UNDERSTANDING THE ROLE OF NETWORKS IN BLOCKCHAIN TECHNOLOGY AND WIDE APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Sujanth Babu Guntupalli
Department of Computer Science
University of North Carolina at Charlotte
sguntup1@uncc.edu | 800987789

Abstract---The term ‘blockchain’ is quite popular and the Blockchain technology is in huge demand nowadays thanks to the Bitcoin and other cryptocurrencies. But blockchain is neither the same as Bitcoin nor is limited to cryptocurrency. Blockchain technology is proving to be a game changer in the fields of the Internet of Things, cloud computing, software-defined networking, FinTech solutions, smart contracts and can also be used in music distribution, online voting and much more. This technology is giving the network engineers new challenges.

The key features of blockchain are its peer-to-peer distributed networking, high safety to the level of impossible to hack. It is a distributed ledger containing blocks of valid transactions across a distributed network of computers. All these computers are peers sharing the available resources without a master node or centralized administration. We can say it is a database but it’s not the same as a traditional database. Blockchain provides an efficient and less costly means to secure the integrity of a large number of transactions. The blocks in blockchain ledger cannot be altered or changed without the general agreement of other peers and altering the subsequent blocks in the ledger.

In networked systems, cryptography has a crucial role. Even Blockchain technology uses cryptography. To be precise blockchain uses public key cryptography. Cryptography is used to secure the identities of users who are using it. Also, it prevents the alteration of blocks or the transactions in the blocks. Cryptographic hashes are used to link a new block to the previous block and help to secure the integrity of the blocks. The structure used inside the blocks to store transactions is Merkle Tree.

Another important feature of blockchain is data replication. A copy of data is stored on every node in the blockchain distributed system. Adding of a new block is broadcasted to other nodes on the network and data is replicated to those nodes. This prevents loss of data and makes it fault-tolerant.

1 Introduction

A 2008 paper by a person or group of persons called “Satoshi Nakamoto” first described the term blockchain [1]. It also described the term bitcoin and for some time both blockchain and bitcoin were used as synonyms. But later Blockchain technology was discovered to have many applications other than bitcoin and many blockchains were created for different applications.

Blockchains are linked lists that contain data and a hash pointer to the previous block, thus forming a chain of connected blocks. Blockchain is also a public ledger which everyone can see and is shared among all its users. To modify any transaction in the blockchain, the ledger would have to be changed among the most users. But it’s impossible as it is being used by so many users already and is a very difficult task to change in all the nodes. With more people joining in it, blockchain becomes even more secure to modify the transactions. Also, if any new transaction must be added to the transaction record, it must be confirmed by the majority of blockchain users for the transaction to be considered as valid. Blockchain is not a bank or government and there’s no central authority setting regulations on it. So, if blockchain is used for financial transactions we can cut out the middlemen who collect fee on the transactions done through them. All these amazing features makes Blockchain technology the next big thing.

1.1 Block

A block is a data structure containing a header and a long list of transactions (see in **Fig. 1** [2]). The transactions in a block are contained in a structure called a Merkle tree or binary hash tree. Every block in the blockchain has the cryptographic hash of the block before it. Block hash acts as the identifier of the block.

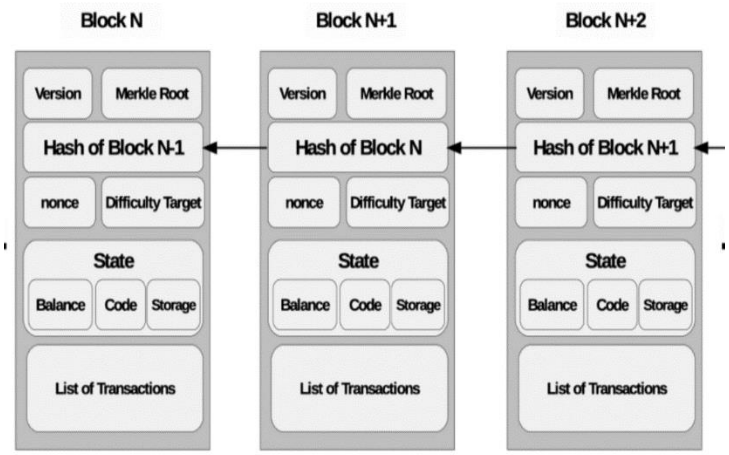

Fig. 1. Blocks with header and body structure

1.1.1 Block Header

A block header contains metadata about a block. It contains **version**, **previous block hash, timestamp, difficulty target, Merkle tree root and nonce**.

