BLOCKCHAIN – THE PATH TO DECENTRALIZED INTERNET

Anjana S Murthy
Assistant Professor
Dept of BCA
New Horizon College, Marathalli,
Bangalore, India.

Abstract: A blockchain is technically record of databases or a general book(ledger) of all transactions or digital events that have been done and shared among users. Every transaction in the general book is verified by node(consensus) of a majority of the users in the system. And, once entered, the data can never be removed. The blockchain contains a certain and checked records of every single event ever happened. Bitcoin is a decentralized P to P digital currency, which is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked perfectly and found wide range of applications in both financial and non-financial world. The main objective is that the blockchain establishes a system of creating a distributed node(consensus) in the online worldwhich allows participating users to know for certain that a digital event happened by creating an undeniable record in a public book. It opens the door for developing a decentralized system. There are massiveoccasion in this unruly technology and revolution in this space has just begun. In this paper describes blockchain technology and some compelling specific applications in both financial and non-financial sector.

Keywords: Blockchain, Consensus, Ledger, Bitcoin, Node.

I INTRODUCTION

A blockchain is nothing butrecords of database or public book (ledger) of all events that have been made and shared among users. Each event in the public book (ledger) is verified by node(consensus)of a majority of the users in the node. And, once entered, data can never be erased. The blockchainexists of a certain and checked record of every single event ever made. To use a basic expliniation, it is easy to steal a candy from a jar of candies, kept in a secluded place than stealing the candy from a jar of candies kept in a market place, being watched by hundreds of individuals.

Bitcoin is a popular model that is closelyrelated to blockchain. It is also the most arguable one since it helps to enable crores of rupees in global market of stealth transactions without any governmental disruption. Hence it has to go through a few regulatory issues involving national governments and banks. However, Blockchain itself is non-controversial and has worked perfectly over the years and is being successfully used in both financial and non-financialworld applications.

In 2014, Marc Andreessen, the doyen of Silicon Valley’s capitalists, listed the blockchain distributed nodes (consensus) models the most essential invention since the era of 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 users. Our all online transactions rely on trusting someone to speak out the truth—it can be an service provider claiming that our package has been delivered; it can be a authority telling us that a certain digital certificate is trustworthy; or it can be a social network telling us that our posts regarding our life events have been shared only with our friends or it can be a banks telling us that our money has been delivered reliably to our dear ones in a remote locations.

The fact is that we live our life dangerously in the digital world by relying on a third parties for the security and privacy of our digital properties. The fact remains that these third party sources can be compromised. This is where the blockchain comes handy. It has the potential to decentralize the digital world by enabling a distributed nodes (consensus) where each and every online transaction, past and present, involving digital assets can be verified at any time further. It does this without compromising the privacy of the digital property and users involved. The distributed nodes (consensus) and privacy are two important characteristics of blockchain.

The advantages of Blockchainis greater than the regulatory and technical challenges faced curently. One major up-coming use case of blockchaincontains “smart contracts”. Smart contracts are basically an algorithm that can automatically execute the contents of a contract. When a pre-defined condition in a smart contract amongst the usersentities is met then the users involved in a nodal agreement can be automatically made payments as per the terms in a transparent manner.

In this paper, 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.

How Blockchain works?

Let’s see the concept of the blockchain by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the blockchain is applicable to any digital asset transaction online.

1. Validate Entries
2. Safeguard Entries
3. Preserve Historic Record
YUP! HE SENT THE MONEY!
$10,000

E-commerce is specifically 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 save transactions. A certain amount of fraud is expected in online transactions and that needs mediation by financial transactions. This results in high transaction costs. While 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 crypto-currency 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 book. Verifying node needs to ensure two things before recording any transaction:

1. Spender owns the crypto-currency—digital signature verification on the transaction.

2. Spender has enough crypto-currency 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.

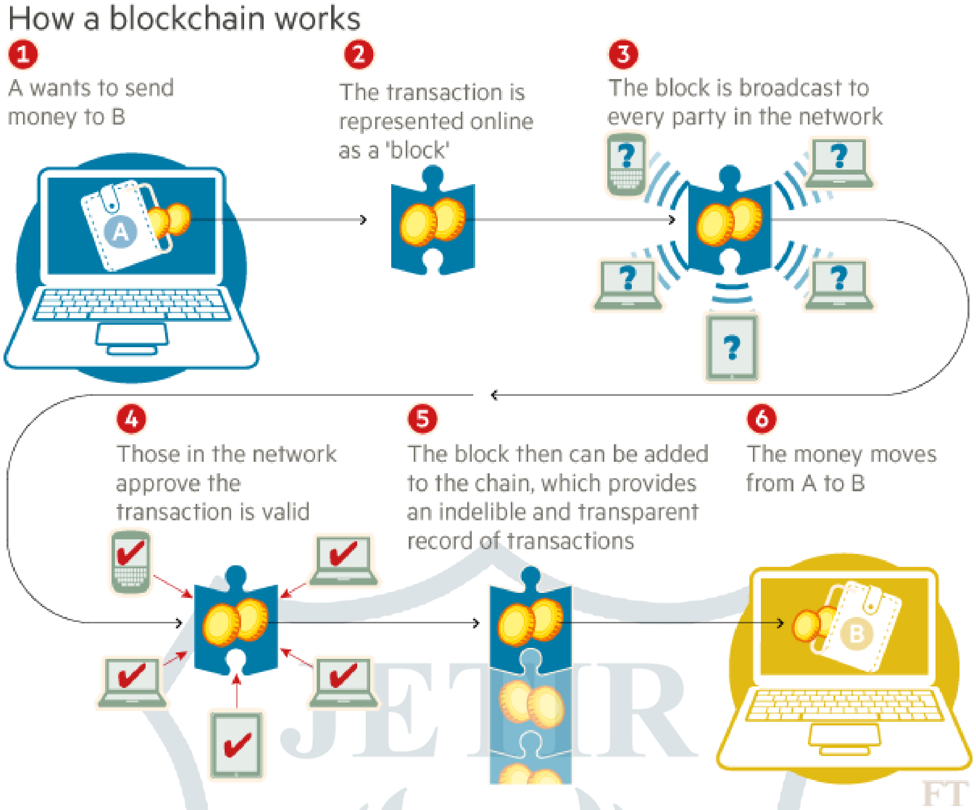
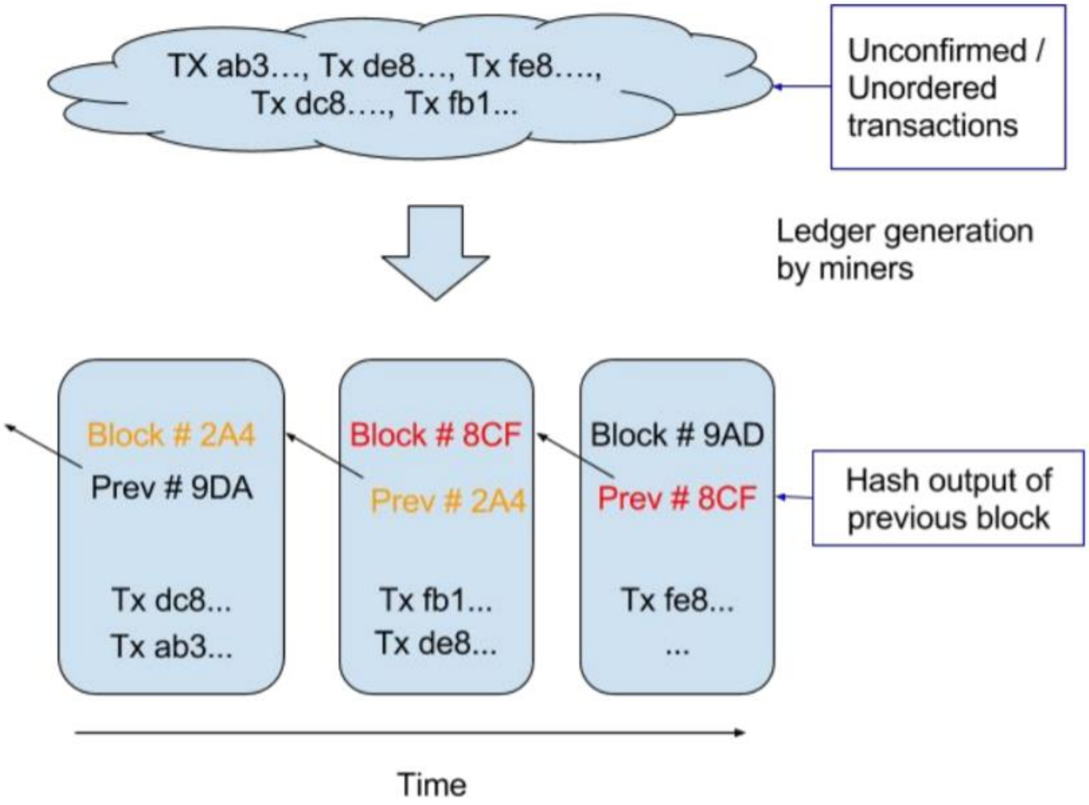

How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent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

Figure: How a blockchain works

However, there is question of maintaining the order of these transactions that are broadcast to every other node in the Bitcoin p-to-p 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 crypto-currency 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. 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.



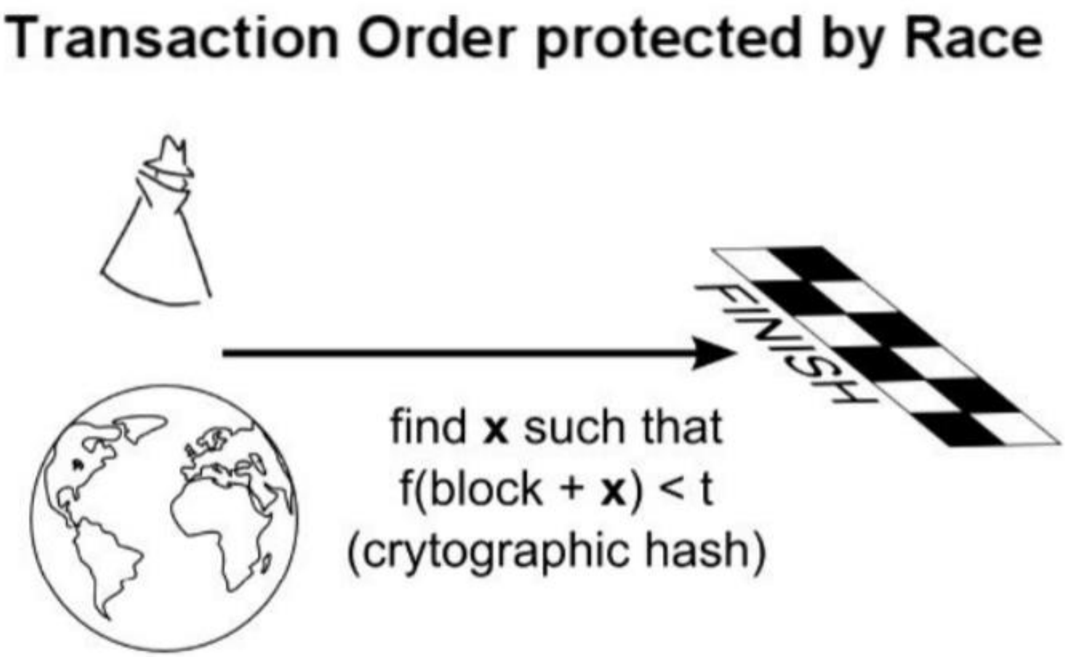
\

Figure: p to p network

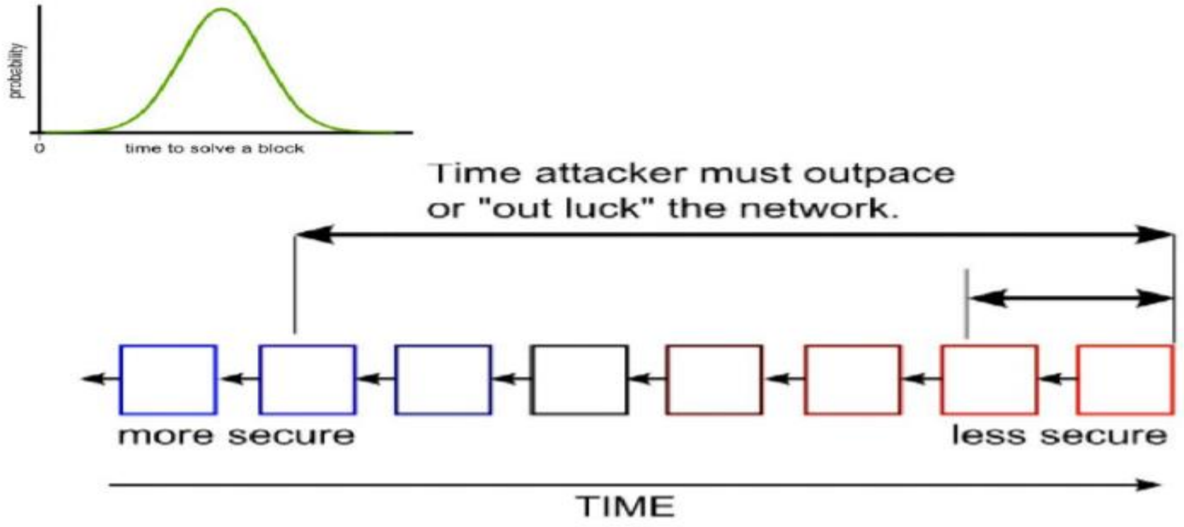
The Bitcoin solved this problem by a mechanism that is now popularly known as Blockchain. The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are considered to have happened at the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



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. 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 in agreement 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 effort



II APPLICATIONS OF TECHNOLOGY COMPELLING USE CASES IN BOTH FINANCIAL ANDNON-FINANCIAL SECTOR:

1. Financial Applications:

1.1. Private Securities It is very expensive to take acompany 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 . This is 6 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 Start-up called chain.com to 7 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.

Mediciis 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.

Blockstream is 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.

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 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.

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, create/read/update claims (by insurance companies) and create/read/update police reports on diamonds.

2. Nonfinancial 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

Stamper 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 the one of the companies which uses clearinghouse protocol for notary service. Block Notary is an iOS app which helps you to create proof of existence of any content (photo, files, and any media) using TestNet3 or Bitcoin network. Crypto Public Notary which uses Blockchain of Bitcoin to notarize documents by using trivial amount of bitcoins to record the file’s checksum in public blockchain. Proof of Existence is another service which uses blockchain to SHA256 digest of the document in bit coin block chain. Ascribe is another company which does authorship certification using blockchain. It also offers transfer of ownership service with attribution to the original author.

III CONCLUSION:

To conclude, Blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of Blockchain, makes it very attractive technology to solve the current Financial as well as non-financial business problems. As far as the technology is concerned, the crypto-currency based tech is either in the downward slope of inflated expectations or in trough of disillusionment. 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. The large financial institutions like Visa, MasterCard, Banks, NASDAQ, etc., are investing in exploring application of current business models on Blockchain. In fact, some of them are searching for the new business models in the world of Blockchain. Some would like to stay ahead of the curve in terms of transformed regulatory environments of Blockchain. To conclude, we envision Blockchain to go through slow adoption due to the risks associated. Most of the Startups will fail with few winners. We should be seeing significant adoption in a decade or two.

REFERENCE:

[1] https://www.blockchain.com/learning-portal/bitcoin-faq

[2] https://blockgeeks.com/guides/what-is-blockchain-technology/

[3] https://www.blockchain.com/explorer

[4] https://en.wikipedia.org/wiki/Blockchain

[5] https://www.investopedia.com/terms/b/blockchain.asp

[6] https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/

[7] https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/blockchain-explained.html

[8] https://www.finextra.com/blogposting/12378/how-i-explained-blockchain-to-my-grandmother

[9] https://www.cio.com/article/3055847/what-is-blockchain-and-how-does-it-work.html

[10] https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae

[11] https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners

[12] https://blockgeeks.com/guides/what-is-blockchain-technology/

[13] https://www.quora.com/How-does-Bitcoin-Blockchain-work-and-what-are-the-rules-behind-it

[14] https://lisk.io/academy/blockchain-basics/how-does-blockchain-work

[15] https://www.forbes.com/sites/kpmg/2018/09/11/blockchain-and-the-future-of-finance/#5261a807620f

[16] https://www2.deloitte.com/nl/nl/pages/financial-services/articles/blockchain-technology-use-cases-in-financial-services.html

[17] https://www.coindesk.com/information/how-blockchain-technology-change-finance

[18] https://hbr.org/2017/03/how-blockchain-is-changing-finance

[19] https://hackernoon.com/how-is-blockchain-revolutionizing-banking-and-financial-markets-9241df07c18b

[20] https://www.expresscomputer.in/interviews/the-non-financial-side-of-blockchain/18813/

[21] https://gomedici.com/30-non-financial-use-cases-of-blockchain-technology-infographic/

[22] https://www.newgenapps.com/blog/non-financial-use-cases-of-blockchain

[23] https://bravenewcoin.com/insights/ten-companies-using-the-blockchain-for-non-financial-innovation