Kanpur Philosophers
ISSN 2348-8301
International Journal of humanities, Law and Social Sciences
Published biannually by New Archaeological & Genological Society
Kanpur India
Vol. X, Issue I(K): 2023

BLOCKCHAIN TECHNOLOGY

Ms. Vaishali Mishra, Assistant Professor**,** Department of Information and Technology**,** Nirmala Memorial Foundation College of Commerce and Science

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. And, 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 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. And, 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 easy 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'sblockchain, 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.

Current digital economy is based on the reliance on a certain trusted authority. Our 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, past and present, involving digital assets 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 pre-configured 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, smartphone etc. 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 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 today 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 year 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 word 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 that began with the Genesis block of 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.

– 2008	
• **August 18**	Domain name "bitcoin.org" registered
• **October 31**	Bitcoin design paper published
• **November 09**	Bitcoin project registered at SourceForge.net
– 2009	
• **January 3**	Genesis block established at 18:15:05 GMT
• **January 9**	Bitcoin v0.1 released and announced on the cryptography mailing list
• **January 12**	First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

The popularity of the Bitcoin has never ceased to increase since then. 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.

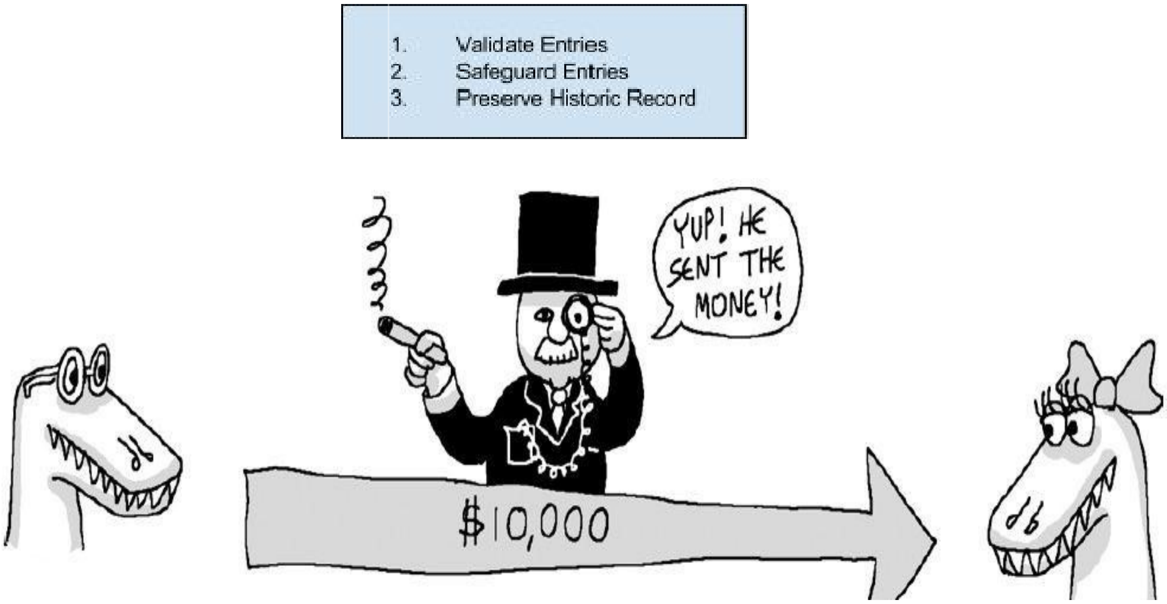

Figure 1. Traditional online financial transactions using third trusted party (Banks, Paypal etc.)[1].

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 for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to spend money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency verifies the digital signature –thus ownership of corresponding "private key"--on the transaction using the "public key" of the sender.

Each transaction is broadcast 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. Verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency—digital signature verification on the transaction.
2. Spender has sufficient cryptocurrency in his/her account: checking every transaction against spender's account ("public key") in the ledger to make sure that he/she has sufficient balance in his/her account.

