Blockchain Technology

Ekta Malkan
Department Of Computer Science
UCLA
emalkan@cs.ucla.edu

ABSTRACT

Blockchain Technology developed by Satoshi Nakamoto was a breakthrough in the digital currency arena. It successfully solved the "Trusted Third Party" problem present in the traditional financial system, and the "Double Spending Problem" present in prior digital currencies. In this paper we have reviewed the history of digital currencies, current state of Bitcoin Blockchain Technology, the other areas of application apart from Cryptocurrencies, etc. This paper also highlights the current open problems including Scalability, Transaction Malleability, etc. and their solutions. This paper aims to understand the Blockchain Technology from a simple perspective, and understand the impact that this digital innovation can have in different industries.

KEYWORDS

Bitcoin, Blockchain, Trusted Third Party Problem, Double Spending Problem, Bitcoin Transaction, Fork, Blockchain Mining, Proof Of Work, Cryptography, Lightning Network.

1 INTRODUCTION

Bitcoin has been around since 2008 and has recently seen growly popularity. Some people understand it as a digital version of gold without any storage issues. Whereas, many believe that cryptocurrencies like bitcoin would replace the traditional currencies, removing the confusion over foreign exchange conversions, hefty transaction fees charged by Trusted Third Parties such as banks, etc. If Bitcoin is accepted as a medium of exchange, then the dream of open Global Markets could be achieved. In this paper, we have tried to review the evolution of digital cryptocurrencies, primarily focusing on the Bitcoin cryptocurrency. Taking this as a foundation, we then review the principles underlying Blockchain Technology, how transactions get processed in the Bitcoin Blockchain, applications of Blockchain outside cryptocurrencies.

Blockchain can be understood as distributed ledgers stored across many nodes, as opposed to a single centralized database or server. Those ledgers are secured by means of cryptography and transaction data is hard to tamper. The data stored can be transactions, identities or smart contracts. The Blockchain can be visualized as a long chain of blocks of transactions. New blocks are appended to the top of existing blocks. The blocks are made secure using cryptography techniques. Every new transaction and block is verified and confirmed by all nodes in the network. Any upgrade to the existing logic requires consensus by a majority of the nodes in the network.

This paper is structured as follows: Section 2 talks about the characteristics and features of the Bitcoin BlockChain and how Bitcoin solves the untackled problems of traditional or earlier digital currencies. Section 3 talks about Literature review of cryptocurrencies. Section 4 explains the internal Block Structure of blockchain. Section 5 elaborates on how blockchain works and payments are processed. Section 6 solves "Forking" that might happen in blockchain, Section 7 talks about the Double Spending problem, and how bitcoin blockchain solves it. Section 8 is about different Blockchain applications apart from cryptocurrencies. Sections 9 and 10 explain advantages and disadvantages of the bitcoin blockchain. Section 11 talks about open problems in current bitcoin cryptocurrency, and Section 12 explains the possible solutions being contemplated by the Blockchain community for those problems. Section 13 talks about Altcoins, which are other digital cryptocurrencies and how they provide enhanced features over Bitcoins. This is followed by Conclusion and Acknowledgement.

2 TECHNICAL DEFINITION

2.1 Characteristics and Features

The Blockchain is a historical record of ordered and timestamped transactions, shared amongst many computers rather than being stored on a central server. It usually stores financial transactions, however, is now being used for identity management, smart contracts, etc.

Blockchains are basically open and immutable Distributed Ledgers, meaning every node in the ecosystem has a copy of every transaction that has ever taken place. These nodes can verify new transactions. As every node is stranger to rest of the nodes, it successfully amortizes on the principle of "Trust No One".

Blockchains exist over a peer-to-peer network, every node receives information about new transactions and blocks and relay this information to its connections. The security and privacy of transactions and users is maintained using Digital Signatures and Cryptographic hashing techniques. Unlike traditional banking systems, a transaction once committed to the blockchain is hard to modify without anyone in the network noticing it.

2.2 Blockchain as a Solution

Traditional financial systems rely on the availability of a "**Trusted Third Party**" for transaction proof and security. Banks, Credit card companies, Governments and other financial institutions bank on those needs and charge huge amounts for payment processing, account creation, credit card annual fees, late payment fees, etc.

In the new era of digitization, the concept of Blockchain and digital currencies challenge the age-old necessity of Third Parties for ensuring "trust" during a transaction. The Blockchain concept relies on secure Cryptographic techniques for replacing trust otherwise ensured by a bank.

In the early days of digital currency before bitcoin, developers and researchers were trying to solve the "**Double Spending**" problem. Double spending refers to using the same cash spent once again and again.

Early Digital and Electronic cash was basically like any other file on your computer. It could be copied from one folder to another, you could email it to your friends creating as many new copies as desired. This nullified the concept of currency exchange as now any person will have had any amount of money to do any many transactions as he wishes. The person could spend 10$ to buy a burger, and then use the same 10$ to buy ice-cream. Satoshi Nakamoto solved this problem of double-spending by introducing the Bitcoin currency based on Blockchain Technology [1]. In the Blockchain world, once a transaction is confirmed, it is impossible to double spend it.

3 LITERATURE REVIEW

The earliest published research using cryptography as a basis for electronic funds is from 1982 by David Chaum, a Ph.D. graduate in Computer Science from the University of California at Berkeley. He introduced DigiCash [2] which in the 1990s came very close to the global level of success, however it later faced technological, political and social challenges. DigiCash was a brilliant system that provided anonymity to the users as well as security to the vendors. DigiCash was also famous for supporting "micropayments", along with other broad ranges of payment size options. Email was used as a primary means for currency trading in DigiCash.