Version is the version number of the current block. It indicates which set of block validation rules to follow.

The UNIX time timestamp is the number of seconds that have elapsed since the first of January 1970.

Difficulty target is the computational problem that needs to be solved to produce a valid signature or hash output so that the block becomes eligible to be added into the blockchain. The difficulty target specifies the number of leading zeros should be there in the digital signature of a block and is used to maintain block time. Block time is average time taken by a blockchain network to add one block of transactions to the blockchain. Block time is approximately 10 minutes for Bitcoin, and 17.5 seconds for Ethereum. Difficulty target is adjusted according to computation power of miners. It is increased with increase in computation power [2].

Merkle root is the hash value in the root of the Merkle tree of the block's transactions.

The nonce is the value that is changed by the miners to produce different permutations to achieve the difficulty level required for the block to be made eligible to fit into blockchain.

1.1.2 Cryptographic Hash Function

Cryptographic hash function is a function which takes input data of any size and outputs a fixed size alphanumeric string (See in **Fig.2**[1]). The resulting output is called hash, hash code, hash value or digest. The hash is unique to the given input. It is difficult to reconstruct an input by knowing a hash value. They are used to verify integrity of transmitted data. The ability to store and identify data of any size with a fixed length output can help in vast storage savings and to increase efficiency. Also, the length of output depends on the hashing function used. SHA and MD are two of the most commonly used cryptographic hash functions.

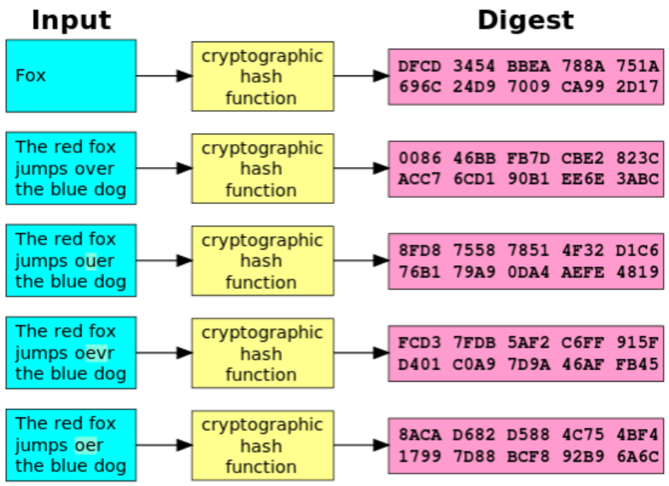
Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Fig. 2. Cryptographic hash function at work

1.1.3 Merkle Tree

Merkle trees are named after Ralph Merkle who invented this concept. Merkle trees follow a bottom-up approach. Merkle trees are data structures where each non-leaf node's key is obtained by hashing the keys in child nodes. The example in **Fig. 3**[2] is the simplest form of a Merkle tree formed from four leaf nodes. The result is a Binary Merkle tree. The root has the hash of entire tree. The structure of the tree is such that it enables us to easily identify where changes in that data occur. With Merkle trees one can verify if the hashing of data is consistent all the way up the tree and if not, they help to look in the correct position without having to look at all the hashes in the tree. So, with this property of Merkle tree we can verify the integrity of whole data by obtaining a branch of the tree and a publicly known Merkle tree root or otherwise known as root hash.

