Blockchain and Distributed Ledgers

Vishwas Sreevalli Ramamohan
Vsreev2@uic.edu
Dept. of Computer Science
University of Illinois at Chicago

***Abstract*— Blockchain as the name suggests, is a chain of blocks that contain information. In this paper, the basic idea of the Blockchain and Distributed Ledger technology is discussed. The blockchain and different variants of its system, along with the impacts that it has on the world and a few existing use cases have been discussed. Finally I present an idea for a use case that I would like to call as "Self-repairing motor vehicle systems", which is an extension to the application of blockchain that uses Internet of Things. The underlying mechanisms are explained and the advantages of the system are clearly indicated.**

I. Introduction

Trust, as we've seen is the fundamental thing for transactions. It is very delicate and close to us, also very easily breakable. Imagine a fraud prevention system for conducting transactions wherein trust is immutable. A system which is transparent and incorruptible, where you can guarantee the validity of a transaction [1]. A durable and robust system that is not centralized and a mechanism to bring all transactions to the highest degree of accountability. Yes, Blockchain technology is a distributed ledger that changes the way we trust.

When it comes to transacting anything of value, people and businesses have mostly relied on a centralized intermediary to ensure authenticity. These intermediaries perform a series of tasks to build trust in these transactions, like validity and record maintenance [2]. Now with the help of blockchain, these intermediaries can be eliminated without worrying about trust or malicious transactions. This distributed ledger keep track of who owns what and has a network of replicated data, synchronized and available within the network. These networks can be made private, like an intranet, or publicly available to everyone on the internet. Looking at the recent improvements in the technology, we can say that blockchain has created the foundation to a new type of internet.

Transactions happen securely in the network. During a transaction, all the relevant details are put into protected blocks cryptographically and sent out to the network. Since multiple transactions can occur at the same time, a short time interval is set for sending out blocks to the network. The members in the network with high computational power (also known as miners) then validate the transactions by solving complex encrypted problems. The first member to arrive at the solution is usually rewarded (as in the existing systems like Bitcoin) and the validated block is time stamped and added on to the chain in a chronological order. Newer blocks are linked to the previous existing block, thus forming a chain containing all the blocks in the history of the particular blockchain. The network is continuously updated and every ledger holds the most updated data. This helps the members identify ownership at any given point of time.

The transactions here are peer to peer and the cryptographic nature of it enhances security benefits. Various centralized intermediaries are usually affected by security threats such as hacking and phishing and information leaks, which now becomes obsolete in the blockchain technology. This is because, if hackers wants to obtain information from a block on the blockchain, they would not only need to decrypt that particular block, but also all the previous blocks going back to the beginning of the blockchain. And since the ledger is distributed, they would have to do it on all the ledgers in the network, simultaneously, which could be a lot, maybe in millions.

II. System

Like we already know, the distributed ledger is an open system that contains blocks of digitally sealed information. This ledger is replicated across several computers assembled in a peer-to-peer network. All communication inside the network makes use of cryptography to identify the sender and receiver. When a new set of data needs to be added to the ledger, a consensus is formed in the network to determine if the data has to be added; the consensus is known as a block.

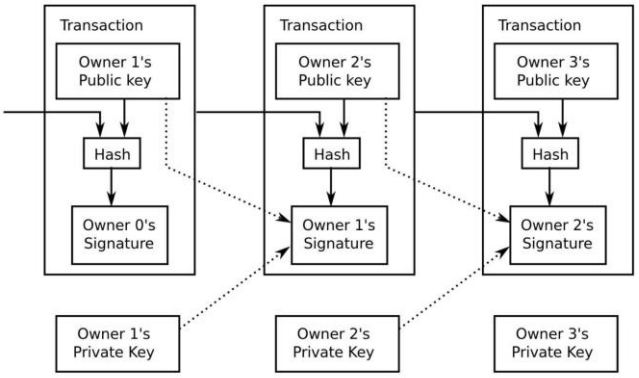
The block contains the data, a hash value and the hash of the previous block. The data here depends on the type of blockchain. A Hash can be compared to a fingerprint; it identifies the contents of the block and is always unique. Once a block is created, its hash value is calculated. Changing something inside the block changes the hash value entirely. The hash of the previous block effectively creates a chain of blocks and this technique makes the blockchain highly secure.
The first block in the chain is a special block, called the genesis block, and it does not contain a link to any previous block. All the following blocks contain the link to previous blocks. In case a block is tampered with, it causes the hash of the block to change as well. In turn, this will make the successor block and all the following blocks invalid as they no longer contain the valid hash of the previous block.