In the 1990s, the Cypherpunks began to develop the idea of a digital cash whose value would be independent on the organization issuing it. Nick Szabo invented BitGold, which is a form of digital cash recognizable as being limited in supply, and therefore usable as money, by being provably difficult to create. This could be done by defining units of the digital cash in terms of proof-of-work. Other proposals for digital collectibles circulated on the cypherpunk mailing list, including b-money by Wei Dai. In 1993, Cynthia Dwork and Moni Naor introduced "proofs of work" concept [3]. Proof-of-work systems require some work to be done by the service requestor in terms of computing power or time i.e. expending resources. This concept is very important as it was later used in the bitcoin blockchain.

The idea of making proofs-of-work reusable for some practical purpose had already been established in 1999 by Marcus Jakobson. In 2002, the first proof-of-work based cryptocurrency was introduced (Rivest and Shamir) [4]. In 2007, Hal Finney introduced the idea of reusable proof of work (RPOW). Finney's purpose for RPOW was as token money. Just as a gold coin's value is thought to be underpinned by the value of the raw gold needed to make it, the value of an RPOW token is guaranteed by the value of the real-world resources required to 'mint' a POW token. In Finney's version of RPOW, the POW token is a piece of Hashcash.

In 2002, Sherman S.M. Chow introduced the use of the peer-to-peer network as a way of elimination of trusted third party problem for digital currency [6]. It was based on Byzantine Agreement, that aimed to develop algorithms for the distributed nature of the internet. These algorithms do not require any centralized control that have some guarantee of always working correctly.

In June 2005, Flavio D. Garcia and Jaap-Henk Hoepman introduced "Offline Karma: A Decentralized Currency for Peer-to-peer and Grid Applications". This paper introduced how the P2P systems can be made fair for all users, in which users get as much as they spend.

And finally, in 2008, Satoshi Nakamoto introduced "Bitcoin", the first ever digital currency to solve the double spending problem of digital tokens.

Now, we will understand the Blockchain technology in more detail, taking the Bitcoin Blockchain as a reference. The Bitcoin Blockchain is complex as it serves following purposes simultaneously-

a) Anyone should be able to create/mine transactions and write to the blockchain.

b) Anyone can verify an existing transaction, i.e. view any transaction.
c) Nobody should be able to alter already existing transactions in the blockchain.

4. BLOCK STRUCTURE

A block can be understood as a group of transactions mined at the same time and appended to the blockchain. Blocks are timestamped, and new blocks are linked to the earlier blocks forming a blockchain.

As shown in Figure 1, a Block comprises of:

- Prev_Hash: The hash value of the previous block. The purpose is to chain all blocks together forming the blockchain.
- Tx_root: The hash value of the root of a hash tree (Merkle tree) over all transactions in that block.
- Timestamp: The creation time of block, as seen by block creator. The timestamp is checked by other clients.
- Nonce: any arbitrary number used to make sure the resulting hash value of this block is below the target hash value. The Nonce is a 32-bit number and the 2^32 number space is exhausted during mining within less than a second.
- Blocks own hash- All the above values (except Tx_Root) are header items that get hashed into the block hash, which is then used by the next block as a reference to the current block.

5. HOW BLOCKCHAIN WORKS

For understanding how Blockchain works, let us take the example of Alice, who must pay 2.5 Bitcoins to Bob (a vendor) for burger and coke. To make this payment, Alice scans Bob's barcode in the "Bitcoin wallet" app in her mobile phone. Bob receives a message saying a payment of 2.5 Bitcoins has been initiated by Alice. This payment is not yet confirmed. After about 10 minutes, Bob receives a confirmation message that he has received the payment. Now let us understand what happens behind the scenes.

5.1 PAYMENT INITIATION

The Bitcoin wallet software on Alice's smartphone works as follows :

- It checks for Sufficient Balance- Before paying to Bob, Alice had received Bitcoins from Eve (2 BTC) and Ethan (1 BTC). She can only spend coins which she has. Alice attaches Transaction chain as inputs. This chain is a list of transactions that confirm she has enough unspent bitcoins to the transaction.
- It provides Recipient's (Bob's) address- This is basically Bob's Public key.
- It attaches Alice's own **Digital Signature**- This is created using a hash of Alice's private key and the transaction message.
- The wallet software now creates a transaction and broadcasts this transaction to all nodes in Alice's Network.

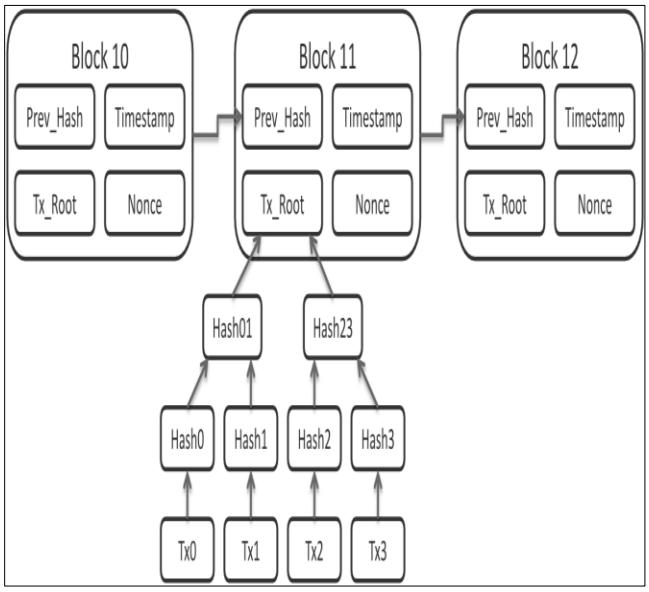

Figure 1: A Block in BlockChain

5.2 PAYMENT VERIFICATION

The nodes that are connected to Alice in the network :

- Verify whether Alice has enough unspent bitcoins to make this transaction.