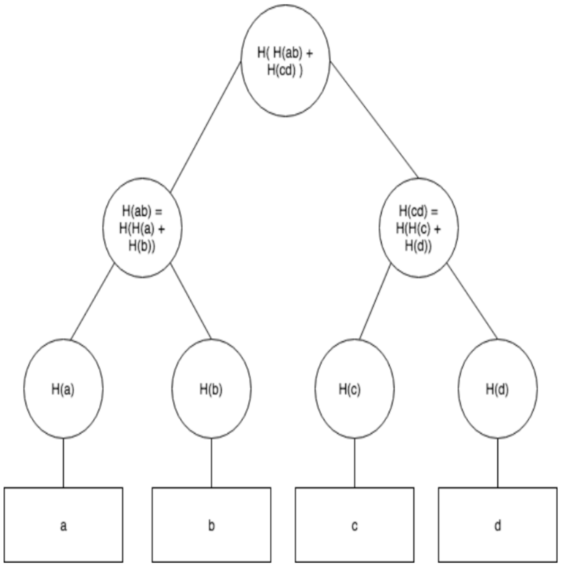

Fig. 3. Binary Merkle Tree

2 Decentralized networking in Blockchain

Decentralization means there is no central point of control (See in **Fig. 4** [4]). Absence of single point of control makes the network fault-tolerant and more secure.

[1] Refer to https://en.wikipedia.org/wiki/Cryptographic_hash_function

[2] Refer to https://hackernoon.com/merkle-tree-introduction-4c44250e2da7

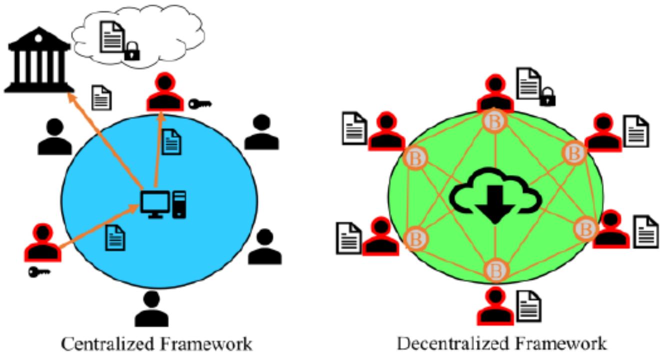

Fig. 4. Centralized blockchain systems versus decentralized blockchain systems

Blockchain technology instead of relying on a central authority for secure transactions with other users, uses consensus protocols. Consensus protocols among the nodes in the network helps to validate blocks and add them to blockchain without violating data integrity. Since blockchain is a public ledger keeping data integrity is a major concern.

Since there is no central authority, we can stop paying any authorities to secure our transactions and we need only to pay nominal fees to miners and people who run nodes (full and lightweight). Also, there is no single point of failure due to decentralization of blockchain. We can store blockchain data on multiple nodes and thus data is always available.

2.1 Consensus Protocol

Consensus protocol is another important concept in blockchain technology. It describes rules of communication and transmission of data among nodes. Consensus is a general agreement about something among some group of people and here it is group of nodes. This protocol helps nodes around the world to come to an agreement in considering a block as valid and adding it to the blockchain. When enough nodes on the network agree that a block is valid it is then allowed to be added to blockchain. This prevents fraudulent and duplicate blocks being added to the blockchain and getting corrupted by hackers. This is used in the mining process and distribution of blockchain data to other nodes in blockchain technology. There are different consensus protocols which are meant to make the blockchain foolproof. They are all very difficult to implement or fake them in terms of time and computation power they take. Different consensus protocols use different ways to stop people from doing fraudulent activities on blockchain.

2.1.1 Proof of Work (PoW)

Proof of Work is the most popular consensus protocol which is also used by cryptocurrencies Bitcoin and Ethereum. In Proof of Work protocol, for a block mined by a miner to be agreed as valid among other nodes or miners, the miner of the block must find solution to a complex mathematical problem for finding eligible digital signature for the block by using hash function. This solution is found by brute force approach using a lot of computational power. The digital signature mined by a miner is then validated by other miners against preset rules. Miners with more computational power are likely to find the solution first.

To cheat Proof of Work system, the attacking miner trying to modify a past block should also modify all the blocks between that block and the current block being worked on by miners. He also should do this modification before all the other miners finish working on current block.

2.1.2 Proof of Stake (DPoS)

In a Proof of Stake system, the person who has more stake creates the next block. This stake is issued to them by the users or they earn them by mining. So, user puts his wealth at stake to verify transactions. Randomization is also employed to make sure that the richest holder not always gets to validate blocks and earn rewards. Users who create new blocks in this system are called 'forgers' unlike 'miners' in Proof of Work system. If a forger validates a fraudulent block, he loses his stake. Some cryptocurrencies using this system currently are BlackCoin, Lisk and Peercoin.