Using hashes is not enough to prevent manipulation. With the use of computers with high computational power, one could calculate a large number of hashes quickly. So not only the block can be tampered, but all the hashes of other blocks in the chain can be recalculated to make a different blockchain valid again. To mitigate this, the technology has an advanced consensus mechanism called the proof of work, which slows down the creation of new blocks. Now with this mechanism, it is highly difficult to manipulate the blocks, because to do so on one block, the entire proof of work needs to be calculated for all the following blocks. So using the hashing and proof of work creatively, and being distributed, the blockchain attains its security. Therefore, the blocks that are manipulated will be rejected by other nodes on the network. Finally, to successfully tamper with a blockchain, one needs to manipulate all the blocks on the chain, redo the proof of work for each block and take control of more than 50% of the peer to peer network and only then will a tampered block becomes accepted by everyone else on the network, which is almost impossible to do.

A. HASH

A hash is a one way function that has multiple uses in decentralized systems. All the digital media, like documents, videos or audios are just strings of binary digits, ones and zeroes. A hash function takes any digital media and runs an algorithm on it to produce a fixed length and unique digital output, known as a hash. The hash is much smaller than the original input. Every time the same digital media is put through the function, it produces the exact same hash value. Even if a single bit of data in the digital media is changed, the hash value changes completely than the original one. The algorithm behind the function ensures that there is no way to derive the original digital data from its generated hash value, thus making it one way.

The technique of digital signatures was originally described in 1991 by a group of researchers and was intended to timestamp digital documents so that it is not possible to back date them or to tamper with them. However it was mostly unused until it was adapted by a group to build the most popular cyptocurrency ever in 2009, the Bitcoin.



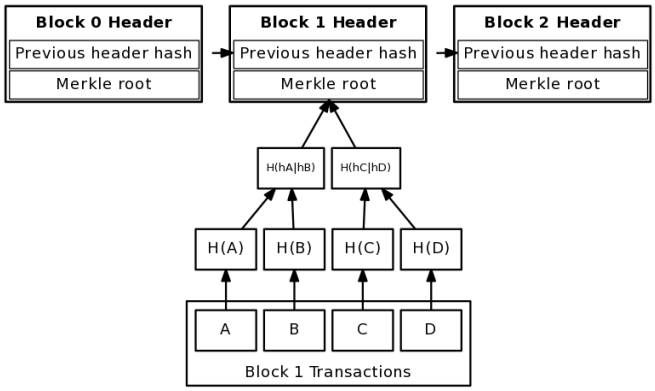
Everyone on the network generates a pair of public key and private key. A digital signature is usually a string of ones and zeroes, usually of 256 bits. Altering the message even slightly completely alters the signature.

B. MINING

In blockchain, the notion of mining requires miners to solve a problem with a partially known input derived from the latest state of the blockchain. These miners are different members on the network, competing to see if their local block is going to become the next block on the chain, for the entire network. The miners need to guess the digital input that can create the hash target, thus solving the problem. Since the hash is one way, the miners are required to solve many combinations of input to create the hash target and thus solve the problem, which uses a lot of CPU resources. The first miner to solve the problem wins and a new block is hence added. A member on the network is not a miner by default; it's a voluntary process to turn a member into a miner. Usually there is small reward that is associated with every transaction for the successfully miner. Additionally, there may be an extra incentive added by the transacting parties for the winning miner, thus encouraging the members on the network to become miners.

C. MERKLE TREES

Merkle trees are a basic part of blockchain that enhances data integrity. A block can contain multiple transactions which each contain data.



Merkle tree connecting block transactions to block header merkle root

In the above figure, we have four different transactions: A, B, C and D. Each of the transaction's data is passed through the hash function generating unique hashes, one for each transaction. Now, pairs of hashes are combined and then passed through the hash function again, which produces two separate and unique hashes that are based on the combination of two hashes of two transactions. The two hashes are combined again and passed through the hash function. This results in a single root hash, which becomes the Merkle root and hence forming a complete Merkle tree. The tree allows for detection of any changes to any data within the transactions of a block by simply rerunning the hash function for the transactions and comparing the results to the original root hash.

D. CONSENSUS – PROOF OF WORK

"Proof of work" is the most commonly used consensus mechanism in blockchain. It involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. A block once formed after satisfying the proof of work, cannot be changed without redoing the proof of work all over again. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it. Proof of work is essentially one member one vote. The member that invests the greater proof of work effort will have the longest chain and that is used to represent the majority decision. To ensure that the competition is equal for varying hardware speed the proof-of-work difficulty is determined by targeting an average number of blocks per hour.

III. TYPES OF BLOCKCHAINS

A. PUBLIC BLOCKCHAIN

A block of peer to peer transaction is verified and synced with every node affiliated with the blockchain before it is written to the system. Until this completes, the next transaction cannot occur. Due to this, the public blockchain becomes slow yet extremely secure. Though users can maintain anonymity in the public network, it uses up a lot of resources, such as electricity and CPU which increases with every additional node in the network. A public blockchain is most suitable when the network needs to be decentralized. When security and decentralized network is at high priority, it's always best to use a public blockchain. Best example is a cyrptocurrency, like Bitcoin.