This is done by checking for Alice's input transaction list. This list has 2 transactions (Ethan-> Alice and Eve-> Alice). The nodes will check for any other transaction where Alice has mentioned the same input. If they found such a transaction, the new transaction becomes void. Else, they proceed to the next step.

- Verify Alice's signature using her Public Key.

As Alice's public key is known, the nodes now verify whether the transaction has come from a valid sender i.e. Alice. This is done by using Alice's public key to verify her Digital signature. . If Alice was the true creator of this transaction, the Verify algorithm will return true else it will return false.

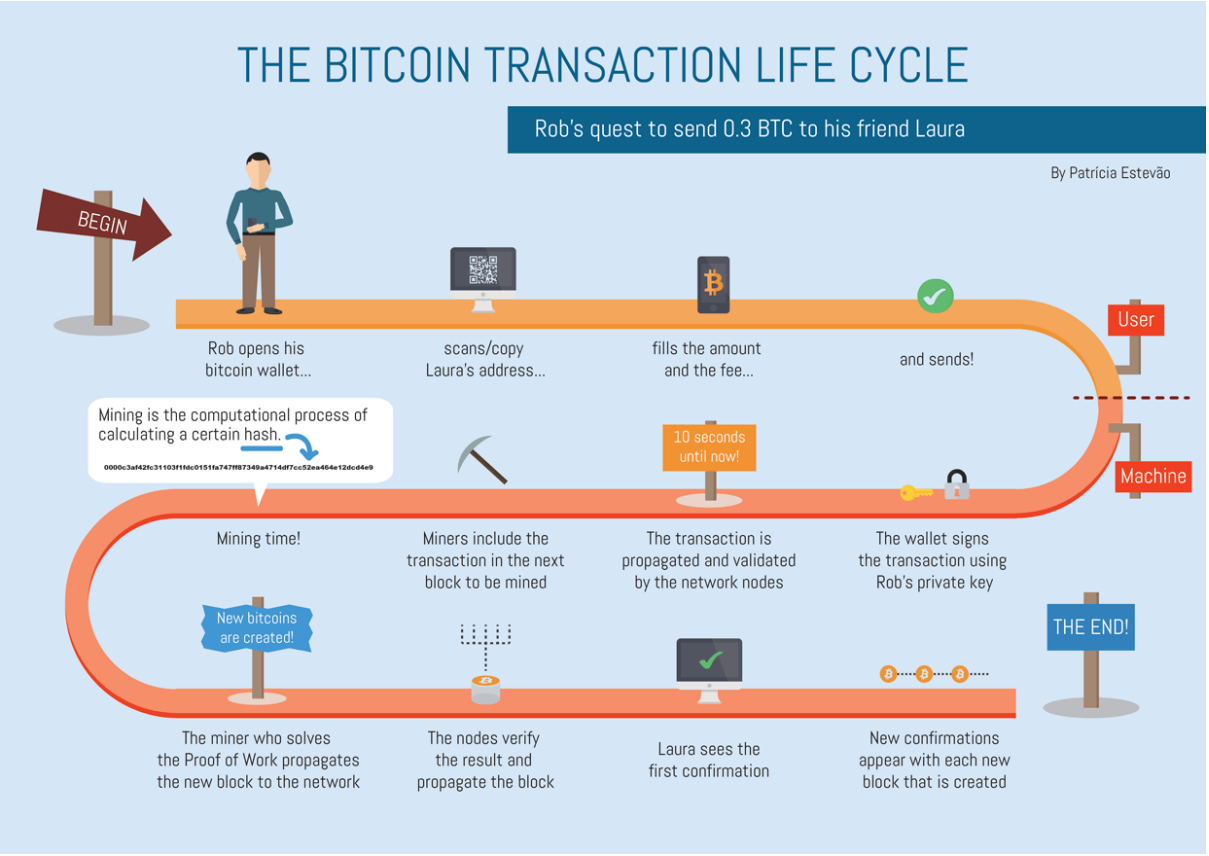

Figure 2: How a transaction takes place using Blockchain

Illustration By: http://janzac.com/wp-content/uploads/2017/12/Bitcoin-transaction-life-cycle.png

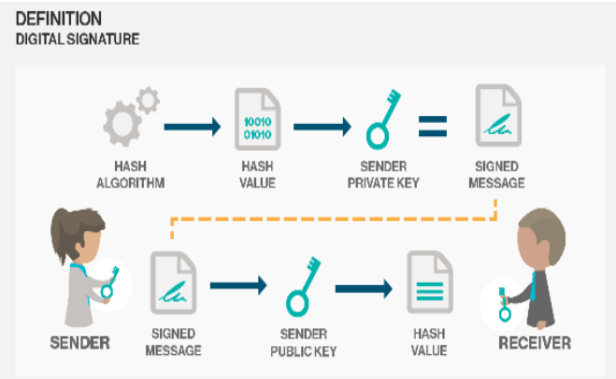

Figure 3 : Digital Signatures

- Store it in their local Pool of *Unconfirmed Transactions*
- Forward the transaction to all their connections.

