OCTOBER 2016

PitchBook

FINTECH

ANALYST REPORT

PART 2

BITCOIN/BLOCKCHAIN

Including data from the PitchBook Platform, which tracks more than 33,000 valuations of VC-backed companies.

Contents

CREDITS & CONTACT

PitchBook Data, Inc.

JOHN GABBERT Founder, CEO

ADLEY BOWDEN Vice President, Market Development & Analysis

Content, Design, Editing & Data

EVAN B. MORRIS Analyst

DANIEL COOK, CFA Senior Data Analyst

NIZAR TARHUNI Senior Analyst

GEORGE GAPRINDASHVILI Managing Editor

JENNIFER SAM Senior Graphic Designer

Contact PitchBook

pitchbook.com

RESEARCH
reports@pitchbook.com

EDITORIAL
editorial@pitchbook.com

SALES
sales@pitchbook.com

COPYRIGHT © 2016 by PitchBook Data, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, and information storage and retrieval systems—without the express written permission of PitchBook Data, Inc.

Contents are based on information from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. Nothing herein should be construed as any past, current or future recommendation to buy or sell any security or an offer to sell, or a solicitation of an offer to buy any security. This material does not purport to contain all of the information that a prospective investor may wish to consider and is not to be relied upon as such or used in substitution for the exercise of independent judgment.

Analyst Note

Bitcoin and blockchain have been some of the most exciting yet misunderstood technologies to emerge in the last decade. Investors have pumped some $1.8 billion into equity investments in companies utilizing the technology since 2013. This doesn't include the individuals and groups pouring resources into the technology's supporting hardware, which in aggregate holds 8x the processing power of the world's 500 fastest supercomputers. Meanwhile, every bank, brokerage house and multinational worth its salt has issued a press release announcing one multimillion dollar partnership or another to explore the implications for their business.

This is a pivotal moment for blockchain. Institutional investors have wagered that the technology will more than pay off by revolutionizing global payments, securities clearing and financial services, with further wide-reaching implications for monetizing media and content distribution, the sharing economy and IoT. While recent high-profile missteps have cast a shadow over the industry, its continued scaling only goes to illustrate how rapidly the technology has burgeoned thanks to outsized consumer and enterprise interest.

Evan B. Morris

How We Got Here

Many of the emerging use cases of blockchain are still highly abstract. Examining the disruptive potential of a new technology requires first exploring the historical process and pressures that created the status quo.

Above all, payment systems must insure that each unit of value is rightfully held by the spender so that each unit of currency can only be spent once. This is referred to as the double spend problem. Historically, this was solved with intrinsically valuable metallic coins, and later with bank-issued paper currency that was difficult to counterfeit. In order to facilitate overseas trade prior to electronic long-distance communication, the Medicis developed double-entry accounting listing two columns for assets and liabilities. For each credited account, another account would be debited so that each transaction took place in a closed system. Updated ledgers were copied and distributed to far-flung branches.

Double ledgers could be centrally copied and distributed to far-flung branch networks to account for transactions and balances.

Bankers kept track of deposits and liabilities using double ledger accounts on each other's books since banknotes were backed by gold deposits. These metallic reserves were difficult to transport, so banks needed a way to keep track of who owned what. This decentralized system had other inefficiencies. Having multiple banks issue their own banknotes opened up the possibility of fraud due to the sheer diversity of paper bills in circulation. Since consumers had to be sensitive to perceived solvency, this created a higher likelihood of bank runs. Central banks emerged to take over and standardize banknote issuance and further centralize the multilateral banking system, as each constituent bank now had an account with the central bank.

As we will examine later, blockchain has the potential to bring heightened transparency to asset ownership. Tracking ownership of alternative assets has always been opaque, in some ways even more so than gold or currency accounts. While stock certificates tracking claims on assets were hard to forge even in the days before high-quality printing, transactions—and thus overall ownership—could only be tracked through a central broker-dealer or clearinghouse. Cap tables listing equity ownership and creditors were only cleaned up in the case of a liquidity event such as a merger or acquisition. This lack of transparency makes events such as bankruptcy proceedings very costly and tedious.

Central banks became even more essential to providing liquidity and issuing standardized paper currency once fractional reserve banking emerged, as banks only kept a small portion of capital on hand as deposits. However, central banks gradually did away with the gold standard, as the Keynesian doctrine of running deficits in lean times and surpluses in good times proved difficult to implement during the Great Depression and World Wars.

In a democratic society—even if the central bank is independent—there is a bias toward more expansionary/inflationary monetary policy. In the current macro environment, central banks and governments have coordinated to promote inflation through asset purchases and perpetual budget deficits, which increase the money supply every year and dilute the value of currency over time. In addition to what we see in the developed world, the limitations of government-backed currencies as a store of value have been proven time and time again, such as in hyper-inflationary episodes in Germany, Zimbabwe and every few years in Latin America. Bitcoin exhibits opposite (deflationary) properties, as you will see in later sections.

The incentive structures created by fractional reserve lending and modern central banking are inherently inflationary.

Thus far, we've examined the gaps in historical financial infrastructure that have helped support bitcoin/blockchain's importance and rise. Yet, similar to many other emerging tech, the invention of the internet has played a pivotal role in bitcoin/blockchain's growth. The development of the internet, however, did not initially address any of the issues with the existing financial infrastructure, in part due to the reticence of institutions to relinquish tight control over centralized ownership databases. Even so, conducting fast and secure online payments was one of the obvious use cases of the internet. However, developers took some time to fix the double spend problem—the issue of ensuring each currency unit is only spent once. Initial online payment platforms often took months to settle transactions in order to jump through many hoops including fraud prevention. David Chaum patented an early online payments system called DigiCash that operated similarly to how airlines now process credit cards in-flight. Payer and receiver exchange serial numbers and, once electronically connected to central digital ledger, the transaction could be verified. The system enabled much smaller unit payments than was cost effective with existing credit card payment networks, and had a much higher level of security. DigiCash filed for Chapter 11 bankruptcy in 1998 but, to be clear, its failure did not stem from issues driven by its technology being poorly adopted. The company offered a secure payment system that solved the double spend problem, the greatest issue bitcoin strives to solve, yet unfortunately, poor management at the executive level left many promising projects half-completed.

Online payments took a long time to implement due to security concerns and technical issues around keeping track of balances.

A confluence of seemingly unrelated early internet technologies enabled the development of cryptocurrencies. One early method to solve the ubiquitous problem of email spam was the forcing of a sender to complete a digital puzzle in order to send a message. Although the required computational power was insignificant to a home or business user, a spambot sending thousands of unsolicited messages would be cut at the knees. Since many forms of hacking require "brute force" to exploit systems, a built-in speed bump like solving a puzzle represents a considerable security upgrade and, as we explain later, is an essential aspect of blockchain technology. The 1990s also saw the development of anonymous browsing on the Tor network developed by research labs associated with the US military. Tor encrypts data and sends it through a network of peer nodes where it becomes impossible to track to any one point. This allows for near anonymization, as traffic becomes broadly distributed across the entire network. Rather than rely on one chain of centralized servers, traffic is requested and routed across whomever has available resources to handle the bandwidth. While each of these technologies has had varied standalone impact, the confluence of these and other tech has played a pivotal role in the emergence of blockchain.

Bitcoin draws from a number of early internet technologies, including the Tor P2P network used for filesharing and hard-to-track browsing, and a technique for preventing email spam.

How Bitcoin Works

In 2009, “Satoshi Nakamoto” pseudonymously released the paper “Bitcoin: A Peer-to-Peer Electronic Cash System.” Satoshi envisioned bitcoin as a distributed digital payment system that bypasses the status quo centralized financial intermediaries. The protocol incentivizes a peer-to-peer network to validate transactions and ownership on a shared public ledger known as the blockchain.

The legitimacy of each bitcoin is backed by a record of all previous transactions on the network. The owner transfers bitcoin by providing their address, the address of the sender, a private key or password to verify rightful ownership, and the hash of the previous block to serve as a timestamp in the list of all transactions. New transactions are broadcast to all nodes. Each node (miner) collects new transactions into a block, currently averaging around 1,500 transactions per block every 10 minutes. Nodes (miners) accept the block only if all transactions are valid and not already spent. They express acceptance of the block by using its hash as an input when working on creating the next block. To be confirmed, transactions are stored in the “mempool” of nodes that receive them, which has a capacity of around 50,000 pending transactions.

