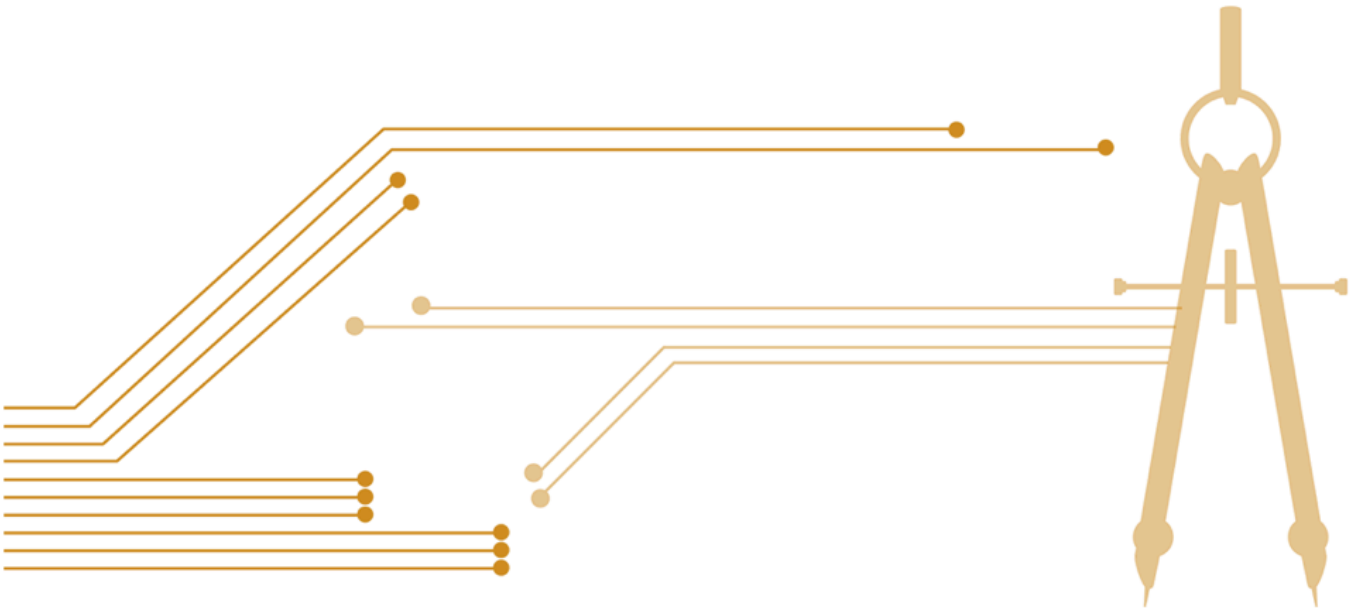
AIR

Applied
Innovation
Review

Issue No. 2
June 2016

Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering

Berkeley



BlockChain Technology: Beyond Bitcoin

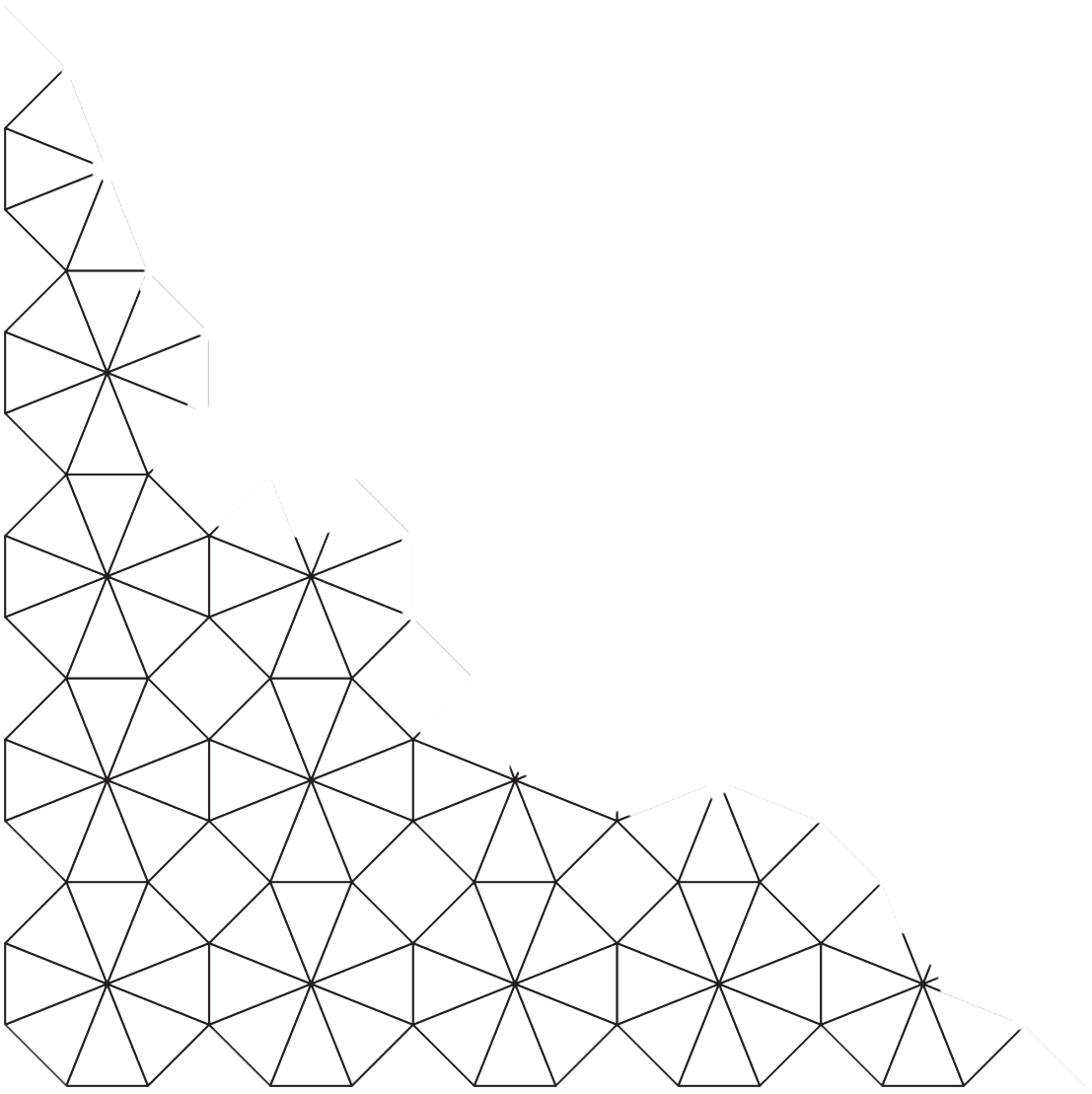
Authors:
Michael Crosby (Google)
Nachiappan (Yahoo)
Pradan Pattanayak (Yahoo)
Sanjeev Verma (Samsung Research America)
Vignesh Kalyanaraman (Fairchild Semiconductor)

Abstract

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world.

The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology, and the revolution in this space has just begun.

This white paper describes blockchain technology and some compelling specific applications in both financial and non-financial sector. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world.



Introduction

A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easier to steal a cookie from a cookie jar, kept in a secluded place, than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people.

Bitcoin is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions.

However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain *distributed consensus model* as the most important invention since the Internet itself. Johann Palychata from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond[1].

Current digital economy is based on the reliance on a certain trusted authority. All online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third party sources can be hacked, manipulated or compromised.

This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a *distributed consensus* where each and every online transaction involving digital assets, past and present, can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The *distributed consensus* and *anonymity* are two important characteristics of blockchain technology.

The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One key emerging use case of blockchain technology involves "*smart contracts*". Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a preconfigured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.

Smart Property is another related concept which is regarding controlling the ownership of a property or asset via blockchain using Smart Contracts. The property can be physical such as car, house or smartphone, or it can be non-physical such as shares of a company. It should be noted here that even Bitcoin is not really a currency: Bitcoin is all about controlling the ownership of money.

Blockchain technology is finding applications in wide range of areas; both *financial* and *non-financial.*

Financial institutions and banks no longer see blockchain technology as a threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications.

Non-Financial applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved.

In this report, we focus on the disruption that every industry in today's digital economy is facing due

to the emergence of blockchain technology. Blockchain technology has potential to become the new engine of growth in digital economy where we are increasingly using Internet to conduct digital commerce and share our personal data and life events.

There are tremendous opportunities in this space and the revolution in this space has just begun. In this report we focus on few key applications of Blockchain technology in the area of Notary, Insurance, private securities and few other interesting non-financial applications. We begin by first describing some history and the technology itself.

Section I: BlockChain Technology

1. Short History of Bitcoin

In 2008, an individual (or group) writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System". This paper described a peer-to-peer version of the electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. Bitcoin was the first realization of this concept. Now "cryptocurrencies" is the label that is used to describe all networks and mediums of exchange that uses cryptography to secure transactions-as against those systems where the transactions are channeled through a centralized trusted entity.

The author of the first paper wanted to remain anonymous and hence no one knows Satoshi Nakamoto to this day. A few months later, an open source program implementing the new protocol was released, beginning with the Genesis block of

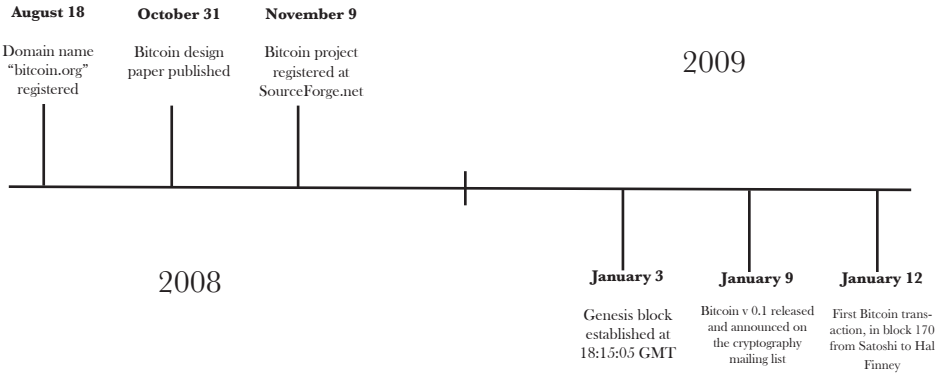


Figure 1: The History of Bitcoin

50 coins. Anyone can install this open source program and become part of the bitcoin peer-to-peer network. It has grown in popularity since then.

The popularity of the Bitcoin has never ceased to increase since then. Moreover, the underlying BlockChain technology is now finding new range of applications beyond finance.

2. Blockchain Technology: How does it work?

We explain the concept of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the blockchain technology is applicable to any digital asset transaction exchanged online.

1. *Validate Entries*
2. *Safeguard Entries*
3. *Preserve Historic Record*

Internet commerce is exclusively tied to the financial institutions serving as the trusted third party who process and mediate any electronic transaction. The role of trusted third party is to validate, safeguard and preserve transactions. A certain percentage of fraud is unavoidable in online transactions and that needs mediation by financial transactions. This results in high transaction costs.

Bitcoin uses cryptographic proof instead of the trust-in-the-third-party mechanism for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature, is sent to the "public key" of the receiver, and is digitally signed using the "private key" of the sender. In order to spend money, the owner of the cryptocurrency needs to prove his ownership of the "private key".

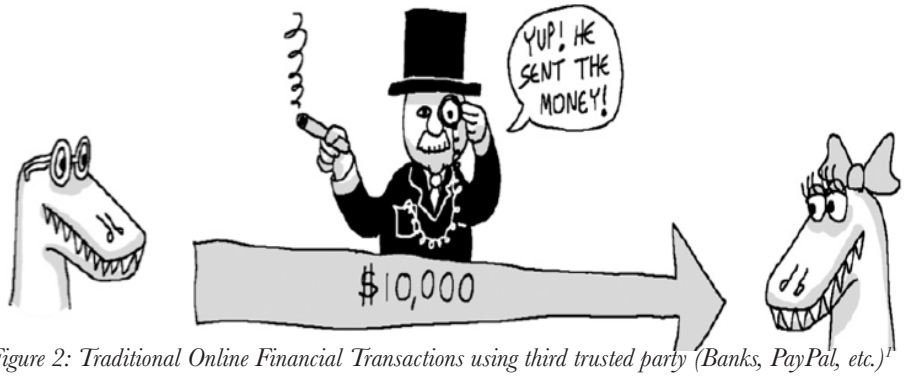


Figure 2: Traditional Online Financial Transactions using third trusted party (Banks, PayPal, etc.)[1]

The entity receiving the digital currency then verifies the digital signature, which implies ownership of the corresponding "private key", by using the "public key" of the sender on the respective transaction.

Each transaction is broadcasted to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger. The verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency, through the digital signature verification on the transaction.

2. Spender has sufficient cryptocurrency in his account, through checking every transaction against the spender's account, through checking every transaction against the spender's account, or "public key", that is registered in the ledger. This ensures that there is sufficient balance in his account before finalizing the transaction.

However, there is question of maintaining the order of these transactions that are broadcasted to every other node in the Bitcoin peer-to-peer network. The transactions do not come in order in which they are generated, and hence there is a need for a system to make sure that double-spending of the cryptocurrency does not occur. Considering that the transactions are passed node by node through the Bitcoin network, there is no guarantee that orders in which they are received at a node are the same order in which these transactions were generated. The above means that there is a need to develop a mechanism so that the entire Bitcoin network can agree regarding the order of transactions, which is a daunting task in a distributed system.

The Bitcoin solved this problem by a mechanism that is now popularly known as Blockchain technology. The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are considered to have happened at the same time. These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous block.

There still remains one more problem: Any node in the network can collect unconfirmed transactions and create a block and then broad

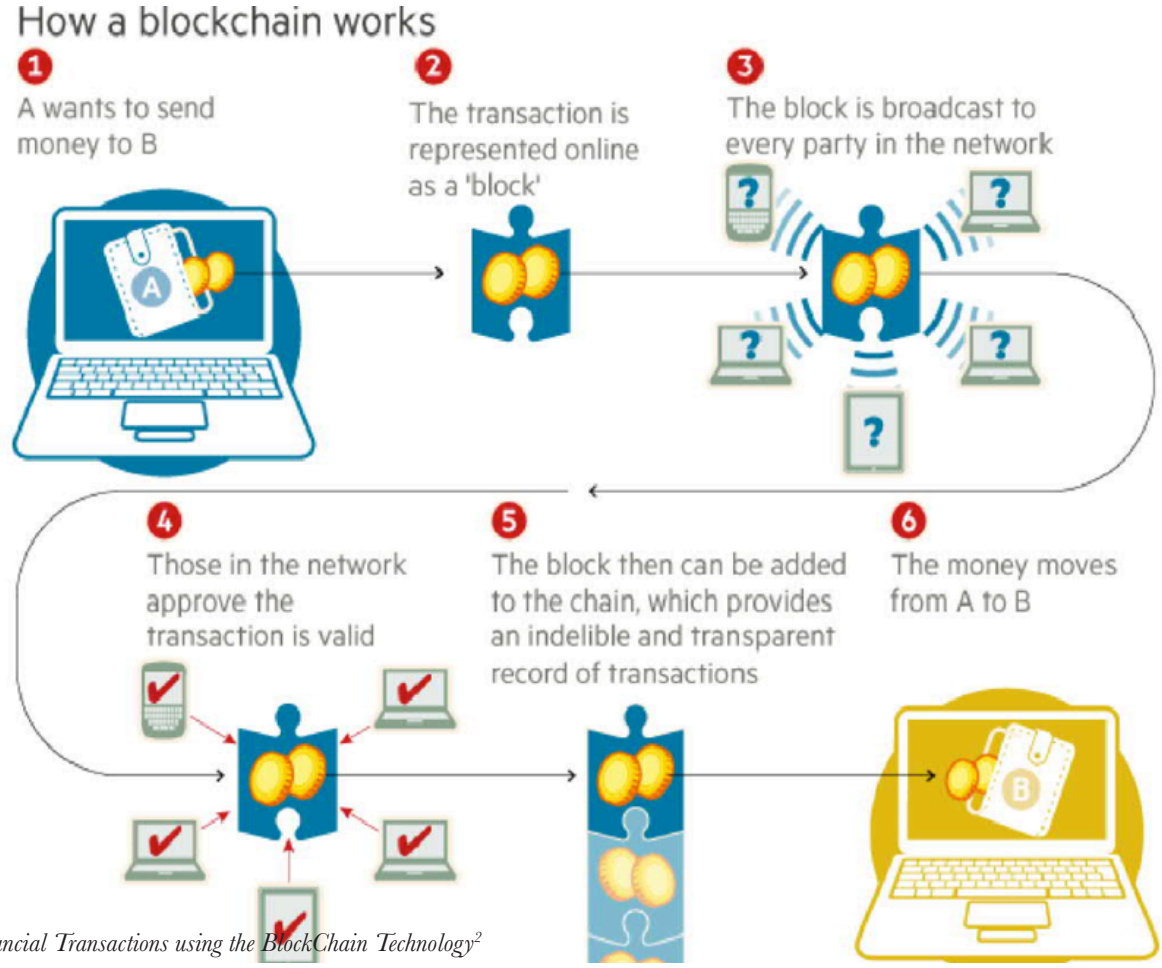


Figure 3: Financial Transactions using the BlockChain Technology[2]

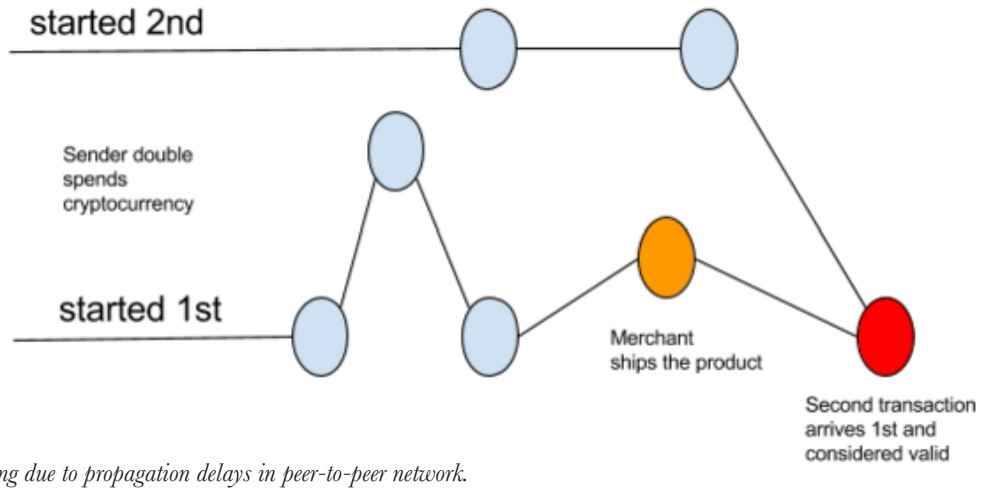


Figure 4: Double spending due to propagation delays in peer-to-peer network.

cast it to the rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain? There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network.

Bitcoin solves this problem by introducing a mathematical puzzle: each block will be accepted in the block chain provided it contains an answer to a very special mathematical problem.

This is also known as "proof of work": a node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For instance, a node can be required to find a "nonce" which when hashed with both transactions and hashes of previous blocks produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

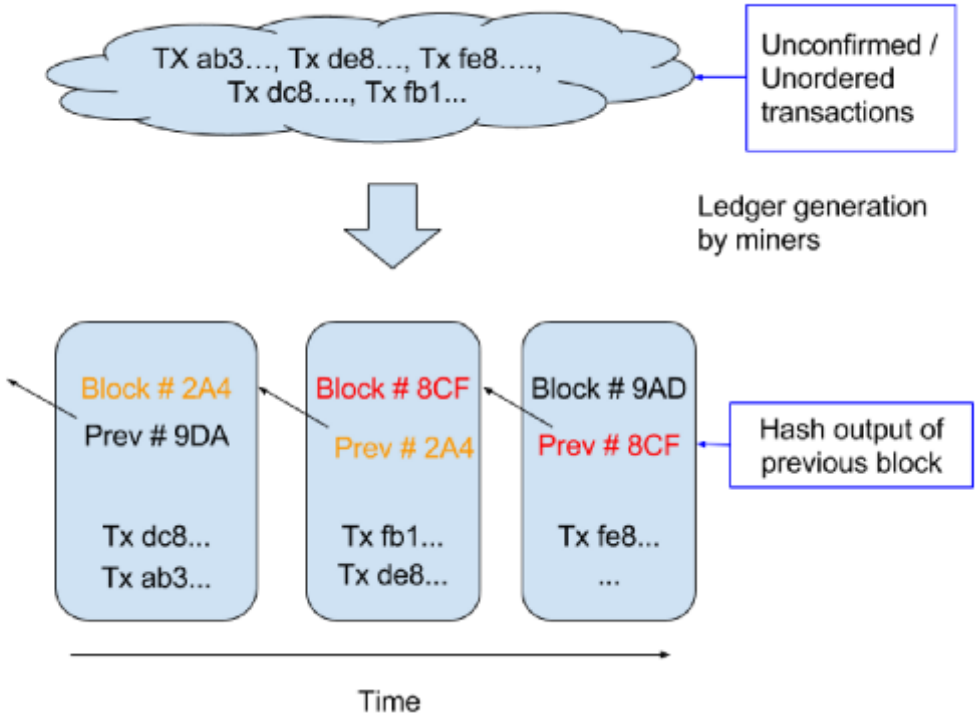


Figure 5: Generation of BlockChain from unordered transactions

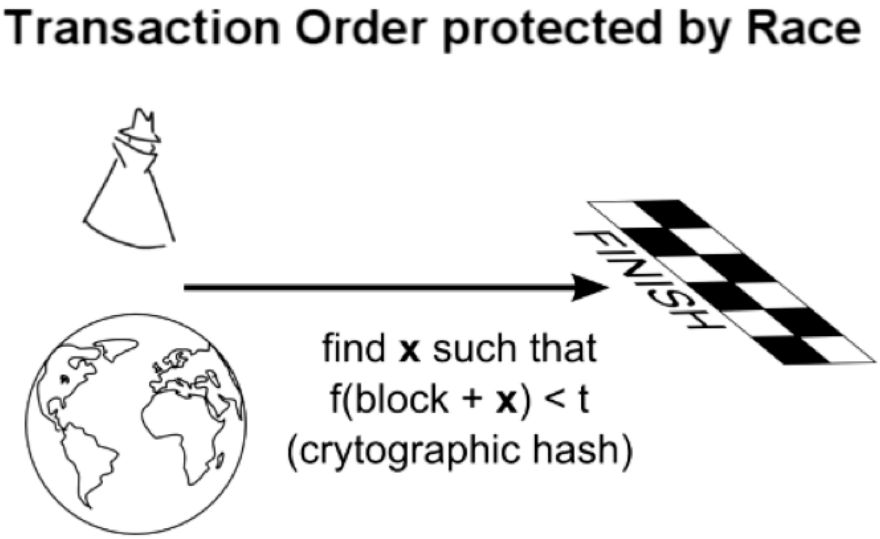


Figure 6: Mathematical race to protect transactions - I[4]

This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that on average it takes ten minutes for a node in the Bitcoin network to make a right guess and generate a block. There is very small probability that more than one block will be generated in the system at a given time. The first node, to solve the problem, broadcasts the block to the rest of the network. Occasionally, however, more than one block will be solved at the same time, leading to several possible branches. However, the math needed to be solved is very complicated and hence the blockchain quickly stabilizes: after this, every node is in agreement about the ordering of blocks.

The nodes donating their computing resources to solve the puzzle and generate blocks are called "miner" nodes" and are financially awarded for their efforts.

The network only accepts the longest blockchain as the valid one. Hence, it is next to impossible for an attacker to introduce a fraudulent transaction since it has not only to generate a block by solving a mathematical puzzle, but it also has to race mathematically against the good nodes to generate all subsequent blocks in or-

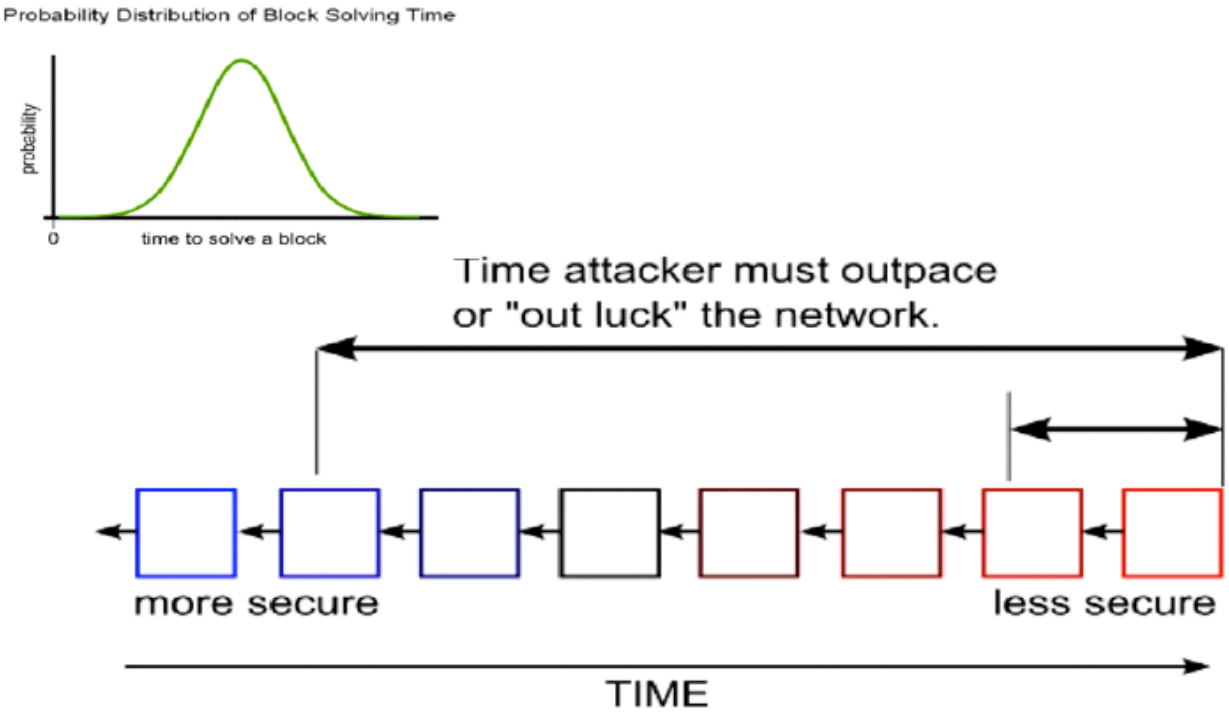


Figure 7: Mathematical race to protect transactions - II[4]

der for it to make the other nodes in the network accept its transaction and block as the valid one. This job becomes even more difficult since blocks in the blockchain are linked cryptographically together.

Section II: Existing Market

Blockchain technology is finding applications in both financial and non-financial areas that traditionally relied on a third trusted online entity to validate and safeguard online transactions of digital assets. There was another application "Smart Contracts" that was invented in year 1994 by Nick Szabo. It was a great idea to automatically execute contracts between participating parties. However, it did not find usage until the notion of crypto currencies or programmable payments came into existence. Now the two programs, Blockchain and Smart Contracts can work together to trigger payments when a preprogrammed condition of a contractual agreement is triggered. Smart Contracts are really the killer application of the cryptocurrency world.

Smart Contracts are contracts which are automatically enforced by computer protocols. Using blockchain technology has made it much more easier to register, verify and execute them. Moreover, open source companies like Ethereum and Codius are already enabling Smart Contracts using blockchain technology and many companies which operate on bitcoin and blockchain technologies are beginning to support Smart Contracts. Many cases where assets are transferred only after meeting certain conditions, which require Lawyers to create a contract and Banks to provide Escrow services, can be replaced by Smart Contracts. In particular, Ethereum has created lot of excitement for its programmable platform capabilities. The company allows anyone to create their own cryptocurrency and use that to execute and pay for Smart Contracts, while it also possesses its own cryptocurrency (ether) which is used to pay for the services. Ethereum is already powering a wide range of early applications in areas such as Governance, autonomous banks, keyless access, crowdfunding, financial derivatives trading and settlement, all by using Smart Contracts.

Also, there are a number of blockchains in existence to support a wide range of applications besides cryptocurrency. Currently there are three approaches in the industry to support other applications and overcome perceived limitations of Bitcoin blockchain:

Alternative Blockchains: A system of using the blockchain algorithm to achieve distributed consensus on a particular digital asset. The system may share miners with a parent network such as Bitcoin's, which is called merged mining. These Alternative Blockchains have been suggested to implement applications such as DNS, SSL certification authority, file storage and voting.

Colored Coins: An open source protocol that describes a class of methods for developers to create digital assets on top of Bitcoin blockchain by using its functionalities beyond digital currency.

Sidechains: Alternative Blockchains which are backed by Bitcoins via a Bitcoin Contract, just as dollars and pounds used to be backed by Gold. One can possibly have a thousands of Sidechains "pegged" to Bitcoin, all with different characteristics and purposes, and all of them taking advantage of the scarcity and resilience guaranteed by the Bitcoin blockchain. In turn, the Bitcoin blockchain can iterate to support additional features for these experimental Sidechains, once they have been tried and tested.

Companies such as IBM, Samsung, Overstock, Amazon, UBS, Citi, Ebay, and Verizon Wireless, to name a few, are all exploring alternative and novel uses of the blockchain for their own applications. Nine of the world's biggest banks including Barclays and Goldman Sachs[5] have recently joined forces with the New York based financial technology firm R3 in September 2015 in order to create a framework for using the blockchain technology in the financial market. This is the first time banks have come to work together to find applications of blockchain technology. Leading banks like JP-Morgan, State Street, UBS, Royal Bank Of Scotland, Credit Suisse, BBVA and Commonwealth Bank of Australia have joined this initiative.

Now we turn to give a short description of the types of interesting applications and projects that innovative and visionary companies are doing in this space.

Section III: Applications of Technology-Compelling Use Cases in both Financial and Non-Financial Areas

1. Financial Applications:

1.1. *Private Securities*

It is very expensive to take a company public. A syndicate of banks must work to underwrite the deal

and attract investors. The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner. It is now theoretically possible for companies to directly issue the shares via the blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the blockchain. Here are some examples:

NASDAQ Private Equity: NASDAQ launched its Private Equity Exchange in 2014[6]. This is meant to provide the key functionalities like Cap table and investor relationship management for the the pre-IPO or private companies. The current process of trading stocks in this exchange is inefficient and slow due to involvement of multiple 3rd parties. NASDAQ has joined hands with a San Francisco based Startup called *chain.com*[7] to implement private equity exchange on top of BlockChain. Chain.com is implementing BlockChain based smart contracts to implement exchange functionality. This product is expected to be fast, traceable and efficient.

Medici is being developed as a securities exchange that uses the Counterparty implementations of Bitcoin 2.0. The goal here is to create a cutting edge stock market. Counterparty is a protocol that implements traditional financial instruments as the self-executing smart contracts. These smart contracts facilitate, verify or enforce the negotiation of contracts and eliminate the need for a physical document. This eliminates the need for an intermediary, such as a broker, exchange or bank.

Blockstream is an open source project with focus on Sidechains to avoid fragmentation, security and other issues related to alternative cryptocurrencies. Uses can range from registering securities, such as stocks, bonds and derivatives, to securing bank balances and mortgages.

Coinsetter is a New York based bitcoin exchange. It is working on a Project Highline, a method of using the blockchain to settle and clear financial transactions in T+ 10 minutes rather than the customary T+3 or T+2 days.

Augur is a decentralized prediction market that will allow users to buy and sell shares in anticipation of an event with the probability that a specific outcome occurs. This can also be used to make financial and economic forecasts based on the "wisdom of crowds".

Bitshares are digital tokens that reside in the blockchain and reference specific assets such as currencies or commodities. The Token holders may have the unique feature of earning interest on commodities, such as gold, and oil, as well as dollars, euros and currency instruments.

1.2 *Insurance*

Assets which can be uniquely identified by one or more identifiers that are difficult to destroy or replicate can be registered in blockchain. This can be used to verify ownership of an asset and also trace the transaction history. Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in blockchain and the ownership, transaction history can be validated by anyone, especially insurers.

Everledger is a company which creates permanent ledger of diamond certification and the transaction history of the diamond using blockchain. The characteristics which uniquely identify the diamond such as height, width, weight, depth, color etc are hashed and registered in the ledger. The verification of diamonds can be done by insurance companies, law enforcement agencies, owners and claimants. Everledger provides a simple to use web service API for looking at a diamond, and create, read or update claims by insurance companies, and to the same for police reports on diamonds.

2. Non-Financial Applications:

2.1 *Notary Public*

Verifying authenticity of the document can be done using blockchain and eliminates the need for centralized authority. The document certification service helps in Proof of Ownership (who authored it), Proof of Existence (at a certain time) and Proof of Integrity (not tampered) of the documents. Since it is counterfeit-proof and can be verified by independent third parties, these services are legally binding. Using blockchain for notarization secures the privacy of the document as well as those who seek certification. By publishing proof of publication using cryptographic hashes of files into blockchain takes the notary timestamping to a new level. Using blockchain technology also eliminates the need for expensive notarization fees and ineffective ways of transferring documents.

Stampery is a company which can stamp email or any files using blockchain. It simplifies certifying of emails by just emailing them to an email specifically created for each customer. Law firms are using Stampery's technology for a very cost effective way to certify documents.

Viacoin is one of the companies which uses clearinghouse protocol for notary service.

Block Notary is an iOS app which helps you create proof of existence of any content (photo, files, any media) using TestNet3 or a Bitcoin network.

Crypto Public Notary uses Blockchain of Bitcoin to notarize documents by using trivial amount of bitcoins to record the file's checksum in a public blockchain.

Proof of Existence is another service which uses blockchain to SHA256 digest of the document in bitcoin blockchain.

Ascribe is another company which does authorship certification using blockchain. It also offers transfer of ownership service with attribution to the original author.

2.2 *Applications of Blockchain in the Music Industry*

The music industry has gone a big change in last decade due to the growth of Internet and availability of a number of streaming services over the Internet. This change is impacting everyone in the music industry: artists, labels, publishers, songwriters and streaming service providers. The process by which music royalties are determined has always been a convoluted one, but the emergence of the Internet has made it even more complex giving rise to the demand of transparency in the royalty payments by both artists and songwriters.

This is where the blockchain can play a role. The technology can help mantain a comprehensive and accurate distributed database of music rights ownership information in a public ledger. In addition to rights ownership information, the royalty split for each work, as determined by Smart Contracts, could be added to the database. This Smart Contracts would in turn define the relationship relationships between different stakeholders (addresses) and automate their interactions

2.3 *Decentralized proof of existence of documents*

Validating the existence or the possession of signed documents is very important in any legal solution. The traditional document validation models rely on central authorities for storing and validating the documents, which presents some obvious security challenges. These models become even more difficult as the documents become older.

The blockchain technology provides an alternative model to proof-of-existence and possession of legal documents. *Proof of Existence* is a simple service that allows one to anonymously and securely store online proof of existence of any document. This service simply stores the cryptographic digest of the file, linked to the time in which a user submits his document. It is worth noting that the cryptographic digest or fingerprint is what is stored, and not the actual document. In this way, the user does not need to worry about the privacy aspect and protecting his information.

This allows then a user to later certify the existence of a document that existed at a certain time.

By leveraging the blockchain, a user can simply store the signature and timestamp associated with a legal document in the blockchain and validate it anytime using native blockchain mechanisms.

The major advantages of this service is security and privacy that allow a user to give decentralized proof of the document that can't be modified by a third party. The existence of the document is validated using blockchain that does not depend on a single centralized entity. Proof of Existence webservice is available at *https://proofofexistence.com/*.

2.4 *Decentralized Storage*

Cloud file storage solutions such as Dropbox, Google Drive or One Drive are growing in popularity to store documents, photos, video and music files. Despite their popularity, cloud file storage solutions typically face challenges in areas such as security, privacy and data control. The major issue is that one has to trust a third party with one's confidential files.

Storj provides a blockchain based peer-to-peer distributed cloud storage platform (see Appendix for detailed description) that allows users to transfer and share data without relying on a third party data provider. This allows people to share unused internet bandwidth and spare disk space in their personal computing devices to those looking to store large files in return for bitcoin based micropayments.

Absence of a central control eliminates most traditional data failures and outages, as well as significantly increasing security, privacy and data control. Storj's platform depends upon a challenge algorithm to offer incentivization for users to properly participate in this network.

In this way, Storj can periodically check the integrity and availability of a file cryptographically, and offer direct rewards to those maintaining the file.

In this example, Bitcoin-based micropayments serve as both an incentive and method of payment while a separate blockchain is used as a datastore for file metadata.

2.5 *Decentralized IoT*

The *Internet of Things (IOT)* is increasingly becoming a popular technology in both the consumer and the enterprise space. A vast majority of IOT platforms are based on a centralized model in which a broker or hub controls the interaction between devices. However, this approach has become impractical for many scenarios in which devices need to exchange data between themselves autonomously. This specific requirement has lead to efforts towards decentralized IoT platforms.

The blockchain technology facilitates the implementation of decentralized IoT platforms such as secured and trusted data exchange as well as record keeping. In such an architecture, the blockchain serves as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology.

IBM, in partnership with Samsung, has developed a platform ADEPT (Autonomous Decentralized Peer To Peer Telemetry) that uses elements of the bitcoin's underlying design to build a distributed network of devices, or decentralized Internet of Things (IOT). ADEPT uses three protocols in the platform: BitTorrent (file sharing), Ethereum (Smart Contracts) nd TeleHash (Peer-To-Peer Messaging).

Filament is a startup that provides a decentralized IoT software stack that uses the bitcoin blockchain to enable devices to hold unique identities on a public ledger.

2.6 *BlockChain based Anti-Counterfeit Solutions*

Counterfeiting is one of the biggest challenges in modern commerce. In particular, it is one of the biggest challenges that digital commerce world faces today. Existing solutions are based on reliance on trust on a third party trusted entity that introduces a logical friction between merchants and consumers.

The blockchain technology, with its decentralized implementation and security capabilities, provides an alternative to existing anti-counterfeiting mechanisms. One can envision a scenario in which brands, merchants and marketplaces are part of a blockchain network with nodes storing information to validate the authenticity of the products. With the use of this technology, stakeholders in the supply chain need not rely on a centralized entity for authenticity of the branded products.

BlockVerify provides blockchain based anti-counterfeit solutions that introduce transparency to supply chains. It is finding applications in the pharmaceutical, luxury items, diamonds and electronics industries.

2.7 *Internet Applications*

Namecoin is an alternative blockchain technology (with small variations) that is used to implement a decentralized version of Domain Name Server (DNS) that is resilient to censorship. Current DNS servers are controlled by governments and large corporations, and could abuse their power to censor, hijack, or spy on a consumer's Internet usage. With Blockchain technology Internet's DNS or phonebook is maintained in a decentralized manner and every user can have the same phone book data on their computer.

Public Key Infrastructure (PKI) technology is widely used for centralized distribution and management of digital certificates. Every device needs to have root certificate of the Certification Authority (CA) to verify digital signature. While PKI has been widely deployed and incredibly successful, dependence on a CA makes scalability an issue.

The characteristics of the BlockChain can help address some of the limitations of the PKI by using Keyless Security Infrastructure (KSI). KSI uses cryptographic hash functions, allowing verification to rely only on the security of hash functions and the availability of a blockchain.

Section IV: Risks of Adoption

BlockChain is a promising breakthrough technology. As we described before, there are vast array of applications or problems that can be solved using BlockChain based technology, spanning from Financial (remittance to investment banking) to non-financial applications like Notary services.

Most of these are radical innovations. As it happens with the adoption of radical innovations, there are significant risks of adoption.

Behavior change: Change is constant, but there is resistance to change. In the world of non-tangible trusted third parties introduced by BlockChain, customers need to get used to the fact that their electronic transactions are safe, secured and complete. The present day intermediaries like Visa or Mastercard (in case of a credit cards) will also go through a change of roles and responsibilities. We envision that these companies will also invest and move their platforms to be BlockChain-based. They will continue to provide services to further customer relationship.

Scaling: Scaling of the current nascent services based on BlockChain presents a challenge. Imagine yourself executing a BlockChain transaction for the first time. You will have to go through downloading the entire set of existing BlockChains and validate before executing your first transaction. This may take hours or longer as the number of blocks increase exponentially.

Bootstrapping: Moving the existing contracts or business documents/ frameworks to the new BlockChain based methodology presents a significant set of migration tasks that need to be executed. For example, in case of Real Estate ownerships,, the existing documents lying in County or Escrow companies need to be migrated to the equivalent BlockChain form. This may involve time and costs.

Government Regulations: In the new world of BlockChain-based transactions, government agencies like FTC and SEC may slow down the adoption by introducing new laws to monitor and regulate the industry for compliance. In a way, this may help adoption in the United States as these agencies carry customer trust. In more controlled economies like China, the adoption will face significant headwind.

Fraudulent Activities: Given the pseudonymous nature of BlockChain transactions, coupled with ease of moving valuables, the "bad guy"s may misuse the technology for fraudulent activities like money trafficking. That said, with enough regulations and technology-support, law enforcement agencies will be able to monitor and prosecute these individuals.

Quantum Computing[8]: The basis of BlockChain technology relies on the very fact that it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the future advent of Quantum Computers, the cryptographic keys may be easy enough to crack within a reasonable time through a sheer brute force approach. This would bring the whole system to its knee. The counter-argument would be for keys to become even stronger so that they may not be easy to crack.

Section V: Corporate Funding & Interest

In 2015, the bitcoin currency has reached yearly highs in both volume and price over the course of September-October. The digital currency is gaining traction both in the consumer marketplace as a tradeable security, as well as with regulators. It isn't just digital-currency enthusiasts that are bullish: equity research firm Wedbush expects it to rise to $600 because of its growind adoption.

This enthusiasm may be because of the large quantities of capital being injected into the digital infrastructure. Excitement grows as Bitcoin and blockchain firms have received a record US$1 Billion in investment as 2015 came to an end. American Express, Bain Capital, Deloitte, Goldman Sachs, MasterCard, the New York Life Insurance Company, the New York Stock Exchange; all of them have poured millions of dollars into Bitcoin firms recently.

Corporate funding into Bitcoin & Blockchain infrastructure is growing and generating interest in several segments. Nasdaq is tapping blockchain technology to create a more secure, efficient system to trade stocks. DocuSign, a company that specializes in electronic contracts, just unveiled a joint idea with Visa to use blockchain to track car rentals and reduce paperwork. Microsoft will unveil details about its venture into Smart Contracts that use blockchain technology. Meanwhile, this new obsession with blockchain technology has reached a point that companies are even experimenting with creating smaller, "private blockchains" inside their own offices: for example, they are hiring companies like BlockCypher, a startup out of Redwood City, California to develop blockchain technology within their own business.

Conclusion

BlockChain is Bitcoin's backbone technology. The distributed ledger functionality coupled with the security of BlockChain makes it a very attractive technology to solve the current financial as well as non-financial industry problems.

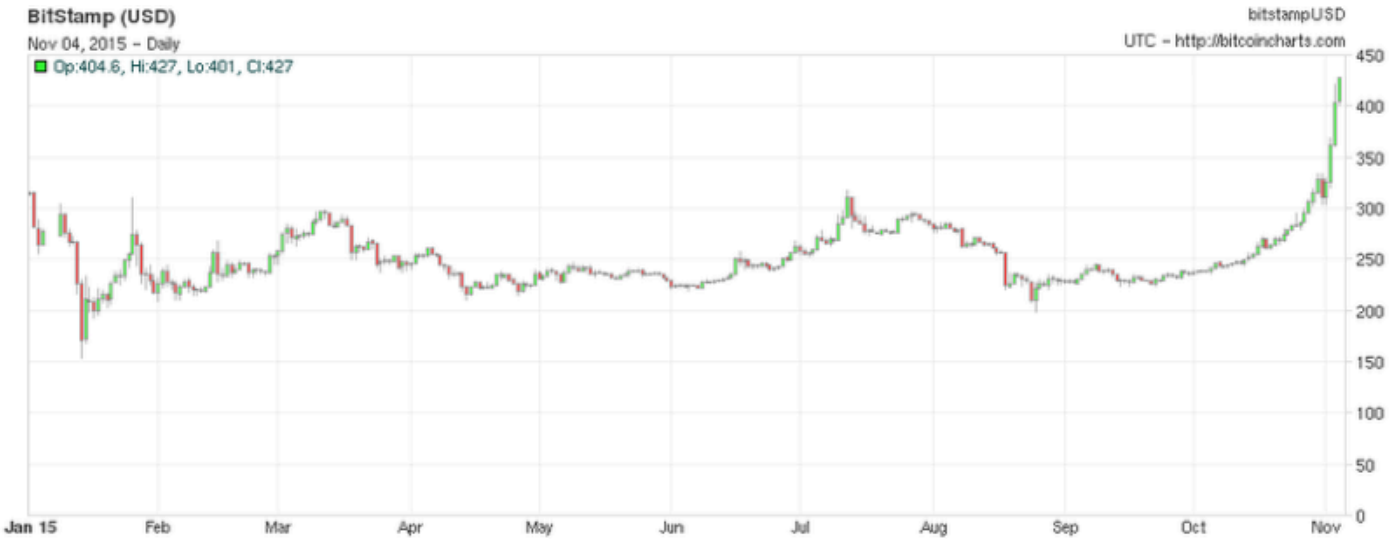


Figure 8: Bitcoin price in 2015[9].

As far as the technology is concerned, the cryptocurrency-based technology is either in the down ward slope of inflated expectations or in trough of disillusionment as shown in Figure 10 in the next page.

There is enormous interest in BlockChain-based business applications and hence numerous start-ups working on them. The adoption definitely faces strong headwind as described before. However, even large financial institutions such as Visa, Mastercard, Banks, and NASDAQ, are investing in exploring applications of current business models on BlockChain. In fact, some of them are searching for new business models in the world of BlockChain.

Some would like to stay that they are even ahead of the curve in terms of transformed regulatory environments for BlockChain[1].

We envision BlockChain technology going through slow adoption due to the risks associated. Most of the start-ups will fail with few winners. Having said this, we should be seeing significant adoption in a decade or two.

Close Date	Company	Classification	Round Size ($m)	Cumulative Funding ($m)	Round
6-Oct-2015	Orb	Financial Services	2.30	2.70	Seed
2-Oct-2015	Coinplug	Universal	5.00	8.30	Second
29-Sep-2015	Safe Cash Payment Technologies	Financial Services	1.12	1.12	Seed
17-Sep-2015	Pey	Infrastructure	0.34	0.34	Seed
10-Sep-2015	Coinalytics	Financial Services	1.10	1.20	Seed
10-Sep-2015	Abra	Financial Services	12.00	14.00	First
10-Sep-2015	Case	Wallet	1.00	2.25	Seed
9-Sep-2015	Chain	Infrastructure	30.00	43.70	Second
8-Sep-2015	ShapeShift	Exchange	1.60	2.13	First
2-Sep-2015	Paymium	Payment Processor	1.12	1.12	Seed

Figure 9: VC funcing in Sep/Oct 2015

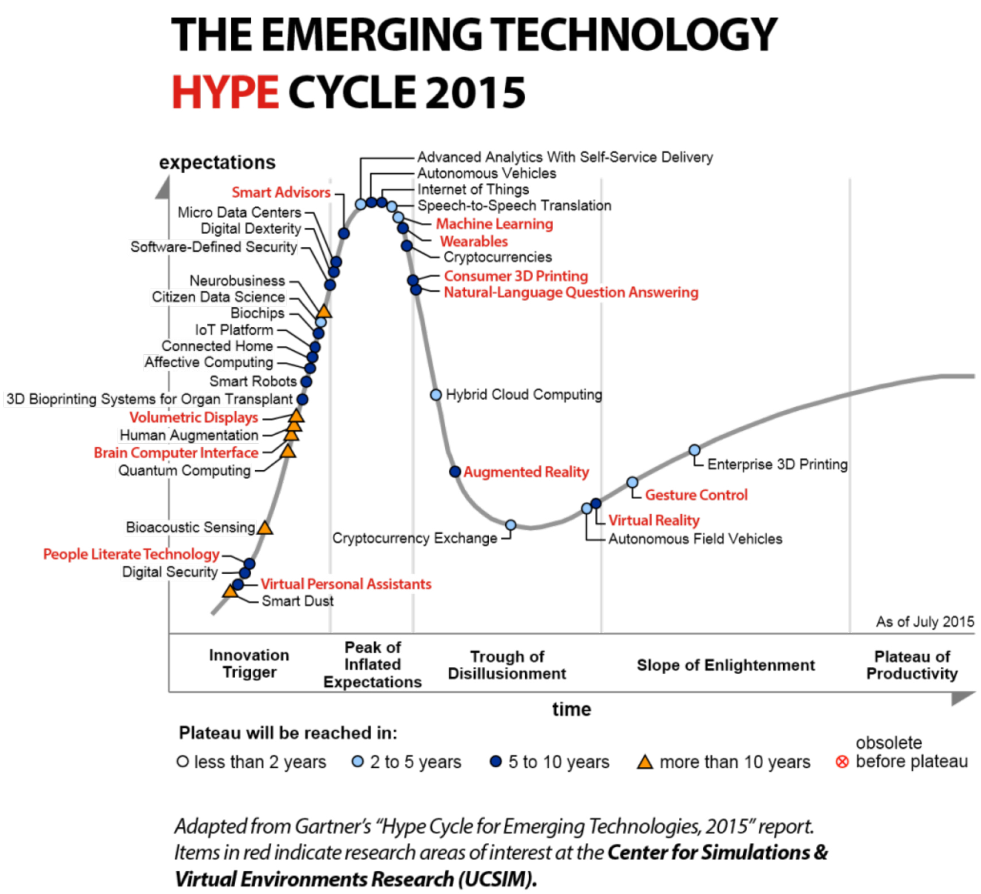


Figure 10: VC Showing cryptocurrencies in the trough of dissillusionment in Gertner's Hype Cycle[10].

References

1. Borenstein, Joram. "A Risk-Based View of Why Banks Are Experimenting with Bitcoin and the Blockchain." *Spotlight on Risk Technology.* N.p., 18 Sept. 2015. Web. 03 May 2016.

2. Barski, Conrad, and Chris Wilmer. "The Blockchain Lottery: How Miners Are Rewarded - CoinDesk." *CoinDesk RSS.* CoinDesk, 23 Nov. 2014. Web. 03 May 2016.

3. Wild, Jane, Martin Arnold, and Philip Stafford. "Technology: Banks Seek the Key to Blockchain - FT.com." *Financial Times.* N.p., 1 Nov. 2015. Web. 03 May 2016.

4. Driscoll, Scott. "How Bitcoin Works Under the Hood". *Imponderable Things.* Jul.14,2013. Web. 03 May 2016.

5. Kelly, Jemima. "Nine of World's Biggest Banks Join to Form Blockchain Partnership." *Reuters.* Thomson Reuters, 15 Sept. 2015. Web. 03 May 2016.

6. "Why NASDAQ Private Market." *Nasdaq Private Market |.* N.p., n.d. Web. 03 May 2016.

7. "Chain | Enterprise Blockchain Infrastructure." *Chain | Enterprise Blockchain Infrastructure.* N.p., n.d. Web. 03 May 2016.

8. Infante, Andre. "Quantum Computers: The End of Cryptography?"- *MakeUseOf.* N.p., 16 Nov. 2014. Web. 03 May 2016.

9. Lee, Timothy B. "Bitcoin's Value Is Surging. Here Are 5 Charts on the Growing Bitcoin Economy." *Vox.* N.p., 03 Nov. 2015. Web. 03 May 2016.

10. Rivera, Janessa. "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor." *Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor.* N.p., 18 Aug. 2015. Web. 03 May 2016.