If the above verifications were successful, the nodes will pass the transactions to their connections, who in turn will pass it on to their connections and so on till the entire network receives the transaction.

As Bitcoin is based on the principle of **"Trust No One"**, every node will verify the transaction using the above steps before passing it on. If an invalid transaction is received by any node, it will be dropped and not passed to its connections. Also, if a certain node plans to opt-out of passing on the valid transactions, the other nodes would still receive it as it is a P2P network and every node is connected to many other nodes. Unconfirmed transactions do not expire.

5.3 BLOCK MINING & TRANSACTION CONFIRMATION

Once a transaction is initiated, it stays in the pool of unconfirmed transactions on each node. These transactions are then confirmed with a process called "Mining". Any users in the network with access to the internet and sufficient computing power can participate in the process of Bitcoin Mining. These users are called "Miners". Miners compete on confirming the new transactions. They do it either for new bitcoin rewards or transaction fees in bitcoins or both. As the

difficulty of Mining keeps on increasing, Miners work together forming mining pools. Each miner in the pool gets the reward of new bitcoins, based on his committed time and computing resources.

Mining is a process by which transactions are grouped together and a block of transactions is created. Miners extract pending transactions from the unconfirmed pool and begin the process of Mining, i.e. creating blocks of transactions. For Block creation, some cryptographic properties need to be satisfied as follows:

Cryptographic one way hash function -
f (timestamp + nonce +previous block reference) => satisfy current difficulty criteria (say below a threshold value).

Merkle Trees are used for grouping and storing transactions in the leaf nodes. **SHA256** is used for mining. The hash of the root of the Merkle Tree is stored in the block, along with a timestamp when the block creation was initiated, a random nonce passed as a seed and the previous block reference on the top of which the current block would fit. Guessing the correct nonce that satisfies the current blockchain difficulty is called proof-of-work. For Nonce to help the block's hash satisfy the difficulty criteria (say less than 100), the Nonce needs to be guessed again and again. The block difficulty criteria is usually a low value, and hence the block's resultant hash must contain a certain number of leading zeroes. This work requires a lot of time and resources like computing power. This work that is performed by the miners is called "proof-of-work". Proof of work basically ensures that enough amount of computation power and time has been spent on solving a problem.

"Difficulty" of proof-of-work is a measure of how difficult it is to find the hash value below a given target. The difficulty changes every 2016 blocks. If the previous 2016 blocks took less than 2 weeks to be solved, the difficulty level is increased. If they took more than 2 weeks to solve, the difficulty level is decreased.

When a miner finds a set that has all the properties, a valid **block** is created. If the current value of the block does not satisfy the threshold criteria predefined by the Bitcoin community, another nonce is chosen and this process continues till a valid nonce is found that satisfies the threshold criteria. This concept of Proof of Work was introduced by Dwork and Naor in 1993.

Newly created Blocks are forwarded to all the Miner's connections, who validate the block and forward it to their own connections and so on until the entire network is aware.

Every node that receives the block –

1. Verifies the block.
2. Adds the Transactions in the Merkle Tree to their own ledger, removing them from their pool of unconfirmed transactions.
3. If they are mining new coins, they will now update their previous block reference to this newly created block and build on the top of that.

Thus, a transaction is successfully executed and confirmed. Bob can now spend the coins he receives from Alice (2.5 BTC). Alice needs to send any extra amount from the transaction input list to herself back. (3-2.5=0.5 BTC).

Once a transaction is initiated and included inside a block, it cannot be undone.

Now let us review a few points about bitcoins:

How are new bitcoins generated?
The block reward to the miners is the only way that new bitcoins are created on the network

How many transactions can a block contain?
Currently, there is a hardcoded limit of 1 MB. It was set to such a low value because all the blocks need to be propagated throughout the network. A larger block size would result in propagation delays. Each bitcoin transaction is around 250 bytes, hence a maximum of 4000 transactions can fit into a block (2000 in practice). There is a new block created every 10 minutes. Hence, 400 transactions per minute, i.e. 6.5 transactions per second.

What Happens If People Try To Send More Than 6.5 Transactions Per Second?
Every transaction cannot be included in the limited block space. Hence, some transactions will be ignored and stay in the pool of unconfirmed transactions. Transactions selected into the block are the ones that offer the highest transaction fee to the miners. Hence transactions compete with each other to secure a place in the block by offering high transaction fees.

Is there a limit to the number of Bitcoins that can be mined?
Total circulation of Bitcoins will be 21,000,000 coins.
It'll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years.
first 4 years: 10,500,000 coins
next 4 years: 5,250,000 coins
next 4 years: 2,625,000 coins
next 4 years: 1,312,500 coins etc...
When that runs out, the system can support transaction fees if needed. It's based on open market competition, and there will probably always be nodes willing to process transactions for free.
-Satoshi Nakamoto

So far, we have seen the Happy Flow of BitCoin Transaction execution. But there are certain challenges that

occur in exceptional scenarios. What if two or more miners mined a block at the same time. They would forward it to their own connections. Hence different nodes in the network will have different copies of the blockchain. This is called "Fork" in the Blockchain and can be explained as follows:

6. FORK

If two or more blocks were created by different miners at the same time and broadcasted, different nodes will have different ledger copies. A Fork is created. In this scenario, each miner node can simply build on the top of the block they first received. Other nodes will build on the top of the block first received by them. When a new block is mined, the length of that branch in the fork increases. A general rule of thumb is "Accept the longest chain of blocks". Hence the miner creating the next block would use the last block of the longest chain as previous block reference. The other branches that were forked will get nullified, and their transactions will go back to the pool of unconfirmed transactions.

