Understanding Blockchain

Author: G Mpala

Student Number:201594339

Computer Science 3B

Introduction

In this research assignment I am going to uncover a lot about blockchain. Starting by giving a little bit of background on it, ending with how is blockchain impacting our lives at this present moment and what the future holds for this type of technology. What then this assignment aims to achieve, is the understanding of this technology (Blockchain), what is blockchain, how does this technology work, and where do we see this technology being used in the current industry. All these aspects, I am going to answer them fully throughout this assignment. This document will be divided into 6 sections. The first section will be the background of blockchain, secondly is the procedure involve in blockchain, thirdly I am going to address the benefits and disadvantages that comes along with this system, fourth section is the evolution into smart contacts and lastly is the use of blockchain in industry.

1. Background

In one of the article it describes blockchain as , "a distributed ledge technology in the form of a distributed transaction database, secured by cryptography and governed by a consensus mechanism" (Beck, et al., 2017). In simple terms this means it's a technology that has no central point and independent to any controlling power that allows the involvement or the participation of every individual to store data or information within the system and allow transactions among each other without the involvement of a third party such as a bank. These transactions are immutable, can only permit transaction but disallow any alteration to be made on the transactions.

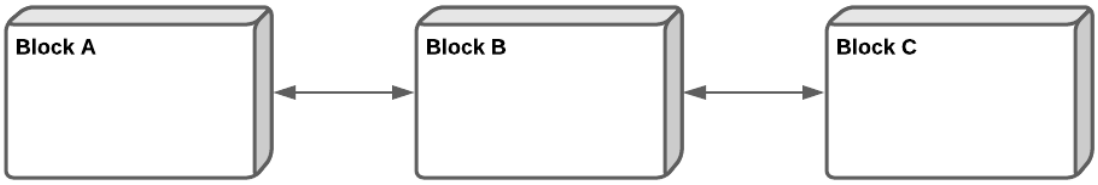
The concept of blockchain it is said to have been introduced by Stuart Haber and W. Scott Stornetta as a cryptographically secured chain of block (Oldenbourg, 2018). The notion was to create a system that was not going to allow a document to be manipulated. This technology only came to its full potential in the year 2008, when Satoshi Nakamoto used the technology to create what we know in this day of an age the world's first digital currency known as Bitcoin (Oldenbourg, 2018). This blockchain application on bitcoin made use of three technology which cryptography, consensus, and the peer-2-peer systems. I am going to expand more further about these technologies later.

It's not only bitcoin that came as a major breakthrough of the use of blockchain technology, in recent years they have been major innovations of blockchain technology such as the creation of smart contract that is the exchange of anything of value without a third-party, transition to proof-of-stake mining which evolves the creation of new block with the transaction approved and lastly the blockchain scaling solutions (Trade Finance Global, 2020).

2. How does blockchain work

Blockchain consists of blocks connected to each other. A single block serves as a container of data that can store files or information. They are three elements involved with a block. Firstly, the data stored in a block. This can be any type of data, in reference to bitcoin the block will store transactional data that will include the amount of bitcoin, the sender details to which the amount is from and the details to where the amount is to be sent. Other example will be storing a file, this will include the filename, the size of the file, who created the file and when the file was created.

Secondly, a block contains a hash that uniquely identifies a single block. A hash makes use of a function called cryptographic hash function. This is a mathematical function that takes an arbitrary amount of data input and returns an encrypted output of a fixed length (Frankenfield, 2020). Through this hash function the data is secured and makes it difficulty to change the content in the block, by examining the integrity and authenticating the information. Lastly, a block contains hash of the previous block. With this in place a chain of blocks can now be created.



A practical example it will be having 3 blocks connected to each other, each block having its own unique hash and a hash that point to the previous block. When a block is been tempated with, the hash will change, reason by being the calculation depend on what is located inside the block. The next block will be incoflict with the previous block not having matching hashes. The system will then render this chain of block broken. How does the system make sure it instills trust among its users and prevents any manipulation of data?. They are to security measures in place within a blockchain, that is a P2P netwok and Consensus algorithm which prevents any form of data manipulation.

2.1 Consensus Algorithm

They are different types of consensus algorithms that are being applied to the blockchain. The POW(Power-of-work) is the algorithm utilized in bitcoin. Its main purpose is to dispense accounting rights and compensations using the hashing power rivalry among the nodes. In light of the data of the previous block, the various nodes ascertain the particular arrangement of a mathematical issue. It is hard to find the mathematical problem. The principal node that tackles this numerical question can make the following obstruct and get a specific measure of bitcoin reward. Satoshi Nakamoto utilized HashCash to plan this arithmetic issue in bitcoin (Mingxiao, et al., 2017).