This system can be randomized to prevent rich stakeholder from validating blocks all the time and getting even richer from earnings. In Delegated Proof of Stake (DPoS), voting is conducted to select validators of blocks by the users.

3 Peer to Peer (P2P) distributed networking in Blockchain:

A peer to peer distributed network is an important concept behind Blockchain technology. It is the reason why blockchain is very secure. In a P2P network, each individual node is referred to as 'peer'. Each peer uses help of and provides help for other peers in the network. They share disk storage, processing power, network bandwidth of each other without help from any centralized control or a master. Many nodes (full nodes) have full copy of blockchain data. So, it is difficult to destroy data of blockchain because to do this the attackers have to delete the data on every node which has blockchain data copy.

3.1 Nodes

A node is any computer or other type of physical hardware device that is connected to blockchain network or any network in general. The nodes should have storage capacity and internet access. They also should run blockchain software which enforces the rules or protocol. Though we might need one node to save blockchain transaction history, blockchain has so many nodes connected to the network. So, if all other nodes are fallen, we need only one node up and running to create a new network again. The more the nodes in the network, the secure the blockchain is. The nodes are synchronized with each other such that even when a node goes offline, it can download data from other nodes once it comes online again.

3.1.1 Types of nodes

In blockchain the nodes can be 'full node' or 'lightweight node'. A full node downloads all the transactions and blocks in the blockchain network. They also accept the transactions and blocks from other full nodes and validate them against consensus rules of the blockchain network. After validation they relay those transactions and blocks to other full nodes.

A lightweight does not have all the transactions and blocks. These nodes use Simplified Payment Verification (SPV) to verify transactions by downloading a copy of headers of blocks on the blockchain which are enough to validate the transactions instead of downloading whole blockchain (See in **Fig. 5** [1]). They depend on full nodes to function and connect to blockchain network. Full nodes may reject blocks and transactions which were accepted as valid by lightweight nodes.

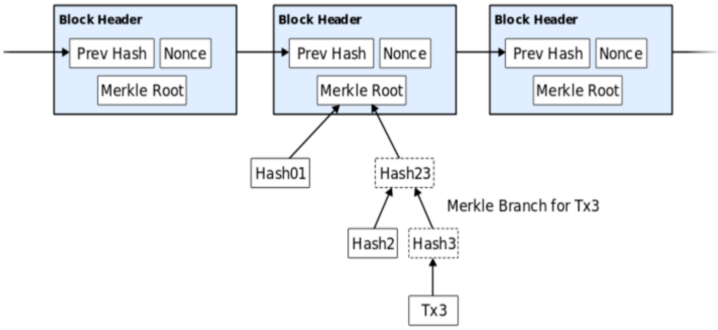

Fig. 5. Simplified Payment Verification in lightweight node

Though miners are not considered as nodes, miners can set up their own nodes and almost every miner have a local node set up. These can be considered as worker nodes. Miner nodes are involved in a very important task of Blockchain technology called "mining". This is the process where the transactions are clustered into blocks. These blocks are then validated and added to the blockchain.

After mining is complete, the miner sends the info of all transactions mined along with the new block that is mined from those transactions to all nodes. The information is now sent from node to node to reach all nodes.

3.1.2 Mining and how it works

Mining process in blockchain is where we can see the prominence of peer to peer networking. Mining is a difficult task that consumes lot of time and resources in Blockchain technology. Here the computing power, internet access and storage of the mining nodes are used to mine blocks. If there is no mining in blockchain, someone could spoof a transaction to gain money or loot someone. They could enter a fraudulent transaction in the blockchain and add so many other such transactions on top of it making the fraud impossible to find.

In mining, many people who are living across the world and doesn't know each other, receive the latest batch of transaction data. This data is passed through a cryptographic hash algorithm that generates a hash which is a string of numbers and letters that helps to determine information's validity. During mining process, information is not revealed to the miners. The miners should always be connected to other nodes to pick up new transactions and also to find the previous block's hash. The miners get paid to do this work.

Here is how the process of mining works ---

Step 1: A user does a transaction from a blockchain application. For example, this application can be a Bitcoin wallet in which you can view your Bitcoin holdings and send or receive Bitcoins.