The difficulty of block acceptance (nonce guessing) makes is impossible for blocks to be mined at the same time. And mining for two or more blocks at the same time in different branches is even lesser probable. Hence, a few blocks from the last block, everyone agrees of the blockchain ordering. The last few blocks known to a node might get forked out. Hence, a payment acceptor must always wait for a few blocks before considering a payment as final.

7. DOUBLE SPENDING PROBLEM

As mentioned earlier, there is some doubt regarding confirmed blocks at the end of the chain. Such confusion creates opportunities for malicious users to deliberately create a fork in the blockchain.

Let us consider a scenario in which Alice has bought a dress online from Bob and has chosen Bitcoins as the mode of payment. Now Alice sends a payment to Bob. In about 10 minutes, Bob receives a confirmation on the payment and he ships the product. Now if Alice was a malicious miner who could mine 2 or more blocks at a time, she can replace the block with Bob's transaction with a chain of blocks, and in one of those blocks, she sends the same bitcoins to her own self. In this scenario, Bob's transaction goes back to the pool of unconfirmed transactions, and it would eventually be dropped by the nodes in the network as a duplicate transaction, i.e. as it uses the same spent inputs. Thus, Bob is out of the shipped product as well as the money. This problem is called "**Double Spending**" Problem.

Hence, in case of the double spending problem, a few users can be cheated as malicious users spend the same bitcoins (or in general digital tokens) twice. Satoshi Nakamoto solved the "**Double Spending**" Problem of Digital currency. The figure below explains how a proof-of-work concept in bitcoins makes it difficult for a double-spending attack to take place.

As shown in Figure 5, if Alice tries to replace an earlier block (say block 74 in the figure), she will have to recalculate all the blocks starting from block 74 up to the latest block. For this, she is in competition with thousands of other miners who would be mining just the one last block, i.e. block 91. Even if Alice has a supercomputer, or many such supercomputers, finding a perfect nonce whose hash of the block data would satisfy the mining criteria before the rest of the network is impossible.

Alice would need the computing power of more than 50% of the network to have at least a 50% chance to come up with more number of blocks before anyone else in the network solves a single block. This is practically impossible.
Thus, the requirement of solving a mathematically difficult problem enables security for the blockchain. This has been illustrated in Figure 4.

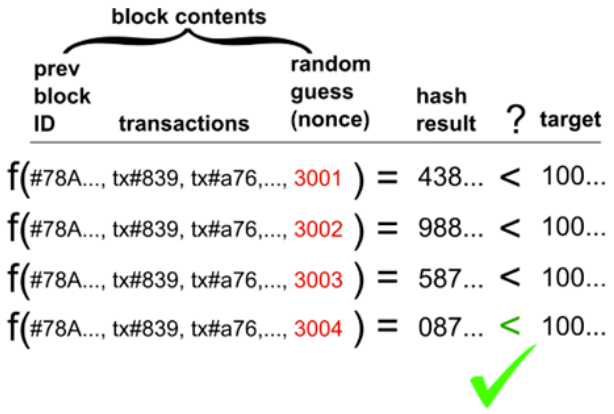

Figure 4: Difficulty of Solving the Math Problem
Source: https://1.bp.blogspot.com/-Ikw7OKhTjJU/VAt5oyzVvgI/AAAAAAAAFyE/PR2f6eMwb7Q/s1600/bitcoin_solving_block.png

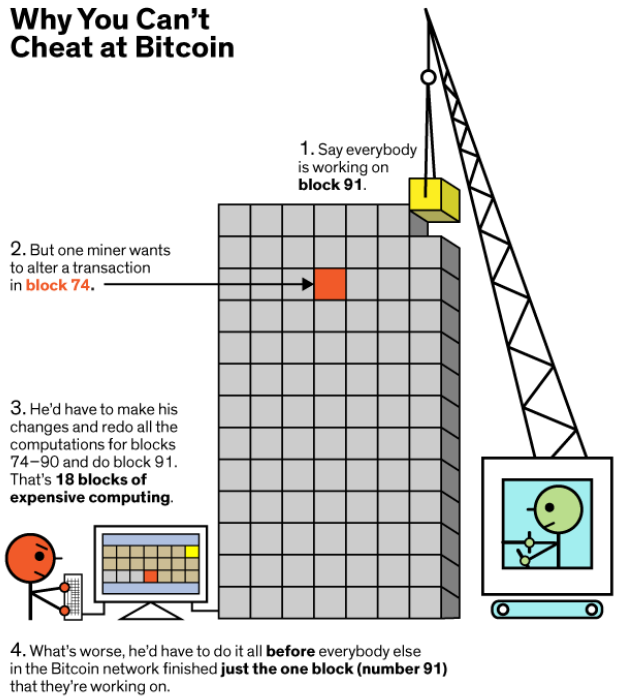

Figure 5: Double Spending Attacks
Illustration: Mark Montgomery/IEEE Spectrum

8. BLOCKCHAIN APPLICATIONS

Although this report uses the BitCoin BlockChain as a reference, the applications of blockchain are immensely growing. More and More companies, banks, governments, lawyers are accepting BlockChain to implement their technology solutions like identity management, record keeping, voting, smart contracts, etc.
Below are some of the companies/domains working towards BlockChain Development:

a) **Storj – It is using Blockchain for cloud storage.**
b) **Chronicled – uses blockchain for version controlling in Contracts and Legal Documents**
c) **Charity- Used to help Syrian Refugees**
d) **BitCongress- Trying to implement an electronic-voting system based on BlockChain.**
e) **MedRec- Blockchain for healthcare**
f) **Digital Identity Management – No need for password-based systems or hackable databases.**
g) **Digital assets- Stocks, Bonds, land titles, frequent flyer miles, etc.**