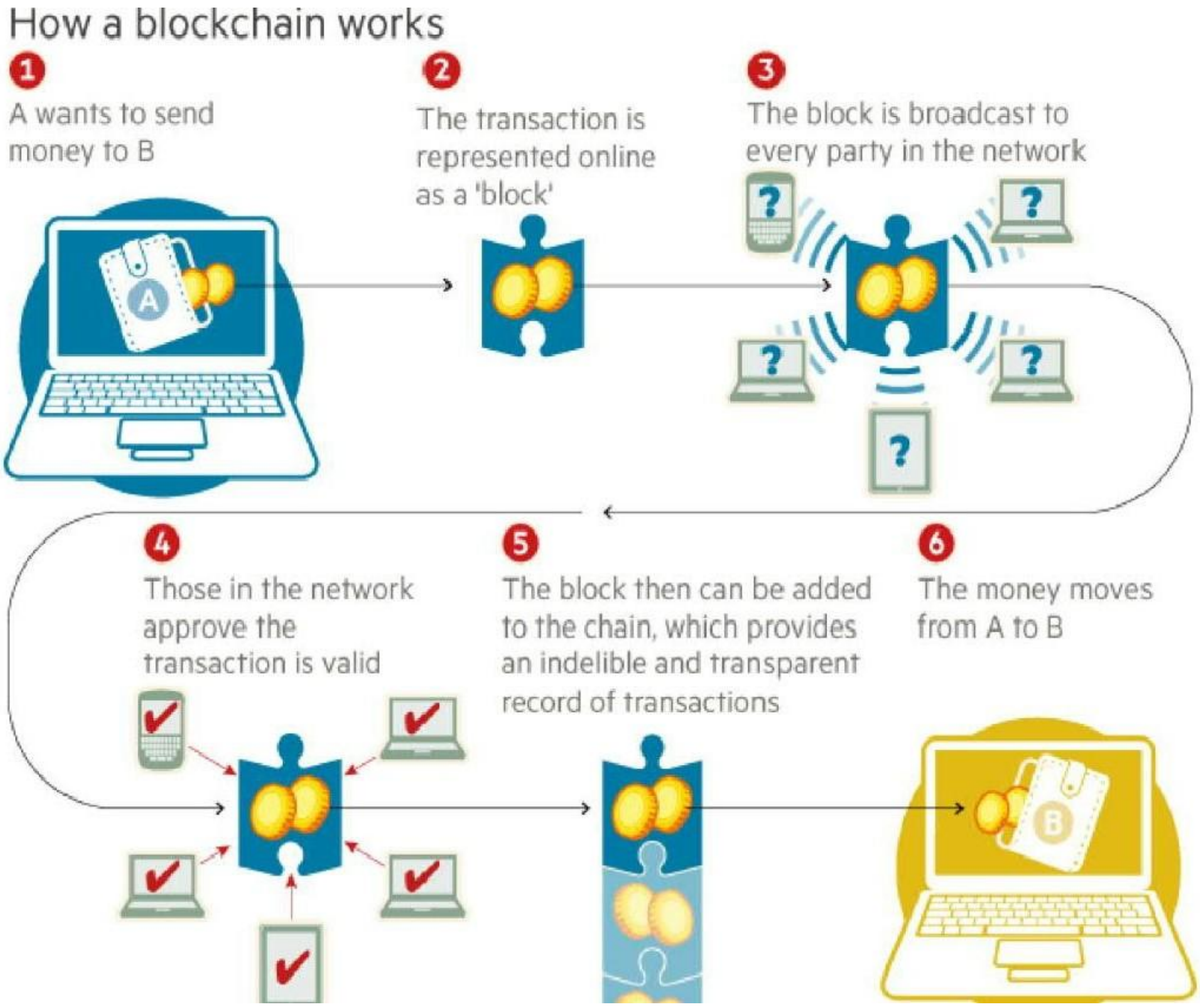
How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B

Figure 2. Financial Transactions using the Blockchaintechnology[2] .

However, there is question of maintaining the order of these transactions that are broadcast 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 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.