B. PRIVATE BLOCKCHAIN

This version of blockchain lets the intermediary exist to a certain extent. The intermediary verifies each transaction, resulting in faster transactions and higher efficiency. It does not offer decentralized security and anonymity. The intermediary can also choose who has read access to the blockchain, allowing for a greater privacy than a public blockchain. This kind of blockchain is suitable for traditional businesses and governance models. Various outdated institutions and models can be brought to modern practices using this. A system of a secure online voting system is a good example for this.

C. CONSORTIUM BLOCKCHAIN

This blockchain is partly private. It provides a hybrid between the public and private models of blockchains. Here any person can participate in the verification of transactions process or allow only one company to have full control and a few selected nodes are decided. It provides efficiency and transaction privacy. The blockchain has many advantages of a private network, but operate under the leadership of a group instead of a single intermediary. This would be most suitable for organizational collaboration.

IV. IMPACT

Blockchain is set to bring a promising change to the world of transactions. From shifting the way internet is accessed to creating a breakthrough in the global economy, the technology is set to transform things around us. Through digitization of assets on the blockchain, it enables a platform where these assets can be exchanged instantly, peer to peer. A new transformation of immediate exchanging of values is emerging, where intermediaries will not be playing a major role anymore. This is system where trust is established not by the intermediaries, but by consensus and complex unbreakable computer code.

As we can see, the applications of blockchain is vast: crypto currencies, money transfers, electronic voting, smart contracts, digitally recorded healthcare management, property assets and proof of ownership of digital content are a few examples. Therefore, blockchain is set to majorly disrupt many industries that heavily depend on intermediaries like banking, real estate, finance, healthcare, insurance and many others. Though elimination of intermediaries might result in mass unemployment, it mostly brings positive benefits. The intermediaries often impose an expensive transactional fee and a high turnaround time. With blockchain, an increased number of people and businesses are encouraged to trade and perform transactions more efficiently and frequently.

While the commercial world is advancing with the outstanding technology challenges of the blockchain, its popularity has increased tremendously in various developing countries where the major element of commerce is trust. Various organizations have been discussing how the blockchain is going to affect the world in the next 10 to 15 years and many believe that it is designed to end poverty, protect the environment and bring prosperity for all. They think that many areas such as security, climate change, urbanization, and people's rights etc. where bringing a drastic change is hard, will now be easy to access using the blockchain technology.

One of the most favorable areas that blockchain is set to impact on a large scale is real estate. Land registrations and managing land titles have always been a hard task and prone to easy manipulation across the world. The independent evaluation group of the World Bank quoted that 70% of the world's population lacks access to proper land titling or demarcation. Considering to address problems like these, many government bodies have started to work towards improving the systems. The National Agency of Public Registry in Georgia is working with an organization called BitFury on a pilot project that is proposed to use a transparent, secure ledger to manage land titles. If this becomes successful, they hope to increase the transparency of land ownership and also cut down the registration fees by up to 95%. Another project which is partially funded by the World Bank is in motion, alongside working with the government to build a prototype for a land registry that uses blockchain.

V. USE CASES

A. BITCOIN

The most popular virtual currency system that is similar to the real world cash system. The Bitcoin currency network is decentralized and there is no central authority. [1] A network of miners validate all transactions on the network. Bitcoin has continued to grow at an exponential rate and the peer to peer electronic currency is a highly valued one at the present day.

B. ETHEREUM

A second gen blockchain technology that was designed to let anybody develop and deploy their own decentralized applications of blockchain. It has its own cryptocurrency called Ether [4] which acts similar to how bitcoin does. The highly accessible ethereum has its own virtual machine that powers the memory and applications, along with its own programmable language called Solidity.

C. SMART CONTRACTS

Autonomous computer systems that are written in code to manage executions between individuals on the blockchain [3]. The Ethereum blockchain contains the code at specific addresses. These contracts are powered by the virtual machine and the currency Ether. To make it more secure and customizable, Ethereum created some high level languages which are used to create the smart contracts for the virtual machine. These are few innovations by Ethereum and allows for many types of autonomous programs.

D. SUPPLY CHAIN

Customers always crave to know the ethical claims companies make about their products to prove them real. Using distributed ledgers, it would be easy to certify that the things that we buy have genuine stories. Transparency comes with blockchain-based time stamping of a date and location — on ethical diamonds, for instance — that corresponds to a product number. Various organizations have started adapting blockchain for supply chain auditing, using the ethereum.