Step 2: This transaction is then broadcasted to the network by the blockchain application. The transaction is now in a pool of unverified or unconfirmed transactions until it is not picked up by a miner. These unverified transactions are collected in small subdivided local pools instead of one giant pool. Miners on the network verify these transactions against the rules set up by creators of blockchain network.

Step 3: Later miners cluster some of these verified transactions into a 'block' along with the metadata. Though every miner constructs their own block, there is a chance that more than one miner can pick the same transaction and include it in their block.

Step 4: To add this block of transactions to the blockchain, the block should have a unique signature. This signature is obtained by solving a very complex mathematical problem that is unique to transactions within the given block. Each block poses a different mathematical problem, so each miner must work on a different problem that is unique to the block they created.

The complex mathematical problem every miner must solve to add a block to the blockchain is to find a hash output or signature for the data in the block, that starts with a certain number of leading consecutive zeros specified in the rules of blockchain. All these problems are hard to solve and consumes lot of computing power.

Step 5: The miner that finds a valid signature for the block of those specific transactions first, broadcasts that signature to all the other miners.

Step 6: All the other miners now must verify if the input transactions actually result in that signature. For this the miner that found a solution should send his 'proof of work' to the other miners. When 'consensus' about the validity of signature as described on the blockchain is reached, the block is then added to the blockchain along with the signature and broadcasted to all other nodes on the network along. All other nodes will accept this block into their copy of data after validating it.

Step 7: Every time a block is added to blockchain it counts as a 'confirmation' for the block beneath it. For example, if a block X has five new blocks added on top of it, then the block X has five confirmations. If number of confirmations for a transaction increases, the transaction becomes more harder to alter. Miners sometimes cannot continue mining because of the blocks they are mining may contain transactions that have been verified as part of the last block that was added to the blockchain. These transactions which are already verified may become invalid, making the whole block invalid.

4 Cryptography in Blockchain

Cryptography is another core aspect of Blockchain technology. It is a process of encrypting and decrypting information or data using complex mathematical algorithms. This is to protect from revelation of data to unintended users. Cryptographic system has five parts – plain text, cipher text, key, encryption and decryption algorithms. Once encrypted, the data can only be read after it is decrypted. We use keys to encrypt or decrypt the data. There are mainly two types of cryptography which are symmetric and asymmetric cryptography. Symmetric cryptography uses only one key to both encrypt and decrypt. Asymmetric cryptography uses two keys called public key and private key for encryption and decryption. Asymmetric cryptography is also referred to as public key cryptography.

In public key cryptography, data is encrypted with receiver's public key. The receiver uses his private key to decrypt it. This preserves the confidentiality of the data as anyone else other than receiver cannot decrypt it. It is computationally infeasible to derive one key from the other. So, user can share his public key to anyone without any worry that someone can find his private key from his public key.

Digital signature is a variety in public key cryptography to promote authenticity of the data or document. It also promotes non-repudiation and integrity of data. Here data is hashed and then signed with sender's private key. The receiver can only decrypt it with sender's public key.

Integrity is preserved by hashing since small change in data can lead to a different hash and resulting cipher text cannot be decrypted by the receiver. So, the receiver knows that data has been tampered.

Non-repudiation refers to a situation where a data or document's author cannot deny its authorship or the validity of an associated contract. Digital signature promotes non-repudiation since it is signed by author or owner of document where signature is unique to each signing author.

Blockchain technology uses digital signatures with hashing. Here the transactions themselves are part of the digital signature because during signing, data is combined with private key to make a signature. If any transactions are tampered, the nodes in the network will consider it as invalid. Modifying the data changes the hash value which changes the whole signature, making the block false and obsolete. Due to this blockchain data becomes immutable. Some blockchains use Multisignature or in short multisig where a transaction needs to be approved by more than one signee here it can be miners or other nodes.