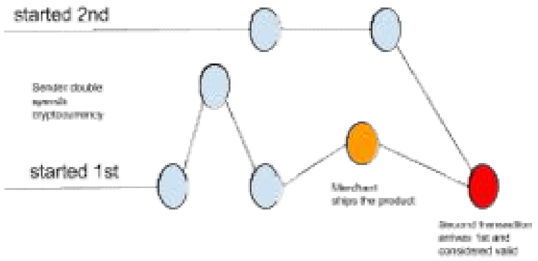
started 2nd
Sender double spends cryptocurrency
started 1st
Merchant ships the product
Second transaction arrives 1st and considered valid

Figure 3. Double spending due to propagation delays in peer-to-peer network.

This means that there is 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.

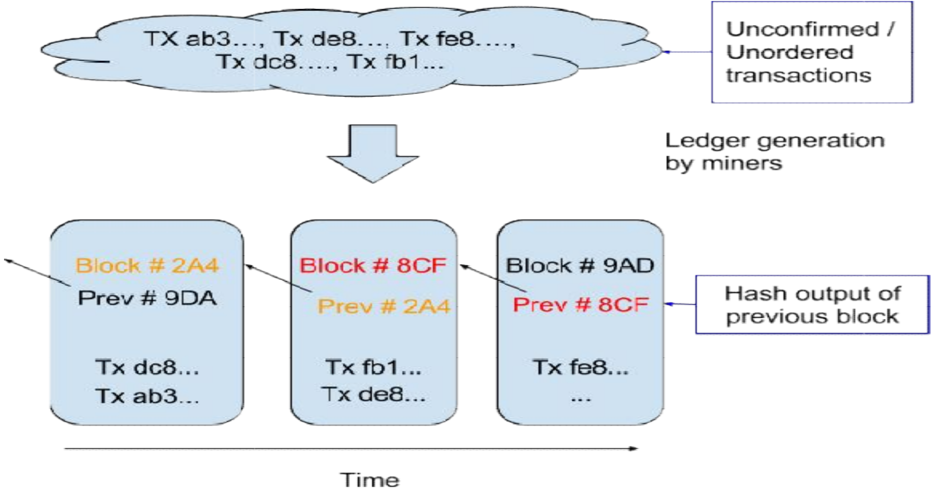

Figure 4.Generation of Blockchain from unordered transactions.

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 problem. Any node in the network can collect unconfirmed transactions and create a block and then broadcasts it to 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 blockchain provided it contains an answer to a very special mathematical problem. This is also known as “proof of work”—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 transactions and hash of previous block 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.

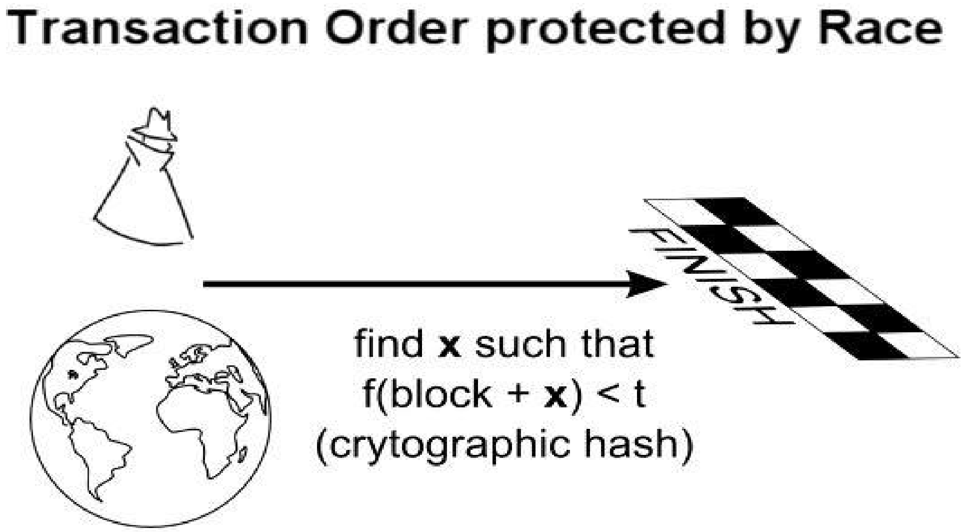

Figure 5 Mathematical race to protect transactions-I[3] .