E. CROWDFUNDING

Many initiatives, such as Kickstarter and Gofundme have started to make use of the peer to peer economy. The number of users on these sites show us that people actually want to have a direct say in the product development. Blockchain has the potential to create crowd sourced venture capital funds, as seen in an experiment by the ethereum based Decentralized Autonomous Organization (DAO) who raised $200 million USD in just 2 months.

F. IDENTITY MANAGEMENT

The identity management on the web is brittle. The ability to verify the identity is the powerful thing on the web that is core to many financial transactions. Distributed ledgers offer enhanced methods in proving

the identity, alongside the possibility of digitizing personal documents. Having a secure identity will be important to create a good credibility and reputation for conducting online transactions. This however, has proven to be highly complex to develop. It requires the cooperation between private bodies and the government to obtain a universal online identity solution. Netki, a startup has proposed to create an SSL standard for blockchain.

G. STOCK TRADING

The highly efficient and secure blockchain technology can be used for stock trading. Trade confirmations become almost instantaneous when it's done peer to peer, hence removing the intermediaries such as the clearing house and auditors. Many stock and commodities exchanges have built prototypes for their services using blockchain. Nasdaq has recent announced the development of a blockchain prototype project for proxy voting on the Estonian Stock Market.

H. FILE STORAGE

It is always advantageous to have decentralized file storage on the internet. Distributing data throughout the network prevents files from getting hacked or lost and hence the data is protected. The IPFS helps us understand how a distributed web might operate. Like the bittorrent moving data around the internet, IPFS gets rid of the centralized client-server system. The file transfer and streaming times can be improved efficiently if the websites are decentralized. It is seen as a necessity to upgrade the system as the web is currently overloaded with content delivery systems.

VI. MY IDEA

The paper till now talks about the core blockchain technology and its implementation, along with its impacts and various use cases in multiple fields. Now I would like to propose an IOT based use case. I would like to call it "Self-repairing motor vehicle systems".

The existing repair and upgrade operations for digital systems in vehicles mostly happen through a centralized party. The centralized service providers who have the equipment to provide the upgrades or make repairs usually charge an expensive fee and take a considerate amount of time to provide the service. Any digital system is prone to attacks and if a system in a vehicle is attacked, not only it would bring the vehicle to a halt, but also endanger the lives of the people on the vehicle.

Let's add the IOT enabled vehicles as trusted identities in a system. By making use of a suitable blockchain model (private or consortium) to keep the vehicles updated, we can eliminate the dependency on the centralized service providers. Using reputation systems and smart contract to govern who can make changes in the system based on a set of rules, we can make the system more secure, efficient and trustworthy. Here the companies that own the vehicles can optimize to connect peers in the best way possible, maybe with the use of a reputation calculator or a customized service.

Using a blockchain based system, any number of individual vehicles within a network could form an agreement between themselves regarding the latest services available, for example, a software version that is the most stable one. In the case of system failure at one node in the network, i.e. an individual vehicle, it can consult others in the network and using IOT applications, bring back itself to the most updated version of the particular software.

Now, extending this idea to a real time scenario: Consider a set of 'n' airplanes that belong to a particular aircraft manufacturer in a closed network. With the help of IOT, the manufacturer builds a communication system that enables peer to peer transactions. Let an airplane A1 that is currently flying discovers an issue with one of its critical softwares, due to an attack or failure. The airplane now quickly wants to bring the software back on to working state to ensure safety. A1 requests an update from the network of other flying airplanes on the blockchain and hence it gets the most latest agreed upon update, using IOT applications. By this way, the system can be brought up in a very short span of real time and make the plane safe once again. If the attacker wishes to bring down one system, he needs to breakdown the entire network of different planes, A1 to An, which is highly impossible, like I have discussed in the earlier sections of the paper.

VII. CONCLUSION

In this paper we discussed about the blockchain and distributed ledger technology, its working system, the impacts it has on the world and a few existing use cases. In addition to the existing use cases and with the help of an extension from the available technologies, I propose an idea for Self-repairing motor vehicle systems. Further, it is briefly shown how the system can be implemented and the various advantages it has and the set of problems it could solve.

REFERENCES

[1] Bitcoin: A Peer-to-Peer Electronic Cash System.[https://bitcoin.org/bitcoin.pdf]

[2] All you need to know about blockchain, explained simply [https://www.weforum.org/agenda/2016/06/blockchain-explained-simply]

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

[4] Ethereum blockchain app platform. [https://www.ethereum.org/]

[5] The truth about Blockchain [https://hbr.org/2017/01/the-truth-about-blockchain]

[6] Distributed Ledger Technology: beyond block chain [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf]

[7] Blockchain beyond Bitcoin by Sarah Underwood

[8] Growing the Blockchain Information Infrastructure by Karim Jabbar, Pernille Bjørn, University of Copenhagen

[9] https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html