5 Economics of Blockchain Technology

In online transactions, there are many third parties involved like e-commerce websites, payment gateways (Paypal for example) and banks. There is a lot of verification [3] that is involved with these third parties. E-commerce websites need to verify authenticity of their users, enforce terms & conditions for fair use of website by buyers and sellers. Similarly, payment gateways must authenticate their users and verify the credit/debit card details with card providers/bank. Card providers/banks should verify if the user has enough funds to make the purchase. These verifications by third parties become costly and are usually levied on users. With Blockchain technology along with smart contracts we eliminate the third parties which means we cut down the costs of verification. Also, we can eliminate the risks of data breaches like debit/credit details, user personal and transaction details and cut down costs of keeping data secure. Even starting a new blockchain network and growing it is less costly by giving tokens to early adopters for their capital, resources and effort and incentivizing users who join later with tokens for their resources.

6 Applications of Blockchain Technology

Blockchain is introduced a decade ago to store or sent cryptocurrency, Bitcoin. But its applications don't stop there (See in **Fig. 6** [4]). As the awareness about the technology spread worldwide, it is being used in various sectors in innovative ways.

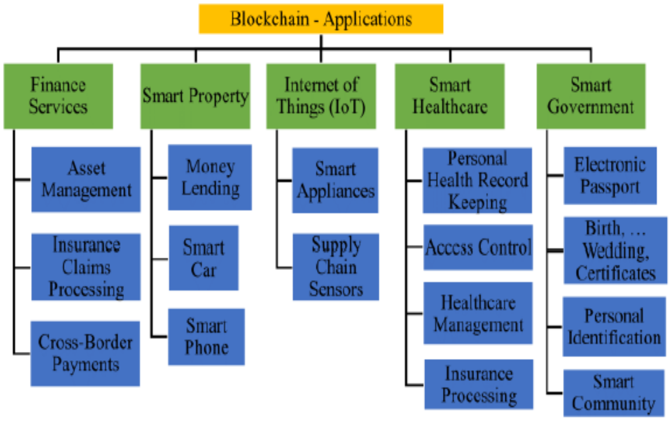

Fig. 6. Applications of Blockchain technology

6.1 Cyber Security

6.1.1 Fraud and data theft protection

By using Blockchain technology we can prevent frauds and data theft in different sectors [4]. If an attacker wants to corrupt or destroy data, he must corrupt or destroy data present on every node of blockchain network which is impossible as there are millions of nodes around the word which full or partial data of blockchain on them. Even one up and running full node can be used to bring back the network again. Thus, Blockchain technology became the most secure form of storing and sharing information.

Guardtime is a software security company that is successfully using blockchain technology to keep data safe. The company distributes the data among the nodes in their network. If someone tries to modify the data, the system analyses the whole blockchain data, compares them to the metadata and then excludes data that don't match up. Their system is always able to detect the data changes and constantly verifies the changes.

6.1.2 Network Security -- Protection from DDoS attacks

Domain Name System (DNS) is an important part of the Internet. It maps human-friendly domain names of machines connected to the Internet or a private network to numerical IP addresses. DNS is partially decentralized meaning a part of it is still centralized. These centralized DNS' acts as single point of failure and makes the systems vulnerable to DDoS attacks. DDoS attacks bring down the servers from serving the users. But using Blockchain technology here helps us to prevent these attacks. The content of DNS is distributed across large number of nodes and the domain editing rights are only given to domain owners such that data cannot be accessed or altered by unauthorized users.

Blockstack is a company which is providing a fully decentralized DNS. They are creating a decentralized worldwide web by replacing all centralized third-party Internet service providers who owns servers, databases and other infrastructure. Also, since DNS data is on multiple nodes it is impossible to destroy or alter data.

6.2 Applications in Government

Any countries which face corruption in its bureaucratic procedures can adopt Blockchain technology since this is tamper-evident and tamper-resistant [5]. Lisk Academy[3] proposed some use cases of Blockchain which government can use like voting and notarization.

6.2.1 Voting

In democratic countries, leaders and officials are elected by voter census. Current voting systems are inefficient and can be rigged. So, Blockchain technology can be used to conduct voting process to prevent rigging. Voter ballots can be encrypted and stored on blockchain network. These encrypted voter ballots cannot be tampered and can be traced back to everyone who voted. Since there is no central authority, rigging by governments in corrupt countries can be prevented.