The industries which would are using BlockChain can be seen as below :

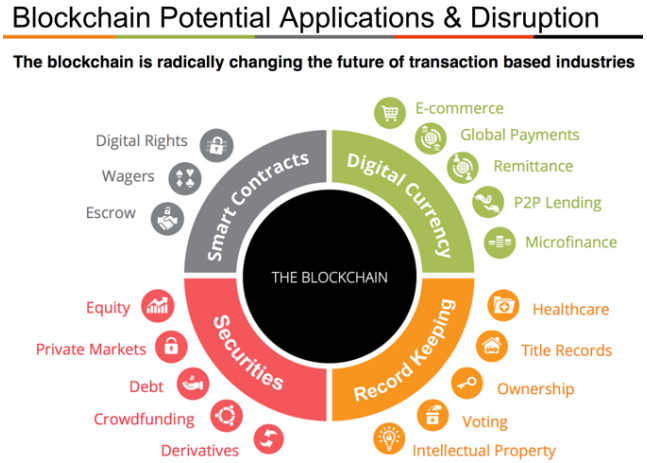

Figure 6: BlockChain Applications
Image Source: https://x9.org/wp-content/uploads/2016/02/Blockchain_FSS.pptx

9. ADVANTAGES

"BlockChain will do to the Financial World, as the internet did to the media" is a popular quote. Below are the advantages of BlockChain technology, especially the Bitcoin Blockchain:

a) TRANSPARENCY

Everyone in the network is aware of all the transactions that have ever taken place. This is completely opposite to the traditional banking systems in which only the involved parties and the bank is aware if the transaction.

b) NO DOWNTIME, 24*7 ACTIVE (vs Banks With Holidays And Time Zone Gaps)

Traditional financial institutions have working hours and are not available during holidays and weekend. Also, sometimes their websites are down for maintenance work. The Blockchain community is globalized and hence is always up. There is no down-time in Blockchain.

c) DECENTRALIZATION

Blockchain provide decentralization, as the transactions are stored in the form of a distributed ledger over a P2P network. There is no centralized server or database where all the data is stored.

d) USER CONTROLLED NETWORK (80 % Consensus for upgrade)

Any changes to the core logic of the bitcoin software must have at least 80% consensus of the network. This includes consensus from users, miners, developers, bitcoin software companies etc. If the new changes made are backward compatible, even users who do not upgrade to the new software can use the system. This is called as "**Soft Fork**". However, if the new software renders the use of previous software not feasible, everyone is forced to upgrade to the new software. This change is called "**Hard Fork**".

e) PERMISSIONLESS (vs SWIFT which is permissioned viewing only)

Traditional financial transactions are stored as SWIFT messages. Only banks and financial institutions are permissioned to view the SWIFT messages, which may then be relayed to the participating users. However, in case of blockchain, every node has access to all the transactions and no permission is required.

10. DISADVANTAGES

a) Too much computing power all over the world is consumed in blockchain mining.

Bitcoin Mining consumes about 23 TeraWatt power per hour. This is equivalent to provide power to the entire country of Equador for one year.

b) Scalability issue- only 6.5 transactions per second.

The Bitcoin Blockchain currently supports only 6.5 transactions per second. This is far less as compared to millions of transaction processed per second by Visa, PayPal, banks etc.

c) Can be used for illegal activities, as only public keys of the users are known.

All the information that one has from a transaction are the public keys of the sender and the receiver. This means that terrorists and criminals find abode in bitcoin for money laundering activities, as well as using bitcoins as means of payment for buying arms and bombs etc.

d) Loss of private key of a user results in loss of bitcoins associated with the corresponding public key.

About 4 million bitcoins have been lost forever, out of the 21 million bitcoins that can ever be mined. This is because bitcoins are associated to an account holders private key. Loss of private key of a user results in loss of bitcoins associated with the corresponding public key. Private keys can be lost due to insufficient backups and hard drive crashes.

e) Increased Mining fees (about 14$) make small transactions impossible.

As there is a limit to the number of Bitcoins that can ever be mined, the only incentive for miners to mine the blocks in the future would be transaction fees. Currently the transaction fees are about 14$. In the future this amount might increase. However as more and more users begin entering the mining business, due to market competition the fees would reach economic equilibrium.

f) Confidentiality vs Transparency. How to adapt for business needs?

Blockchains have many potential applications apart from cryptocurrencies. Many banks, governments and financial institutions have begun to realize the power of blockchain and are coming up with applications using blockchains internally. As these business demands confidentiality, and blockchain lies on the inherent principle of transparency, private blockchains internal to the company need to be built. These private blockchains can be customized to use the privacy and security features of the public blockchain but restrict the participants and the users based on the business needs.