The cryptographic hash function is central to understanding what makes bitcoin tick. The hash function represents the process by which miners verify transactions and mine blocks. Functionally, the hash is a mathematical algorithm that converts data of any length (in this case a list of transactions) to a string (of characters) of a fixed length. Most importantly, the function works in such a way that the output will always be the same for a given input, but the input can only be calculated through trial and error.

Example of a hash:

Take the square root of 5. The result will be 2.236067977499789696409173 6687313. Take the third through seventh digits after the decimal. The output will be 60679.

This is basically a very simple (and weak) hash function. For any given prime number (in this case it has to be prime), one can create an otherwise unrelated five-digit output.

GLOSSARY

ASIC - silicon chips specifically designed to do a single task.

Digital Signature - a way to encrypt documents with digital codes that are particularly difficult to duplicate.

Halving - the number of new bitcoins generated per block is decreased 50% every four years.

Hash - a large number written as a hexadecimal. Bitcoin uses an algorithm to generate verifiably “random” numbers in a way that requires a predictable amount of resources.

Mempool - participants store transactions waiting to get into a block in their memory pool after receiving them, even if they are invalid, to prevent nodes from constantly requesting transactions that they’ve already seen.

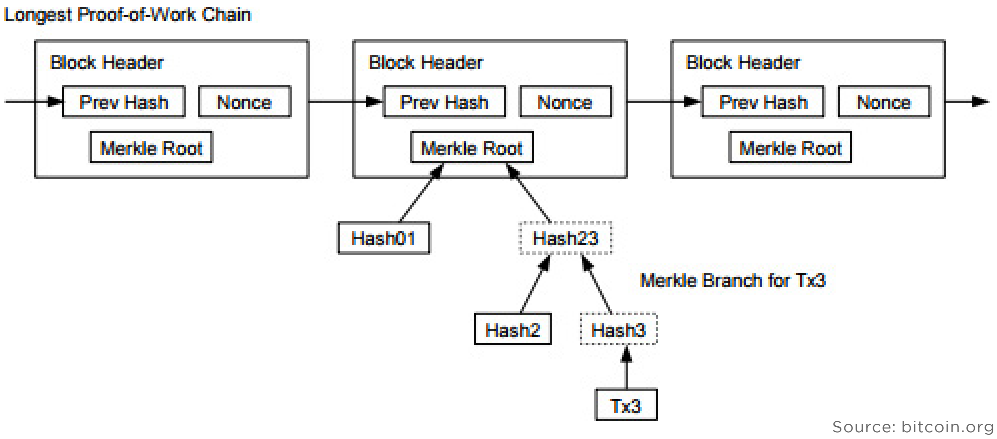
Miners - computers programmed to solve cryptographic problems using computing hardware in order to earn newly released bitcoins.

Node - each bitcoin client currently running within the network.

Nonce - a random guess value included in the hash function in order to prevent previous transactions being used in a replay attack.

Bitcoin incentivizes individual “miners” to lend their computing power to the network. Computing power is the primary resource required to run a transaction network, and the bitcoin protocol allows miners to monetize their processing power. Senders of bitcoin typically attach between five and 20 basis points (.05-.2%) to a transaction to incentivize miners (nodes) to put it on the next block. The other incentive comes from the process to verify each new block, which releases new bitcoin.

The above process is called a “proof of work.” The inputs for the hash that miners need to guess include the sender’s private key, the transaction details, the last transaction from the blockchain and a nonce (random guess value.) The random guess value aims to find an output value with the longest string of zeroes at the beginning, making the process more akin to rolling a die than actual problem solving. The longer the string of zeroes, the more computing power is required to mine. As a result, the longest chain is always considered the correct one, and nodes (miners) will always work on extending it. Over time, the length of the string of zeroes at the beginning grows, exponentially increasing the difficulty of the problem to account for an increase in computing power.



Source: bitcoin.org

Originally, bitcoin miners (nodes) were mostly hobbyists using spare computing resources to contribute to an emerging technology. Over time, miners discovered that the nature of calculations for the hash function made bespoke hardware, or application-specific integrated circuit chips (ASICs), far superior to general-purpose PCs or server farms. Canaan Creative, perhaps the first mass producer of bitcoin mining ASICs, accounted for by far the largest single investment in the space when it was acquired by Shandong Luyitong Intelligent Electric (SHE: 300423) for CN¥ 3.1 billion ($470 million) in June.

Proof of Work - a result that can only be obtained through the use of computational resources. Changing the data in the proof of work requires redoing the work.

Private Key - a string of data that shows you have access to bitcoins in a specific wallet (like a password). Private keys must never be revealed to anyone but you, as they allow you to spend the bitcoins from your bitcoin wallet through a cryptographic signature.

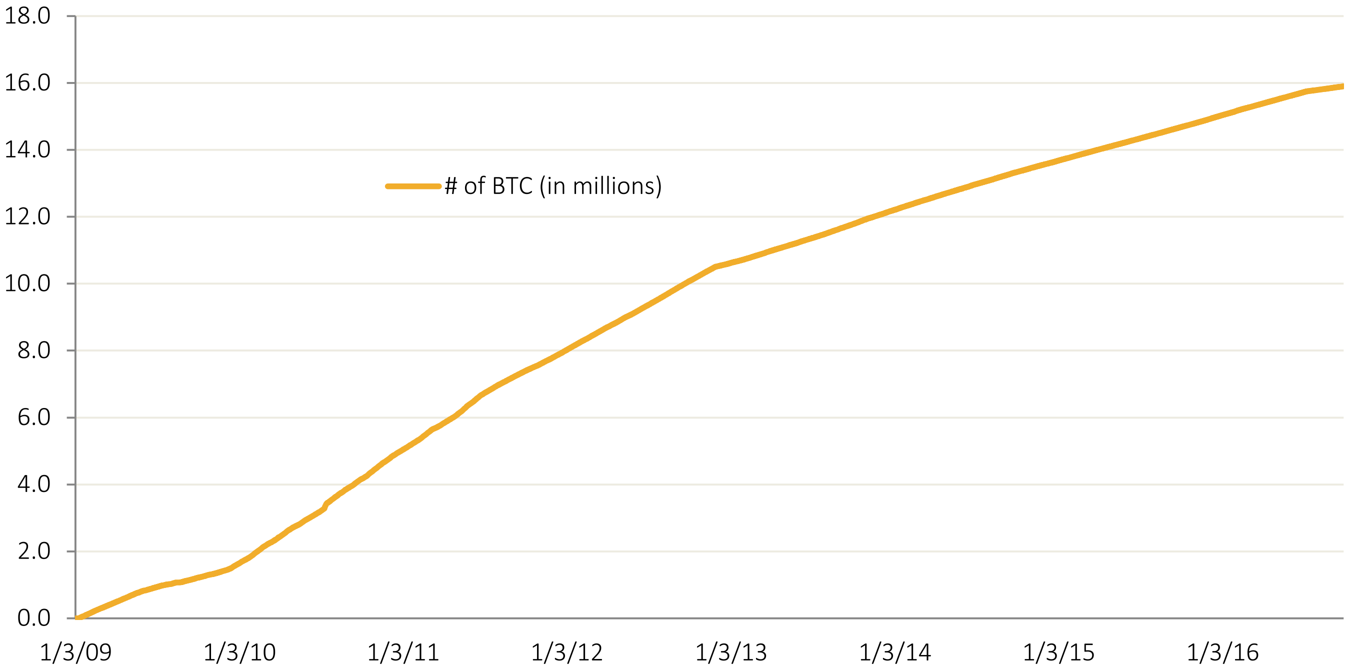
Sources:

www.blockchaintechnologies.com/blockchain-glossary

en.bitcoin.it/wiki/Vocabulary

The total bitcoin (BTC) money supply will gradually reach a maximum. Every time a block is mined, the first node to calculate the hash is rewarded with 12.5 bitcoins. This reward is halved every four years, most recently in July from 25 BTC, and the reward will halve again around the year 2021. There are currently almost 16 million extant bitcoins, just over three-fourths of the maximum of 21 million BTC to be in circulation around the year 2140. The 21 million maximum is ultimately an arbitrary number that is a function of the halving schedule. As the maximum is approached and the block reward decreases, miners will need to be compensated with transaction fees rather than mining proceeds.