6.2.2 Notarization

Documents such as birth and death certificates, driving licenses, educational documents, ownership titles are created, signed and stored on traditional databases which can be hacked to destroy, steal or alter data. The timestamps on these documents are validations for the time when these documents are created and signed and happenings of events in the documents. These documents can be stored on blockchain safely and due to security features of Blockchain technology such as fraud-proof and fault-tolerance these documents will be safe and untampered and are visible only to authorized parties.

Blockchain technology can also be used to provide certified interaction between multiple citizens and governmental bodies simultaneously for processing their documents. This improves the efficiency of governmental bodies and cutting-down the delays for document processing and also the waiting time at the government offices.

The Indian state of Andhra Pradesh which is the first state in the country to embrace Blockchain technology is using it to manage land records and vehicle registrations to protect them from tampering by outsiders and insiders[4].

6.3 Healthcare, Banking and Real Estate

There are a lot of document processing in healthcare and real estate. In healthcare industry, doctor prescriptions, lab reports, vaccination records and insurances of patients and in real estate contracts between realtors, property owners and customers and registrations of properties when sold or ownerships changed are the documents which need to be kept confidential and tamper-proof. Using Blockchain technology in these industries can help them to safely save them and can be used to validate ownerships. Also, in banking account creation documents, loan approval documents, records of processed cheques or money orders can also be saved securely.

MIT's proposed MedRec[6] is a decentralized electronic medical records management system using Blockchain technology. Patients choose different health providers at different stages of their lives and these health providers have the patients' data to themselves. Storing, maintaining and securing all the patients records in traditional methods is a difficult task and sometimes they must remove some records

[3] Refer to https://lisk.io/academy/blockchain-basics/use-cases

[4] Refer to https://www.forbes.com/sites/outofasia/2018/03/05/this-indian-city-is-embracing-blockchain-technology-heres-why/#1a2a5b618f56

due to storage limitations. MedRec proposes all medical stakeholders to be the 'miners' and incentivizing them with useful patient data for their computation power in mining. This data later can be used by researchers to research about patients.

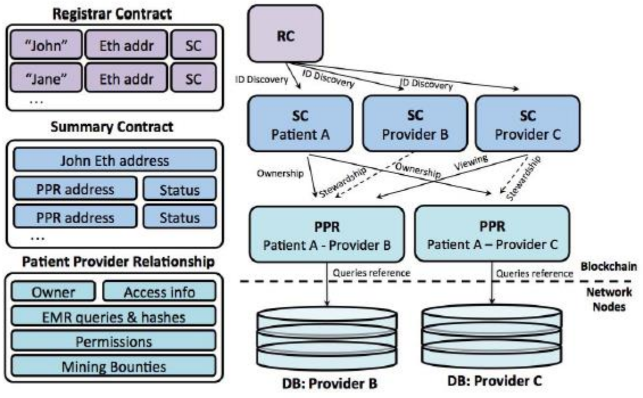

Fig. 7. MedRec smart contracts on the blockchain and data references

6.4 Internet of Things (IoT)

In Internet of Things, lot of devices interact with people and among themselves for personal use or industrial use and create a lot of data during this process. Cisco is predicting 50 billion IoT devices will be connected by 2020. Blockchain technology is set to play an important role in the security of IoT devices [2].

Currently, IoT relies on centralized server/client architecture to process communication among devices. Since IoT devices produce a lot of data sometimes very sensitive data, managing the infrastructure needed to store and secure this data becomes very expensive. If the central authority is compromised the data can be tampered or the control devices can be taken over by malicious attackers and they can disrupt the day to day activities of people. Using Blockchain technology, IoT applications can be decentralized and data can be saved in multiple nodes and thus proving fault tolerance. Since the data is encrypted and fraud-proof, sensitive data is secured and cannot be destroyed. Also, it can be used to sell data for cryptocurrency by IoT device owners.

6.5 Smart Contracts

Using smart contracts in blockchain applications, we can implement self-executing contracts with the terms of the agreement between producer and consumer or server and client or buyer and seller written directly into lines of code. This code is then distributed and decentralized in the nodes of blockchain network so there is no need for central authority for the functioning of the system. The rules specified in the contracts are enforced by the peers in the network. This promotes automation in blockchain applications and the transactions are verifiable and secure. Use of smart contracts lower the transaction costs, saves time of the users compared to traditional contracts. We can see the schematic of a cryptocurrency system using smart contract in **Fig. 8** [7].