11. OPEN PROBLEMS AND SOLUTIONS

A. SCALABILITY

At any given point in time, there are so many transactions that can be put in a block. Initially, when BitCoin was created, there was no limit to the size of the block. However, the creator Satoshi Nakamoto later realized that hackers and malicious parties can create a lot of spam transactions, input them into large blocks, and clog the system. This would result into Denial of Service Attacks. Hence, he added a 1 MB block limit to the size of the blocks.

One of the most prominent problems in the Bitcoin Blockchain is of Scalability. Currently Blockchain supports only 6.5 Transactions per second. As this is very low as compared to the real time demand, following solutions have been proposed by the blockchain community.

As we can observe from the graph data in Figure 7, more and more transactions are being carried out. Due to the

limited block size, users have to wait for a long time before their transactions get accepted into a block. In order to get their transactions processed early, users end up paying a lot of mining fees. This is the Scalability problem in Bitcoin blockchain that the entire community is actively trying to solve.

Figure 8 is the graph of average waiting time for users who pay minimum transaction fees. If you pay low transaction fees, you need to wait for an average of 13 minutes for your transaction to be accepted.

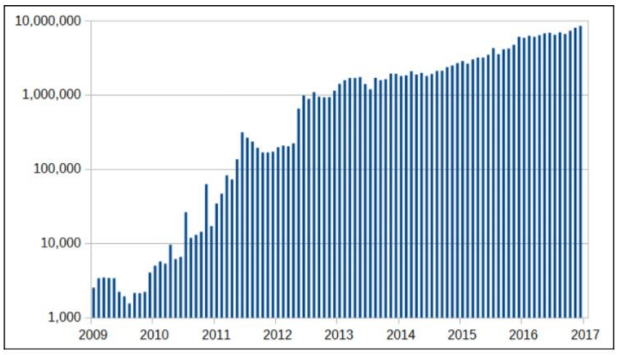

Figure 7: The Graph of Number of Bitcoin transactions per month per year
Source: https://blockgeeks.com/guides/what-is-segwit/

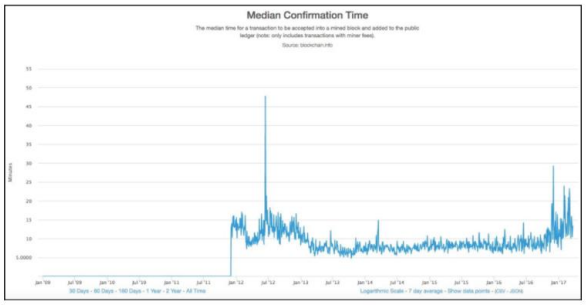

Image courtesy: Business Insider.

Figure 8: Average waiting time for users paying minimum mining fees

B. TRANSACTION MALLEABILITY

The signature data in the transaction may be tampered even before the transaction enters the block. This would result in rejected transactions or the sender being cheated.

For example, Alice sends Bob 2.5 Bitcoins. If Bob uses transaction malleability to alter the transaction data, he can change Alice's signature and the transaction ID. If Bob attaches higher mining fees than what Alice attached, there is a chance that Bob's new transaction would get accepted before Alice's transaction. Alice transaction would be overwritten using same transaction inputs and would be dropped. Bobs' transaction had same inputs and so he would receive 2.5 bitcoins. Yet, Bob can prove to Alice that he never received the earlier bitcoins and Alice would see that her transaction didn't execute and would resend the amount with different inputs. Finally, both the transactions would get accepted and Alice would lose 5$ instead of 2.5$.

Thus, the digital signatures being used inside bitcoins can result into both Scalability as well as Malleability issues.

12. SOLUTIONS

Following solutions have been proposed for these problems. Some of those solutions have already been implemented, while others are still under debate.

12.1 Increase block size (e.g. 1MB to 2 MB or 8MB)

One of the simplest and the most intuitive solutions to having more transactions per second is to increase the block size. Currently, the blocks in the bitcoin blockchain are of 1 MB size. If we increase this size to 2 MB or 8 MB, far more number of transactions can fit the block. However, this would result in a hard fork in the blockchain. Each and every participant needs to upgrade their system to the new block size, as the change will not be backward compatible.
Currently, a lot of debate is still going on in the blockchain community to incorporate this new limit, and what the actual limit should be.

12.2 SegWit : Segregated Witness

One of the significant reasons of huge transaction size in the blockchain is "Transaction Input" Factor present as a part of the signature. The signature consumes about 65% of the space inside a transaction.

As a solution to saving this space inside the transactions, the concept of sidechains was introduced. **Sidechain** is a parallel chain which runs along the blockchain. This sidechain can include signature data of all the transactions, separating it from the main blockchain, thereby saving space from the blocks in the blockchain.

12.3 Schnorr Signatures

When money needs to be sent from multiple address to a single address, the key size becomes huge, as each of these transactions will have their own signature. If it is just one person sending money via different sources like BitWallet, Coinbase etc., there needs to be just one signature and not

multiple signatures. Having multiple signatures consumes up a lot of space in the block which could have been utilized by other resources.

By using Schnorr Signatures, we can have one single signature for multiple transactions from the same person. Thus about 25% storage and bandwidth space would be available.

Schnorr signatures also help increase privacy. Sometimes, we want multiple people authorize a transaction. This is called MultiSig. Using Schnorr Signatures, these transactions also get displayed using a single signature, and hence the outsiders do not know that a MultiSig transaction just took place, thereby increasing privacy.

Sometimes, users spam the network with lots of transactions, essentially sending money from multiple accounts to a single account and vice versa. This increases the pile of unconfirmed transactions and results in denial of service attacks. Schnorr signatures can help to solve this issue as well. If only one signature is required even for multiple transaction from the same party, a lot of block space would be saved. Hence, now the spammer needs to create far more transactions and pay more fees to spam the network creating a DOS attack. Thus, Schnorr signatures provide a certain level of protection against spam attacks, by making those attacks expensive for the attacker.

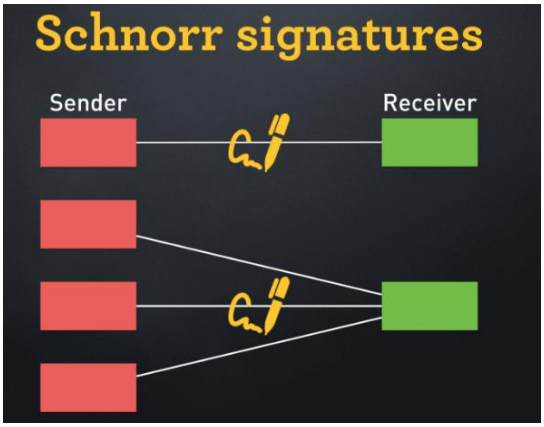

Figure 9: Schnorr Signatures

12.4 Lightning Network

Lightning Network guarantees faster transactions, almost for free. It adds a second layer of payment protocol over the blockchain. Lightning Network specification relies on SegWit that we studied above. The flow of lightning network is as follows:

Suppose Alice and Bob very frequently transact with each other. Hence, they would like their transactions to be instantaneous over the bitcoin. As blockchain has scalability issues, they use Lightning Network solution as follows:

1. Each of them donates an initial amount as fees for opening a separate channel between them. This transaction is broadcasted to the blockchain network and is accepted into the block.

2. For a designated period, depending on the amount committed, this channel would stay open.

3. Alice and Bob can do as many transactions over the channel as they desire in this time period.

4. At the end of the time period, each of them broadcasts the final net amount owed to the bitcoin blockchain. Thus, only the netted amount is known to the blockchain and not the entire history of to and fro transactions.

5. During the time the channel is active, if either of the parties feel that they have been cheated and have not been paid their dues, they simply broadcast the history of all the transactions to the blockchain. The transaction input security now forces the offender to pay back any funds that he/she might have withheld from the other.

13. ALTCOINS

About 1270 cryptocurrencies exist in the world today. Every currency provides some unique feature or solves some problem which is not yet solved in the bitcoin blockchain. Some claim to provide faster transaction settlements than blockchain, others claim more security and faster mining time. The most prevalent cryptocurrencies amongst these are Litecoin, Etheruem, ZCash, Dash, Ripple, etc.
The special characteristics of these “altcoins” have been summarized in Figure 10.

CONCLUSION

Thus, we have we successfully reviewed the principles underlying Blockchain Technology, how transactions get processed in the Bitcoin Blockchain, applications of Blockchain apart from digital currencies. We have also discussed open problems and solutions.

ACKNOWLEDGMENTS

I would like to thank Dr. Miodrag Potkonjak for providing me with this opportunity to research in Blockchain technology and cryptocurrencies. He has constantly encouraged me to improve upon my understanding and kept raising the bar to be achieved.

	LITECOIN	ETHEREUM	ZCASH	DASH (DARKCOIN)	RIPPLE (XRP)
Year	2011	2015	2016	2014	2012
Features	Faster block generation rate	Smart Contracts	Extra Privacy and Selective Transparency	Secretive Bitcoin	Real-time global payment network
	Faster transaction confirmation (2.5 vs 10)	Decentralized Applications	All transactions are recorded and published on blockchain	More Anonymity than Bitcoin	Offers instant, certain and low-cost international payments.
	Uses "scrypt" as proof of work	Ether	Sender, recipient and Amount remain private.	Makes transactions untraceable	Does not need "Mining"
	Scrypt can be decoded with Consumer Grade CPUS		Uses "Zero-knowledge Proofs"		Less Computing power, Less Network latency

Figure 10: Characteristcs of different Cryptocurrencies (Altcoins)

REFERENCES

[1] Satoshi Nakamoto (2009), Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[2] Chaum D.(1982), Blind signatures for untraceable payments

[3] Dwork Cynthia and Naor Moni, (1993). "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology".

[4] Ron Rivest and Adi Shamir, (1996) - "PayWord and MicroMint -- Two Simple Micropayment Schemes", CryptoBytes, volume 2, number 1

[5] L. Kehoe, D. Daltion, C. Lonowicz, T. Jankovich (2015), Blockchain Disrupting the Financial Services Industry?

[6] Sherman S.M. Chow (2007), "Running on Karma -P2P Reputation and Currency Systems"

[7] F. Reid, M. Harrigan (2013), An analysis of anonymity in the bitcoin system, Security and Privacy in Social Networks 197-223.

[8] Y. Zhang, J. Wen (2015), The IoT electric business model: Using blockchain technology for the internet of things, Peer-to-Peer Networking and Applications.

BOOKS and Other Resources

[1] Don and Alex Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World"

[2] Tim Lea, "Down the Rabbit Hole: Discover the Power of the Blockchain"

[3] Melanie Swan, "Blockchain: Blueprint for a New Economy"

[4] Roger Wattenhofer, "The Science of the Blockchain"

[5] Blockchain University (online course on blockchain development)

[6] Miles Price, "The Complete Guide to Understanding Blockchain"

[7] William Mougayar, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology Hardcover"

[8] Phil Champagne, "The Book of Satoshi"