TOTAL NUMBER OF BITCOINS IN CIRCULATION



Source: data.bitcoinity.org
*As of 9/28/2016

Current Applications & Market Development

CONSUMER PAYMENTS

One major application for the bitcoin and blockchain protocol has been to disrupt the slow, high-friction cost structures of the current consumer payments system. For the capability of accepting credit card transactions, the typical merchant with under $100,000 in volume has around a 3% merchant discount rate (MDR)—the amount deducted per transaction for processing fees. This is less for larger retailers and debit card transactions, but slightly more for premium credit cards. The largest portion of the MDR goes toward bank interchange fees, which go entirely to the card issuer. While making up a much smaller part of the fee structure, payments processors MasterCard and Visa (collectively processing 88% of all transactions) have been the target of countless anti-trust lawsuits for trying to maximize fees by shutting out competitors. These notorious anti-competitive behaviors include exclusivity agreements that prevent retailers from encouraging customers to pay through lower cost options and force out competitors such as American Express and Discover. Even so, the high fees fail to protect retailers, as merchants lost 1.47% of revenue to fraud in 1Q 2016, according to a LexisNexis survey. Bitcoin provides a safer transaction medium to help alleviate this concern.

Transaction fees represent a major cost eating into the margins of retail businesses.

Most of the interest in cryptocurrency payments stems around online rather than brick-and-mortar retailers. Currently, for a bitcoin payment to be conducted between an individual and a business, they both only need wallet software in order to provide an address to send and receive payments. Merchants are typically charged a flat fee of around 1% by a bitcoin merchant processing service such as BitPay or Coinbase. Companies may worry about exposure to the sometimes high volatility of cryptocurrency markets, and these wallet services provide the option to avoid holding any bitcoin balances by offering immediate spot price conversion.

Wallet software provides a user-friendly platform to send and accept transactions for both merchants and consumers.

INTERNATIONAL REMITTANCES

Legacy players dominate the market for international remittances. Western Union, MoneyGram and Euronet Worldwide spent decades building franchise businesses across the globe. The companies handle the compliance and operations of money transfer while providing local shopkeepers with a capital-light side business. Today, the global remittance industry takes out $40 billion annually in fees. When expatriate workers wish to send money to their families, many turn to a familiar brand they remember from home. Fees on these transfers typically stand around 2-6% of the total transaction value depending on the volume of the corridor. Bank wire transfers are even more expensive, with fees eating up 10-15%. Banks also tend to focus only on specific corridors with a strong branch network, and thus, some corridors might not have access to the money transfer services they need.

The existing options for sending money overseas take out a significant amount in fees (2-6%), while bank wire transfers can cost 10-15%.

By using bitcoin rails to bypass traditional players such as Western Union, individuals can theoretically send money more quickly and at a lower cost. However, international payments come with varying regulations in each country they operate in, including KYC (know your customer) and anti-money laundering regulation. Furthermore, for payments conducted in bitcoin, liquidity may be an issue. The last-mile conversion into fiat remains a barrier to broader adoption. Western Union and Hawala networks* (popular in the Islamic world) rely on local merchants to prefund transactions in cash. Places like Argentina, with a dismal track record in regard to currency volatility, make consumers see upstart technology favorably as a way to hedge against very real potential for capital controls.

Parallel systems ensure continuation of services in places with a history of monetary instability, such as Latin America and Africa.

*Hawala networks facilitate informal payments among trusted merchants tied together by shared business interests and the Muslim faith.

MICROPAYMENTS

Some of the most heavily disrupted industries such as media and digital music could see a renaissance thanks to online micropayments. Imagine being able to read an interesting Financial Times article sent by a friend for 25 cents instead of having to pay $600 a year for a subscription. Tiny denomination payments have the potential to impact business models by allowing the monetization of previously untenable services through a middle ground between ads and subscriptions. Previously, only the largest players such as Apple iTunes could get away with selling goods like individual digital songs because they bundled multiple purchases into one transaction in order to avoid paying fixed costs more than once. The extremely low transaction costs of bitcoin and the decimalization of transactions allow (in theory) for payments smaller than one cent. This allows for usage-based business models predicated on an expected high volume of small transactions.

Cost-effective micropayments would disrupt content distribution and sharing economy business models through precise metering of use rather than flat fees.

Decimalization - currency property that allows for transactions at the sub-unit level represented in decimals.

In addition to the newspaper article example, how about paying for songs on Spotify on a per-listen basis in the same way that artists are paid. This could also disrupt the annoyingly high fees for accessing hotel or airplane Wi-Fi networks. Imagine checking your email for a few cents without going through the hassle and expense of buying a $20 daily pass. Micropayments create the possibility of highly efficient subscription and tipjar services of all stripes. One current example of the above is BitMonet, which offers a platform for content creators to get paid directly in bitcoin by consumers making small payments.

On standard bitcoin protocol, micropayments of less than about a cent are impractical. The term "dust" refers to these too-small-to-be-profitable transactions. Emerging blockchain technology called sidechains provide a mechanism for micropayments via a second blockchain that records transactions embedded on top of a primary blockchain such as bitcoin. Sidechain startups have received some of the strongest interest by institutional investors. Microtransactions can be facilitated by similar systems developed by the Lightning Network and the bitcoin computing startup 21, backed by a number of notable VCs including a16z, Pantera Capital and the Winklevoss twins. Another VC-backed bitcoin infrastructure company, Blockstream, has been using some $77 million of VC investment to develop sidechain protocols, including the July acquisition of Maltese startup GreenAddress. Both systems enable the opening of sidechain "channels" between parties that record only the opening and closing balance on the blockchain, not individual transactions. The sidechain channels also have the potential to mitigate the issues around the extended block time by marrying the best features of fiat and digital currency.

Sidechain technology is enabling micropayments on bitcoin. Companies developing this technology are among the best-funded in the space.

BANK-TO-BANK

While the bitcoin protocol has some obvious drawbacks such as speed, accountability and the resource-intensity of mining, established financial institutions have grown interested in the blockchain's potential for bank-to-bank transfers. Central banks have also explored blockchain technology with great interest. While the US Federal Reserve has only met with industry leaders and lobbyists, the People's Bank of China, Bank of Canada and Bank of England have been more public with their efforts to explore the possibility of implementing distributed ledger systems. The recent hack that stole hundreds of millions of dollars from the Bank of Bangladesh's account with the New York Fed via the SWIFT system showed that even the existing protocol had gaping flaws.

SWIFT - a telecommunications system used for international interbank communications.

Banks fear not just being hacked, but also outsiders and competitors monitoring transaction data. Financial institutions are most concerned about a truly public ledger, as in many cases this information could be traded against in the public market. Impressive partnerships involving the major players in financial services, technology and industrial corporations have been formed by R3, the Hyperledger Project and Digital Asset Holdings. Ripple Labs founded the Ripple Network in 2012 in order to provide institutions with a fast and secure private blockchain network.

The low transaction fees of the bitcoin network have prompted major corporations and banks to explore using the technology for back-office operations.

Banks also have great interest in the potential for blockchain systems to facilitate the matching of trades and to validate ownership in their back-office operations. Like any business, payroll eats up a huge percentage of banking revenues, and today, banks employ thousands to help operate and manage clearinghouses. Investment banks have been slashing traditional business lines left and right in an attempt to cut costs in a low interest rate environment that has seen net interest margins between the cost of capital and revenues from lending shrink for the entire industry. Money centers are in need of boosting their total profit margins and blockchain holds a considerable amount of potential to this end.

Direct Investment

Because bitcoin is functionally a medium for storing and transacting value, many investors view it as a cash-like investment. Meanwhile, the Commodities Futures Trading Commission classifies it as a commodity. Unlike traditional commodities, however, it doesn't have any other real-world applications. For instance, gold can be used in the production of electronic cables, cell phones, computers or jewelry, while silver is used to make mirrors and batteries. However, in the context of an investment portfolio, bitcoin behaves much differently than either cash or commodities.

Unlike commodities such as gold or silver, bitcoin lacks inherent value.

Although bitcoin has cash-like characteristics, we still view it as an emerging technology with a risk/return profile similar to that of a late-stage venture investment. Although bitcoin is no longer in its infancy, there is the possibility of substantial capital appreciation as the pioneer cryptocurrency continues to gain traction. What's more, investing in bitcoin has a number of advantages over traditional venture investments. First, anyone can add bitcoin to their portfolio, not just the qualified investors that venture and private equity investments are reserved for. Second, investors can invest in bitcoin without paying the hefty fees charged by VCs. Finally, bitcoin is highly liquid, whereas venture investments can often take years before an exit is realized. That said, investing in bitcoin cannot supplant the benefits of diversified venture exposure, nor can it be acquired with the protective terms often negotiated by VCs.

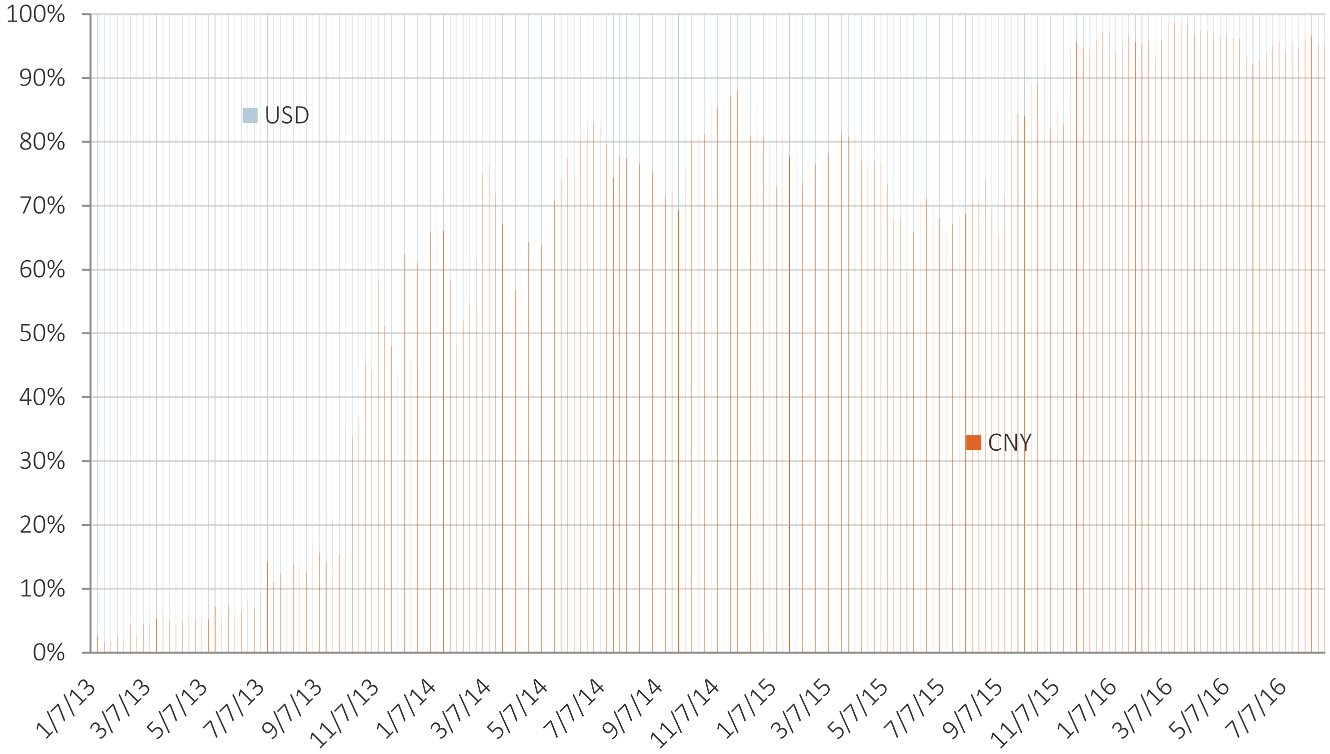
Another attractive characteristic of bitcoin is that it will ultimately be a deflationary asset. The source code for bitcoin outlines that the ultimate supply will be 21 million, which will be reached by the year 2140. Once this terminal supply is reached, it will begin to reduce due to lost bitcoins—either through hard drive failure or physical bitcoin print-outs being misplaced or destroyed. So naturally, its value will grow as the supply is reduced. Inversely, cash is inflationary in nature. Sovereign governments continue to increase the amount of money in circulation, reducing its purchasing power over time; bitcoin is not subject to central bank manipulation. Because of its decentralized nature and the absence of governmental manipulation, many speculators in China have turned to trading bitcoin, looking to exploit its volatility. In fact, according to data provider Bitcoinity, over 94% of bitcoin trading volume was in Yuan in August 2016. The majority of that activity was done by day traders who don't hold bitcoin long-term, as well as by automated trading algorithms.

One attractiveness of bitcoin as an investment is its built-in scarcity due to an ultimately fixed supply.

One glaring restraint to bitcoin investment is its market cap. As of this writing, bitcoin has a total market capitalization of $9 billion, merely the size of publicly traded companies like Nordstrom or Foot Locker. This makes

BITCOIN TRADING VOLUME IN DOLLAR & YUAN DENOMINATED MARKETS

(IN MILLIONS)



Source: data.bitcoinity.org
*As of 9/28/2016

it difficult for institutional investors to take a meaningful position in the cryptocurrency. In smaller portfolios, however, bitcoin can boost the risk/return profile due to its uncorrelated nature with other asset classes.

Bitcoin investing also comes with its own unique set of risk factors. Because it isn't backed by a sovereign government, bitcoin's value is more or less backed by the public's confidence in its security and value. As such, any hacks and thefts of bitcoin can shake the confidence in its security and hurt its value. For instance, from 2011 to 2014, the bitcoin exchange Mt. Gox was hacked to the tune of 800,000 bitcoins, worth about $460 million. Between February and April 2014, when Mt. Gox halted trading and the public began questioning its solvency, bitcoin's value was nearly cut in half.

Without government backing, bitcoin's value comes from confidence in the security and safety of its network.

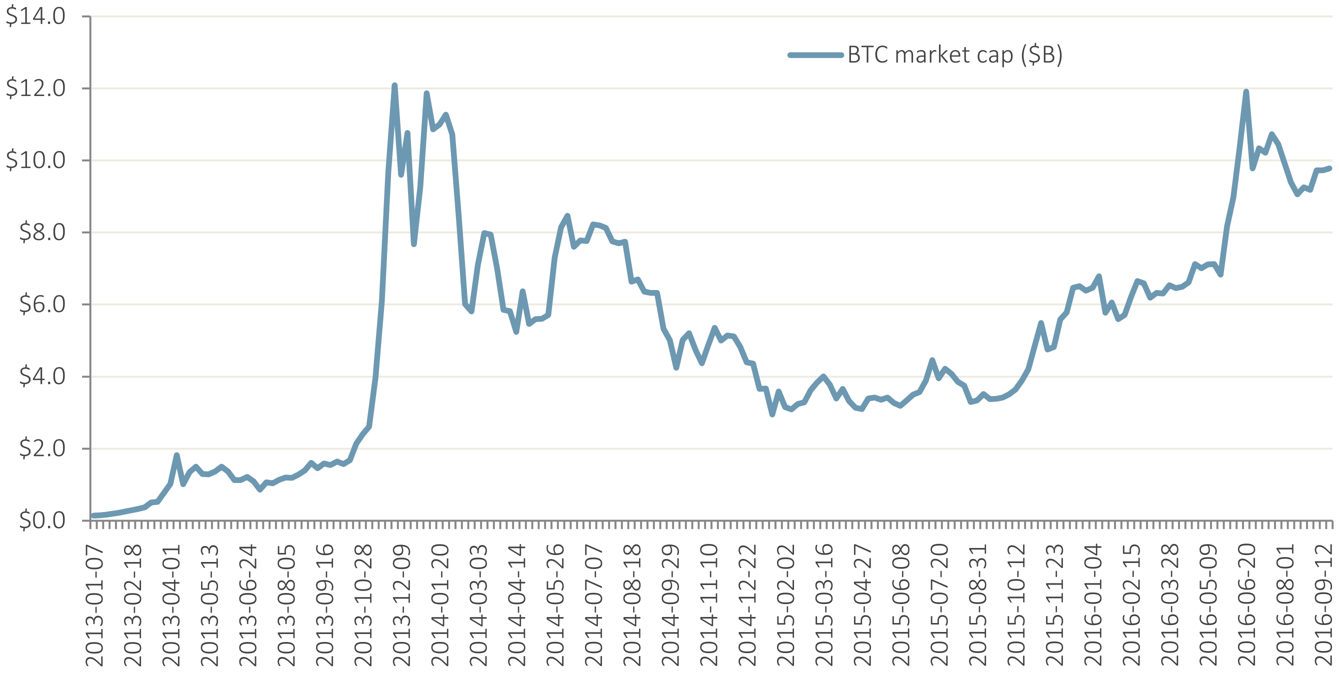
It's worth pointing out that the hack was largely due to vulnerabilities in the exchange, and not in the blockchain technology itself. As more seasoned players have moved into the bitcoin exchange space, the risk of these hacks has decreased. Additionally, governments have begun to more closely monitor and regulate bitcoin and members of its ecosystem.

On the other hand, government regulation poses a major hurdle to bitcoin's usefulness and adoption. Bitcoin transactions are currently regulated at both the federal and state level, and it's a felony to engage in money transmission without a license in a state that requires one. For that reason, funding a bitcoin payment company can be extremely costly, something that venture capitalists are weary of. Perianne Boring of the Chamber of Digital Commerce puts it plainly: "From a currency perspective, the state-by-state licensing regime is by far the biggest hurdle to anyone trying to use bitcoin as a payment instrument." Beyond the state-level regulations, different countries regulate cryptocurrencies in their own ways as well. Standardizing this government oversight will be a major domino to tumble on bitcoin's path to universal adoption.

State-by-state licensing represents a major hurdle for bitcoin money transmission businesses.

As bitcoin becomes more widely adopted, expect to see its value stabilize and its risk profile become more cash-like. However, there is still the risk of other cryptocurrencies overtaking bitcoin as the dominant player in the space. One such challenger is a cryptocurrency known as Ethereum, which hopes to be the Facebook to bitcoin's Myspace. In the next section, we'll unpack how the Ethereum protocol functions, while examining its current state and future implications on blockchain technology.

BITCOIN MARKET CAP, $B



Source: data.bitcoinity.org
*As of 9/28/2016

Ethereum & the Future of Blockchain

While bitcoin promises to revolutionize payments, its limited range of programmable functions has held it back from taking blockchain technology to its full potential. Launched in 2015 with a $15 million crowdfunding campaign, Ethereum has quickly risen to become the second-largest digital currency with a total market capitalization of over $1 billion. Unlike the secretive Satoshi Nakamoto, Ethereum has been overseen by the Switzerland-based non-profit Ethereum Project. Switzerland was chosen as domicile due to a cryptocurrency-friendly legal regime that doesn't require a physical person on both sides of a contract for it to be valid. 21-year-old co-founder Vitalik Buterin stated in a recent interview that previous cryptocurrencies existed as either single use case or as "Swiss army knives," in which a group of smart people got together in a room and made a list of every application they could think of and made a transaction type specifically for each pre-conceived function. Buterin wished to create an open-ended platform that developers could design their own use cases for. More than a cryptocurrency, Ethereum is a global distributed computer network utilizing blockchain technology. Thus, the protocol is "Turing-complete," a property of computers or programming language that mean it can compute anything that any real-world general purpose computer can. The only limiting factor for running applications is the amount of ether one has to execute the code. The currency function (ether) exists both to incentivize miners to devote processing power and to allocate resources on the network. Ether can be traded as currency or used inside Ethereum to run applications or monetize work. Developers can code smart contracts and other applications, paying peers with ether to execute the code. The Ethereum network has also been designed to have a much faster block time than bitcoin.

Ethereum is a Turing-complete distributed computing network powered by a cryptocurrency, ether.

Turing-completeness refers to a property in computing that a programming language or computer can perform any function that a general purpose computer can.

In spite of the presence of a centralized governing body, Ethereum's proof of work function, Ethash, was designed to minimize the comparative advantage of centralizing corporate mining pools. Ethereum's co-founders wanted to recapture the egalitarianism of the early days of bitcoin when many miners were hobbyists with an old desktop. As the entire bitcoin network has 8x the processing power of the world's 500 fastest supercomputers combined, bitcoin strongly rewards application-specific integrated circuits (ASICs), i.e. hardware built specifically for bitcoin mining. Much like how during the California Gold Rush manufacturers and merchants selling picks and shovels tended to fare better than goldpanners, the largest bitcoin/blockchain-related investment involved the acquisition of Canaan Creative, the maker of the groundbreaking Avalon chip, by Shandong Luyitong Intelligent Electric (SHE: 300423) for CN¥ 3.1 billion ($470 million).

Unlike bitcoin, Ethereum mining emphasizes “memory hardness” whereby performance is limited by how fast information can be moved around rather than raw calculations. The best chips for this task are GPUs (graphics processing units), which have wide applications in many emerging technologies including virtual/augmented reality, autonomous vehicles, bioinformatics, computational physics, neural networks and more. Ethereum’s profit motive by design partially incentivizes socially beneficial advances in computing power, as GPU manufacturers will continue to spend on R&D to help facilitate the network.

The broad functionality of Ethereum enables three basic types of contracts: short term smart contracts, slightly longer term autonomous agents and longer term group contracts called DAOs (decentralized autonomous organizations). Ethereum smart contracts enable automatically clearing contracts in automated prediction markets (gambling), financial derivatives clearing and insurance. Many derivatives markets have waned since the financial crisis due to high cost of execution and compliance costs. Automatic execution using Ethereum could enable a return to cost-effectiveness. One such type of derivative that may return is single-name CDS (credit default swaps), an insurance contract that pays out when a bond defaults. A public ledger of derivatives exposure would reduce the counterparty risk that led to Bear Stearns and Lehman Brothers inciting a contagion. During the financial crisis, Bear Stearns failed due to a domino effect of counterparties pulling funds when they feared the bank was unwilling or unable to fulfill derivatives payouts. These binding contracts would enable a range of services in jurisdictions without robust legal systems.

Ethereum’s most promising use case comes from the ability of smart contracts to automate the execution of all sorts of real-world agreements.

Autonomous agents allow for IoT applications such as automated hotel rooms, car rentals, vending machines and Wi-Fi. Smart contract-enabled smart locks, currently in development by companies like Slock.it, have the potential to allow Airbnb hosts to eliminate the hassle of check-in and track when guests come and go.

DISTRIBUTED AUTONOMOUS ORGANIZATIONS

The most controversial application of the Ethereum protocol has been DAOs—distributed autonomous organizations. Though organizers are reluctant to use terms that might imply relevance of securities law, they are essentially publicly traded VC firms where all the investment decisions are made dynamically by the LPs who hold shares. That is, investment firms that can run themselves, without the 2/20 fees. These organizations issue their own tokenized smart contracts in the form of tradable tokens in exchange for ether-denominated investment. These tokens can be traded very much like ether itself, and uninvested "dry powder" can be called on at any time. As part of the smart contract, investors then vote on potential projects for the organization to pursue and receive dividends in return. Many of these projects are "Dapps," short for distributed applications that are typically open-source and reward contributors through smart contracts.

DAOs - distributed autonomous organizations created in smart contracts promise to automate the investment process, cutting out expensive management fees.

So far, there has been just one DAO, commonly referred to as "The DAO." Just a month after The DAO completed the raise of $117 million in the largest crowdfunding ever, an attacker was able to steal around one-third of all DAO ether tokens, representing $55 million. The dollar value of ether halved overnight, and the Ethereum Foundation decided to conduct a hard fork to attempt to recover the lost ether.

'The DAO' was a massive smart contract that raised $117 million to fund Ethereum startups. A flaw in the code allowed hackers to steal $55 million in ether.

The hard fork effectively reversed the transactions by propagating a version of the Ethereum blockchain where the transactions never happened. While the DAO "hack" certainly exposed the vulnerability of smart contracts, many argue that the code executed perfectly and that the fault lies with the DAO and not Ethereum itself. In theory, the agency problem disincentivizes theft of Ethereum since exploiting vulnerabilities weakens the inherent value of the currency. In the future, developers may be more careful to segregate funds into multiple accounts and smart contracts. While the hack exposed a potential flaw in the system, the degree to which Ethereum has bounced back bodes well for the technology in the long term.

Virtually all of the highest profile cryptocurrency hacks have been due to flaws or ethics violations on the part of vendors rather than the protocols themselves.

Headwinds to Adoption

Overall confidence in the system stands as the biggest risk to widespread adoption of bitcoin and blockchain technology. Bitcoin and Ethereum have each generated negative publicity for incidents of hacking or outright theft. The two highest profile bitcoin hacks were Mt. Gox in 2013 and Bitfinix earlier this year. Both examples had more to do with the individual companies playing fast and loose with custodial accounts than fundamental flaws in the protocol. That is not to say that fundamental security risks do not exist. Since the payer in any given transaction will know the most recent inputs and outputs, a malevolent actor can try and steal back the bitcoin they just spent. The payer must outpace the rest of the network mining the "honest" chain and overwrite the transaction seeking to make the fraudulent chain become adopted by the longest chain in the network. The likelihood of pulling off a successful heist decreases exponentially with each additional "honest" block added to the chain. While possible in theory, this does not represent a significant threat given the amount of computing power required to successfully nominate a fraudulent chain.

Furthermore, what protects against more widespread hacking attempts is that exposing flaws would bring down the overall value of the cryptocurrency. Any distributed ledger's greatest vulnerability is to a "51% attack," when one actor controls the majority of mining computing power and can effectively overwrite any blocks they wish. The catch-22 preventing even more of an agency problem is that a compromised blockchain would be nearly worthless. Satoshi structured the bitcoin blockchain to incentivize hackers to cooperate rather than try and exploit the network. At one point the BTC Group controlled 20% of the bitcoin network and once managed to mine six consecutive blocks, a notable feat given the size of the network. The consortium voluntarily disbanded since the perception of a security vulnerability would greatly reduce the value of their massive BTC holdings. The vast size of the entire bitcoin network makes it difficult to capture significant market share. A coordinated effort by the 500 most powerful supercomputers in the world to mine bitcoin would only account for one-ninth of the entire network.

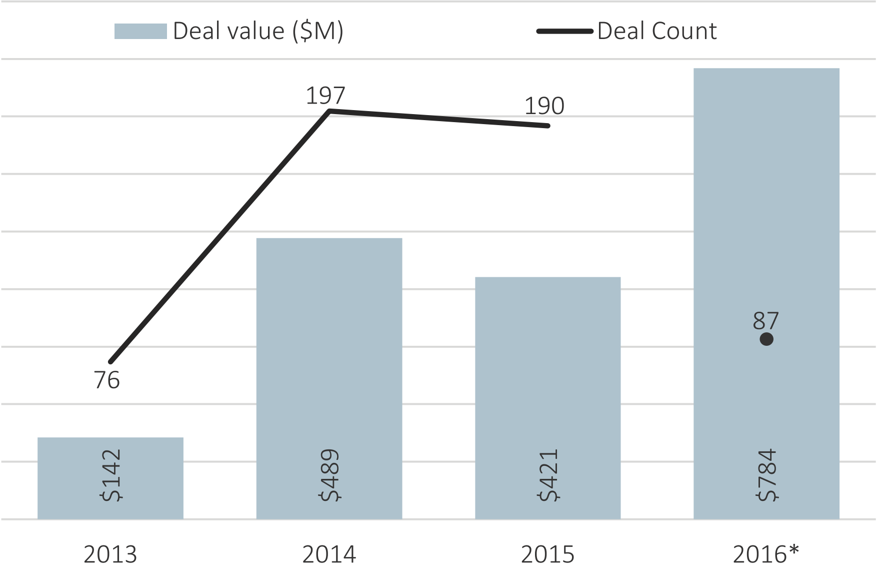
Private Investment and Corporate M&A

DEAL FLOW & CAPITAL INVESTED

Bitcoin- and blockchain-related companies have seen heightened levels of investor interest since the price of bitcoin exceeded $200 in 4Q 2013. Top investors include not just general VCs, but also corporate VC arms, sector-specific VCs, individual angels and banks. Since 2013, a cumulative $1.8 billion of institutional funding has gone into the space across 550 deals. Investor interest peaked in 1Q 2015, when 67 financings were completed, totaling $210 million. Notable rounds in the quarter included cryptocurrency exchange Coinbase's $75 million Series C featuring a16z and Union Square Ventures, and Bitcoin computing startup 21's $52 million Series C, which also included a16z, as well as Pantera Capital and Khosla Ventures.

BITCOIN & BLOCKCHAIN VC DEAL FLOW BY YEAR

(ONLY EQUITY INVESTMENTS INCLUDED)



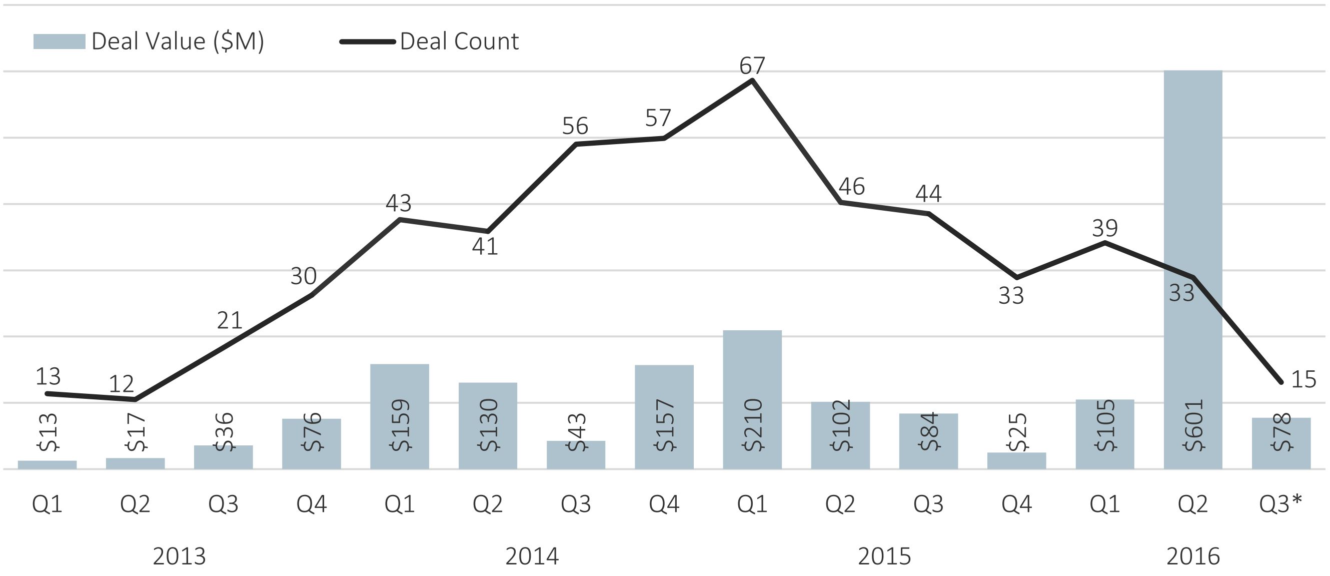
Source: PitchBook
*As of 9/2/2016

Top companies by $ raised	Total raised ($M)
Canaan Creative Company	**$470.56**
Circle Internet Financial	**$136.00**
Coinbase	**$117.21**
21	**$116.05**
Blockstream	**$77.28**
BitFury Group	**$60.00**
Chain	**$43.90**
SETL	**$42.73**
CryptoCorum	**$41.78**
Xapo	**$40.03**
bitFlyer	**$34.07**
BitPay	**$32.80**
KnCMiner	**$32.00**
Blockchain	**$30.50**
Uphold	**$29.26**
itBit	**$28.25**
HKCex	**$27.00**
CoinSeed	**$22.50**
Quoine	**$22.00**
Bitnet	**$14.50**
ABRA (Teller)	**$14.22**
New Continuum Data Centers	**$14.10**
BitGo	**$14.00**
Post-Quantum	**$12.80**
Spondoolies Tech	**$12.50**
SatoshiDICE	**$12.40**
Colu	**$12.10**
Bitaccess	**$10.12**

Source: PitchBook
*As of 9/2/2016

BITCOIN & BLOCKCHAIN VC DEAL FLOW BY QUARTER

(ONLY EQUITY INVESTMENTS INCLUDED)



Source: PitchBook
*As of 9/2/2016

Deal flow has waned so far in 2016, which has seen 87 completed deals through September 2. This comes in an environment of increased belt-tightening by VCs who have seen an increased preference toward easy-to-define business models as opposed to the zero-revenue moonshots that may have received funding in the past. Most bitcoin and blockchain startups represent an entirely new category of business, with fewer comparables to point to. The bulk of the $784 million capital invested in 2016 can be attributed to the CNY 3.1 billion ($470 million) acquisition of Chinese specialty bitcoin-mining hardware manufacturer Canaan Creative by Shandong Luyitong Intelligent Electric in June. This relatively old-school business has a successful product and stable revenues to point to. Other notable deals include payment app maker Circle’s $60 million Series D and bitcoin tool developer Blockstream’s $55 million Series A.

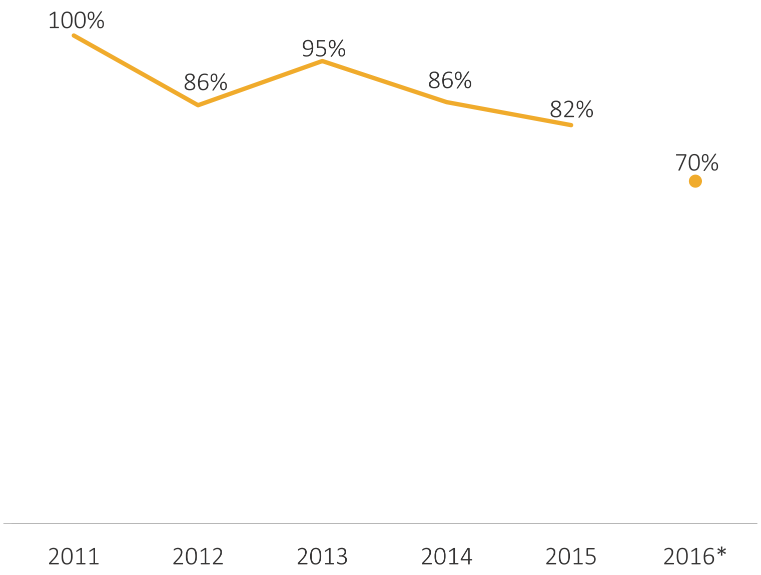
BITCOIN VS. BLOCKCHAIN

Recently, many analysts and pundits have heralded the rise of "blockchain without bitcoin," or "blockchain not bitcoin." However, when looking at investment in the space, 70% of 2016 YTD bitcoin/blockchain financings have gone to bitcoin-related companies. If we were to look at capital invested rather than deal count, the numbers would skew even more heavily toward bitcoin, as the three largest deals so far this year have been a bitcoin mining hardware maker, a bitcoin-based payments platform and a developer of sidechains on the bitcoin protocol.

However, blockchain (excluding bitcoin) investments have accelerated in recent years. As recently as 2013, bitcoin accounted for 95% of all deals in the space, as only four of 76 deals did not involve the bitcoin protocol directly during the period. Year-to-date, this has increased to 26 of 87 deals. Blockchain platforms like Ethereum will only increase interest in the technology and will make possible a range of business models that were previously theoretical. Therefore, we expect the trend of more money flowing into blockchain to continue.

BITCOIN VS. BLOCKCHAIN % OF TOTAL ACTIVITY

(ONLY EQUITY INVESTMENTS INCLUDED)

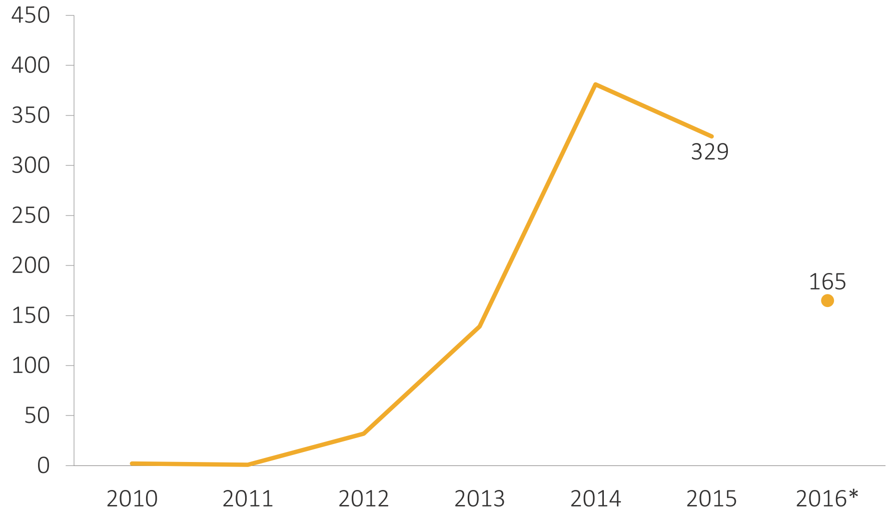


Source: PitchBook
*As of 9/2/2016

ACTIVE & NEW INVESTOR GROWTH

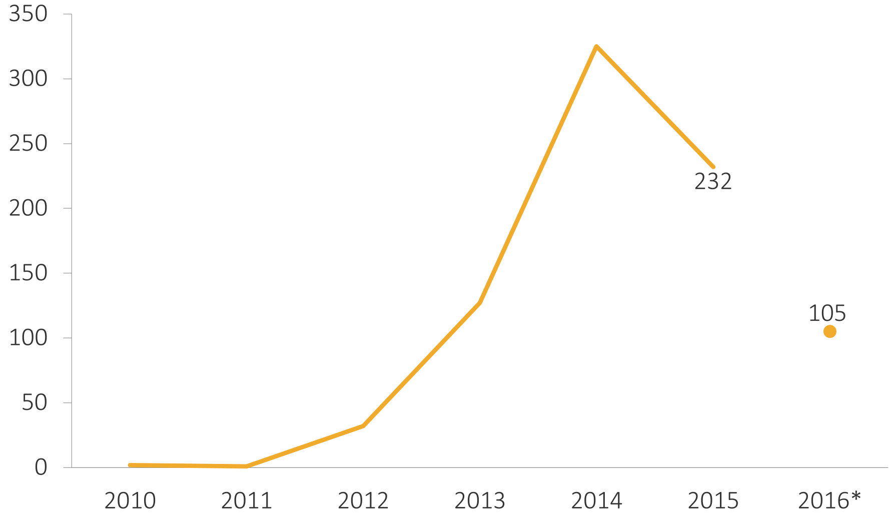
Given the recent development of the space, until very recently, a substantial portion of bitcoin/blockchain investors have been new to the vertical. 2014 saw a peak of 381 investors participating in rounds; A whopping 325 were first time investors, accounting for 85% of participants. While a high number of investors in the space are new, there are a number of blockchain-specialized VCs remaining highly active in the space. Barry Silbert's Digital Currency Group has completed 64 deals since 2013, while Blockchain Capital has completed 42 deals in the same period.

ACTIVE EQUITY INVESTORS (#) IN BITCOIN & BLOCKCHAIN



Source: PitchBook
*As of 9/2/2016

FIRST-TIME EQUITY INVESTORS (#) IN BITCOIN & BLOCKCHAIN



Source: PitchBook
*As of 9/2/2016

Top investors	Deal count (since 2013)
Digital Currency Group	64
Blockchain Capital	42
Boost VC	33
500 Startups	26
Pantera Capital	18
Plug and Play	17
Coinsilium Group	14
RRE Ventures	13
Barry Silbert	13
Roger Ver	12
Sean Percival	12
FundersClub	12
Timothy Draper	11
Techstars	10
Ribbit Capital	8
Future Perfect Ventures	8
Firestartr	8
Ben Davenport	8
SV Angel	7
Paul Veradittakit	7
Saad AlSogair	6
Y Combinator	6
Liberty City Ventures	6
BTCS	6
AME Cloud Ventures	6
Draper Associates	6
Accel Partners	6

Source: PitchBook
*As of 9/2/2016

Moving Forward

Blockchain technology stands at an inflection point. The industry is poised to transition beyond a simple medium for speculators, traders and hobbyists to exchange simple payments and into more sophisticated applications, including smart contracts and micropayments. We think the greatest opportunity around the blockchain comes from the automation of inefficient back-office processes at financial institutions. Banks employ millions of individuals to match trades and settle transactions in an inefficient process susceptible to human error. The existing payments and banking system are a major drag on margins for all sorts of businesses around the globe. Replacing and bolstering back-office operations with robust smart contracts would improve the efficiency, transparency and reliability of the entire financial system, and hence, global economy.

Fintech lacks the luxury of a beta release unlike other emerging technologies, and broader adoption will continue to face headwinds as the technology continuously bounces back from irregular scandals. However, the current state of blockchain feels very much like the internet of the early 1990s. As initial kinks are worked out, the space is one to watch as it offers outsized potential to disrupt arguably the most entrenched and static industry.

We hope this report serves as a valuable resource as you continue to explore this nuanced sector. As the industry continues to mature, we will continue to provide updates on developments and investment trends in the space. As always, feel free to reach out with any comments or questions to reports@pitchbook.com.

Select company profiles

Location: **San Francisco, CA** |
Year Founded: **2012** | Capital Raised to Date: **$142.5M**
First Funding Date: **September 2012** | First Funding Amount: **$600,000**
Latest Funding Date: July 2016 | Latest Funding Amount: **$10.5M** |
Latest Funding Post- Valuation: **$500.5M**

Description: Coinbase operates a digital currency wallet and exchange platform to facilitate merchant and consumer bitcoin and Ethereum payments. Founded in 2012, the company has now expanded to 33 countries. The company debuted the first US bitcoin debit card in 2015 in a partnership with Dwolla and Visa.

21

Location: **San Francisco, CA** | Year Founded: **2013** | Capital Raised to Date: **$116.05M**
First Funding Date: **June 2013** | First Funding Amount: **5.05M**
Latest Funding Date: February 2015 | Latest Funding Amount: **$52M** |
Latest Funding Post- Valuation: **$362M**

Description: 21 provides tools for developers to add bitcoin functionality to online services. The company developed the 21 Computer, software which can turn any desktop into a fully functional bitcoin computer that can send and receive payments. The company also offers a hardware product, the $399 21 bitcoin Computer. The device was designed for developers to create bitcoin-payable apps, services and devices, and can operate as a standalone computer or connect to any Windows, Mac or Linux machine.

BITPESA

Location: **Karen, Nairobi, Kenya** | Year Founded: **2013** |
Capital Raised to Date: **$1.8M**
First Funding Date: **May 2014** | First Funding Amount: **$700,000**
Latest Funding Date: **February 2016** | Latest Funding Amount: **N/A** |

Description: BitPesa provides an exchange platform for bitcoin conversions into and between African currencies, including the Nigerian naira and the shillings of Kenya, Tanzania and Uganda. In addition, it facilitates the sale or withdrawal of bitcoin for mobile money payments and bank transfers. The company allows sending and receiving payments in multiple currencies through its website and mobile app using templates for repeat transactions. Bitcoin can be converted immediately or at a later time with an African bank account or mobile money wallet. The company recently introduced direct payments between African and Chinese bank account holders and an API platform for white-label integration. BitPesa is licensed by the FCA as an authorized payment institution. In February, the company received an undisclosed round of funding from BitFury's investment arm, BitFury Capital.

ripple

Location: **San Francisco, CA** | Year Founded: **2012** | Capital Raised to Date: **$100M** | First Funding Date: **November 2013** | First Funding Amount: **$6.5M**
Latest Funding Date: **September 2016**| Latest Funding Amount: **$55M** | Latest Funding Post- Valuation: **$410M**

Description: Ripple uses its own form of cryptocurrency, XRP, to facilitate large-scale transfers. The system relies on a consensus rather than proof of work to verify payment on a centralized ledger. Ripple functions as a decentralized system of credit, facilitating transactions in both the native XRP cryptocurrency and government-backed fiat. The system automatically routes transactions based upon available credit and bidding for fees. The system does not rely on thousands of decentralized energy-inefficient nodes, but rather a slightly more centralized system of nodes, market makers, and validating servers to provide near instantaneous interbank settlement.

Blockstream

Location: **San Francisco, CA** | Year Founded: **2014** | Capital Raised to Date: **$77.28M**
First Funding Date: November 2014 | First Funding Amount: **$21M**| Latest Funding Date: **February 2016** | Latest Funding Amount: **$55M** |
Latest Funding Post- Valuation: **$77.28M**

Description: Blockstream has developed a blockchain-based mechanism to create cryptographically decentralized IOU such as bitcoin-based cryptocurrency. The company is currently enhancing its sidechain technology, Sidechain Elements: Blockchains that are interoperable with each other and bitcoin to avoid liquidity shortages, market fluctuations, fragmentation, security breaches and outright fraud associated with the use of cryptocurrencies. The company raised $55 million of Series A venture funding in a deal led by Horizons Ventures, AXA Strategic Ventures and DG Incubation in February. The Hive, Data Collective, Digital Currency Group, AME Cloud Ventures, Blockchain Capital, Future Perfect Ventures, Khosla Ventures, Mosaic Ventures and Seven Seas Venture Partners also participated in the round.

XAPO

Location: **Zurich, Switzerland** | Year Founded: **2014** |
Capital Raised to Date: **$40.03M**
First Funding Date: March **2014** | First Funding Amount: **$20M**
Latest Funding Date: **June 2016** | Latest Funding Amount: **$20.03M**

Description: Xapo's primary offering is a bitcoin wallet, although the company also offers an integrable bitcoin debit card. Its bitcoin vault is secured in three layers: cryptographic, with multi-factor authentication and private key segmentation; physical, with storage of offline servers underground in guarded facilities; and jurisdictional, whereby no one government could access other vault locations should one be compromised.

CIRCLE

Location: **Boston, MA** | Year Founded: **2013** | Capital Raised to Date: **$136M**
First Funding Date: **October 2013** | First Funding Amount: **$9M**
Latest Funding Date: **June 2016** | Latest Funding Amount: **$60M** ||
Latest Funding Post- Valuation: **$480M**

Description: A bitcoin broker and wallet platform, Circle offers a web-based or mobile application that employs open internet standards and protocols (including the blockchain) to freely offer international transfer of money. Users may link debit or credit cards or bank accounts in order to send or receive money—the typical fees associated with credit card usage apply. Transactions also typically require two-factor authentication, with specifications possible.

Location: **New York, NY** | Year Founded: **2013** |
Capital Raised to Date: **$8.25M**
First Funding Date: **April 2013** | First Funding Amount: **N/A**
Latest Funding Date: **January 2016** |
Latest Funding Amount: **$7M**

Description: Symbiont has designed a smart contracts platform specifically for institutional financial markets. The company's distributed ledger is "append-only", rendering it immutable and thereby providing a single, global accounting ledger, as all transaction history is replicated by network nodes. Furthermore, users can restrict to necessary organizations and even users by role. More specifically with regard to financial institutions, the securities-related component of Symbiont's platform can model instruments and agreements, support cryptographic authorization and custom workflows and allow for manually initiated or automatic terms and conditions, all stored in the distributed ledger.

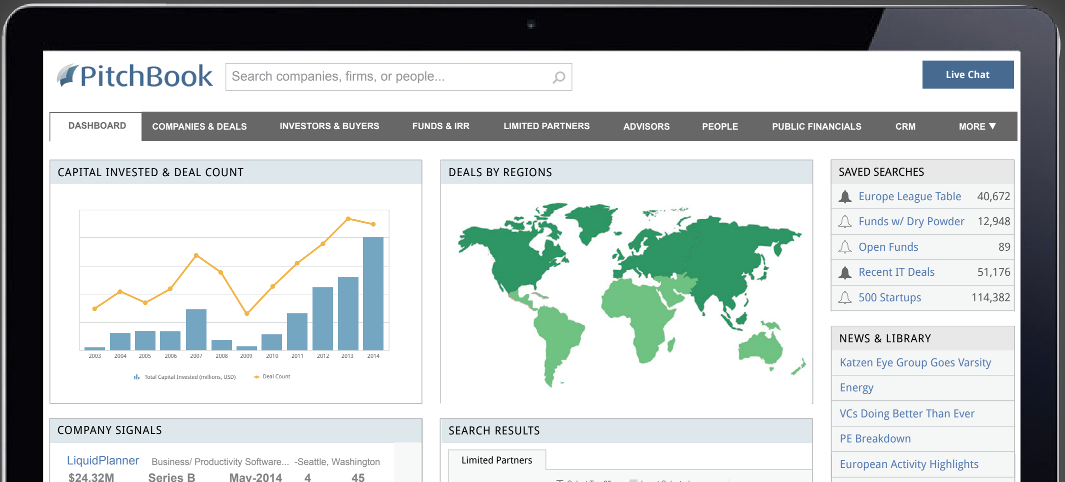
DON'T LET INCOMPLETE DATA LEAVE YOU
IN THE DARK

PitchBook offers more visibility into the private equity & venture capital landscape than any other source

Companies & Deals ○ Valuations & Multiples ○ Funds & Performance ○ Limited Partners ○ Service Providers ○ Investors ○ Financials ○ People

Contact us for a demo of the financial information technology trusted by leading investors, companies and advisors

pitchbook.com | US + 1 206.623.1986 | UK +44 (0) 207.190.9809
demo@pitchbook.com



CAPITAL INVESTED & DEAL COUNT

DEALS BY REGIONS

SAVED SEARCHES	
Europe League Table	40,672
Funds w/ Dry Powder	12,948
Open Funds	89
Recent IT Deals	51,176
500 Startups	114,382

NEWS & LIBRARY

- Katzen Eye Group Goes Varsity
- Energy
- VCs Doing Better Than Ever
- PE Breakdown
- European Activity Highlights

COMPANY SIGNALS

LiquidPlanner Business/ Productivity Software... -Seattle, Washington
$24.32M Series B May-2014 4 45

SEARCH RESULTS