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 First node, to solve the problem, broadcasts the block to 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 of solving is very complicated and hence the blockchain quickly stabilizes, meaning that every node is inagreement about the ordering of blocks a few back from the end of the chain. The nodes donating their computing resources to solve the puzzle and generate block are called "miner" nodes" and are financially awarded for their efforts.

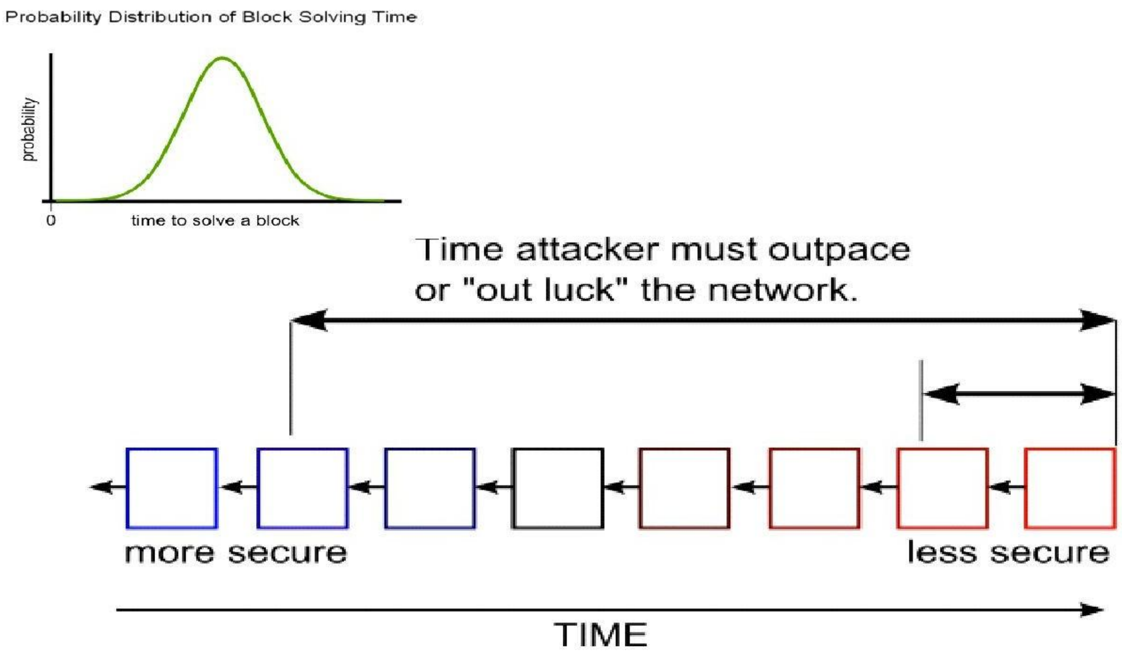
Probability Distribution of Block Solving Time
probability
0
time to solve a block
Time attacker must outpace
or "out luck" the network.
more secure
less secure
TIME

Figure 6. Mathematical race to protect transactions-II[4]

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 has to at the same time mathematically race against the good nodes to generate all subsequent blocks in order for it make other nodes accept its transaction & 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 two programs blockchain and smart contract 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 it has become much more easier to register, verify and execute Smart Contracts. Open source companies like Ethereumand Codiusare enabling Smart Contracts using blockchain technology. Many companies which operate on bitcoin and blockchain technologies are supporting Smart Contracts. Many cases where assets are transferred only on meeting certain conditions which require Lawyers to create a contract and Banks to provide Escrow service can be replaced by Smart Contracts.