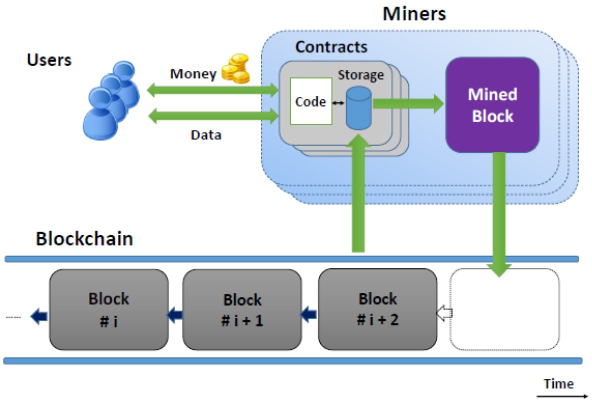

Fig. 8. A cryptocurrency system with smart contracts.

Smart contracts should not be buggy and the transactions on it should be made to ensure fairness to prevent fraudulent transactions and guarantee a safe and secure platform for the users' money without cheating. The programmers who develop these smart contracts should be economic minded as well compared to traditional programmers as these involve financial agreements and transactions [7].

7 Conclusion

In this survey paper, we discussed the networking perspective of Blockchain by discussing its decentralized, distributed peer to peer networking. We discussed how the cryptography and

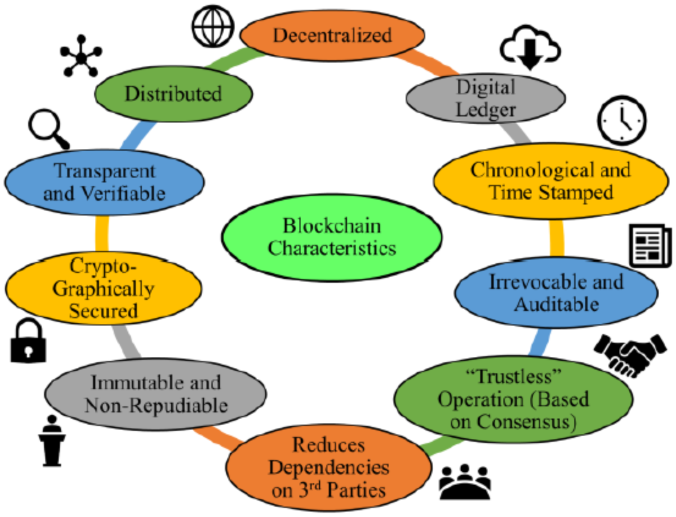
Decentralized
Digital Ledger
Chronological and Time Stamped
Irrevocable and Auditable
"Trustless" Operation (Based on Consensus)
Reduces Dependencies on 3rd Parties
Immutable and Non-Repudiable
Crypto-Graphically Secured
Transparent and Verifiable
Distributed
Blockchain Characteristics

Fig. 9. Characteristics of blockchain [4]

decentralized nature of Blockchain can help us in preventing data attacks and data loss. We discussed how consensus protocols are used to validate the digital signatures or hashes on blocks. We have also discussed how all the features of Blockchain technology helps us in cutting down the costs of maintaining and securing data and by providing intermediary-free platform. We have also discussed various use cases and applications of Blockchain technology other than its first application of cryptocurrency. We have also discussed smart contracts with which we can implement financial contracts directly on blockchain network by writing it into the code without any need for manual verification.

References:

[1] Nakamoto, Satoshi. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf.

[2] Salah, Khaled & Ahmad Khan, Minhaj. (2017). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems. 10.1016/j.future.2017.11.022.

[3] Catalini, Christian and Gans, Joshua S., Some Simple Economics of the Blockchain (September 21, 2017). Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16. Available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," in IEEE Consumer Electronics Magazine, vol. 7, no. 2, pp. 18-21, March 2018.

[5] Ølnes S., Jansen A. (2017) Blockchain Technology as s Support Infrastructure in e-Government. In: Janssen M. et al. (eds) Electronic Government. EGOV 2017. Lecture Notes in Computer Science, vol 10428. Springer, Cham

[6] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30.

[7] Delmolino K., Arnett M., Kosba A., Miller A., Shi E. (2016) Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg