell the securities mentioned in this report should do so through Clal.

Neither Needham, the research analyst nor anyone else acting on behalf of Needham is an Israeli investment advisor, investment marketer or portfolio licensed under the Israeli Regulation of Investment Advice, Investment Marketing and Investment Portfolio Management law, 1995. Accordingly, Needham does not maintain the insurance specifically required of a licensee in accordance with such law.