Ethereum has created lot of excitement for its programmable platform capabilities. Ethereum allows anyone to create their own cryptocurrency and use that to execute, pay for smart contracts. Ethereum itself has its own cryptocurrency (ether) which is used to pay for the services. Ethereum is already powering wide range of early applications in areas such as Governance, autonomous banks, keyless access, crowdfunding, financial derivatives trading and settlement using smart contracts.

Also, there are a number of blockchains in existence to support wide range of applications--not just cryptocurrency. Currently there are three approaches in Industry to support other applications and also to overcome perceived limitations of Bitcoinblockchain:

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

Colored Coins is an open source protocol that describes class of methods for developers to create digital assets on top of Bitcoinblockchain by using its functionalities beyond digital currency.

Sidechainsare alternative blockchains which are backed by Bitcoins via 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--all of them taking advantage of scarcity and resilience guaranteed by the Bitcoinblockchain. The Bitcoinblockchain

Companies such as IBM, Samsung, Overstock, Amazon, UBS, Citi, Ebay, 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 (Sept. 15, 2015) joined forces with the New York based financial technology firm R3 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 JPMorgan, State Street, UBS, Royal Bank Of Scotland, Credit Suisse, BBVA and Commonwealth Bank of Australia have joined this initiative.

Next, we give a short description of what kind of interesting applications and projects 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.

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 contract and eliminate the need for a physical document. This eliminates the need for an intermediary, such as broker, exchange or bank.

Blockstreamis an open source project with focus on sidechains--interoperable blockchains--to avoid fragmentation, security and other issues related to alternative crypto-currencies. Uses can range from registering securities, such as stocks, bonds and derivatives, to securing bank balances and mortgages.

Coinsetteris 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 outcomes will occur. 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 which 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.

Everledgeris 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, create/read/update claims (by insurane companies) and create/read/update 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 and those who seek certification. By publishing proof of publication using cryptographic hashes of files into block chain takes the notary timestamping to new level. It also eliminates the need for expensive notarization fees and ineffective ways of transferring documents.

Stamperyis 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 the one of the companies which uses clearinghouse protocolfor notary service.
Block Notaryis an iOS app which helps you to create proof of existence of any content (photo, files, any media) using TestNet3 or Bitcoin network.
Crypto Public Notarywhich uses Blockchain of Bitcoin to notarize documents by using trivial amount of bitcoins to record the file's checksum in public blockchain.
Proof of Existenceis another service which uses blockchain to SHA256 digest of the document in bitcoinblockchain.
Ascribeis 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. It 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 convoluted one, but the rise of the Internet has made it even more complex giving rise to the demand of transparency in the royalty payments by artists and songwriters.

This is where the blockchain can play a role by maintaining a comprehensive, 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. The “smart contracts” would define relationships between different stakeholders (addresses) and automate their interactions (see Appendix for more details).

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 present 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. 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.

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/her document. It is to be noted here that cryptographic digest or fingerprint--not the actual document- is stored in blockchain, so user need not be worried about the privacy aspect.

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

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.

Storjprovides 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.

Here, bitcoin based micropayments serve as both an incentive and payment while a separate blockchain is used as a datastore for file metadata.

2.5. Decentralized IoT

The **IOT** is increasingly becoming popular technology in both the consumer and the enterprise space. A vast majority of IOT platforms are based on a centralized model in which as 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.

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-a decentralized Internet of Things (IOT). ADEPT uses three protocols-BitTorrent(file sharing), Ethereum (Smart Contracts) and TeleHash (Peer-To-Peer Messaging)-in the platform.

Filament(see Appendix for details)is a startup that provides a decentralized IoT software stack that uses the bitcoinblockchain 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 the modern commerce. It is one of the biggest challenge 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.

BlockVerify(see Appendix for details)providesblockchain based anti-counterfeit solutions that introduce transparency to supply chains. It is finding applications in pharmaceutical, luxury items, diamonds and electronics industries.

2.7. Internet Applications

Namecoinis an alternative blockchain technology (with small variations) that is used to implement 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 your Internet usage. Use of Blockchain technology means since DNS or phonebook of the Internet 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 have been widely deployed and incredibly successful, dependence on a CA makes scalability an issue.