Another consensus algorithm is called PoS(Proof-of-stake). This algorithm aims to supplant the method of accomplishing the consensus within a distributed system, rather that solving the PoW. The node which produces a block needs to give a evidence that it approaches a specific measure of coins previously being acknowledged by the network. Creating a block includes sending coins to oneself, which demonstrates the proprietorship. The required measure of coins is indicated by the network through a trouble alteration measure like power-of-work that guarantees a surmised, steady block time (Vasin, 2014). The creation of a block circle through transaction fees will be rewarded. The underlying dissemination of currency is normally acquired through a time of power-of-work mining.

The last consensus algorithm I am going to discuss, found in blockchain is called the Delegated Proof of Stake(DPOS). In the first stage of design the creator of the online currency (Satoshi Nakomoto) hoped all the mining taking place to be conducted by the CPU by all participants. The hashing force can coordinate the nodes and every node has the chance to take an interest in the decision making of the blockchain. With the advancement of innovation and the valuation for bitcoin, the machines that are uniquely intended for mining are created. The hashing power is assembled in the members that have huge numbers of mining machines. The standard miner seldom have the chance to make a block.

Blockchain with DPoS, every node can choose the witnesses dependent on its stake. Within the entire network, the top number of witnesses that have partaken in the mission and got the most votes have the bookkeeping right. The number of witnesses is characterized with the end goal that at any rate half of casting a ballot partners accept there is adequate decentralization. The chosen witnesses make new block individually as doled out and get rewards. The witnesses need to guarantee sufficient online time. On the off chance that an observer or a witness can not make its assigned block, the action of that block will be moved to the following block and the partners will decide in favor of another observer to supplant it. The blockchain utilizing DPoS is more effective and force sparing than PoW and PoS (Mingxiao, et al., 2017).

2.2 Peer-to-peer network(P2P Nework)

This technology does not involve the central authouroties, but make use of the peer-to-peer network whereby it involves everyone in validatiing the the data. An identical copy of the ledger of transactions is sent to everyone on the network. Similary when an individual creates a block, that gets to be sent to everyone on the network. The individuals within the network gets to verify the block and check for proof-of-work. This process allows the creation of consensus through mass agreement of what the blockchain consist of and also what is not in the blockchain. By doing so, it create an impossible environment for an individual to try and cheat the system. These two factors, consensus and peer-to-peer network are what makes blockchain technology to be secured.

3. Advantages of Blockchain technology

One of the advantages I have highlighted earlier, the Blockchain innovation is decentralized system and it is the primary advantage of this innovation. With this system it is not important to work with the third-party organization It implies that the system works without mediator and all members of this Blockchain make the choices. Every system has the information base and it is critical to secure this information base, since when system is working with the third party, there is a hacking danger of the information base or on the other hand the information may turn up in an inappropriate hands. The cycle of the information base security may take a ton of time and may spend a great deal of cash. In the event that utilization the Blockchain innovation can be evaded, since the exchanges of the Blockchain have own verification of legitimacy and approval to uphold the imperatives. Furthermore, it implies that the exchanges can be confirmed and prepared independently (Golosova & Romanovs, 2018).

Each activity is recorded to the Blockchain and the information of records are accessible to each member of this Blockchain and cannot be changed or erased. The results of this account give the Blockchain's transparency, unchanging nature, and trusty. The transparency of the Blockchain is accomplished on the transactions duplicating process. As it was composed over, every exchange is replicated to either computer in the Blockchain network. Each member can look all transaction, additionally it implies, that each activity is appeared to members of the Blockchain. No one cannot do anything insensibly (Golosova & Romanovs, 2018).

Another advantage of blockchain technology is the time it takes to process data or information. Customarily, the transactions take a ton of time in handling and initialing into banking systems. The utilizing of the Blockchain innovation assists with the decrease of time it takes to process and handles data. Commonly with the centralized systems it takes from around 3 days, but with this technology it takes a few minutes or even second.

3.1 Disadvantage of Blockchain technology

The primary disadvantage of the Blockchain is the high energy consumption. to keep a real-time record the utilization of power is required. Each time the new node is made and in a similar time it speaks with each and other node. Along these lines the transparency is made. Miners within the network are trying to solve a ton of solutions for every second to verify transactions which in return they are utilizing a lot of computer power (Golosova & Romanovs, 2018). The next problem it involves the splitting of the chain. Nodes functioning on an outdated software disallow transactions in the new chain.

4. The evolution into smart contracts

In simple terms smart contracts can be referred to contracts in the real world where an agreement between parties which is enforced by the law, except they are a code that the computer can understand (digital). These contracts are store inside a blockchain, automatically they inherit all the properties of a block. Since they inherit properties, which means they are also immutable and distributed. They are accessible to everyone, can interact with these contracts, they is consensus that is tamper proof and automatically executes itself (Cong & He, 2019). The smart contract can send, receive, and interact with other contracts.

Most of the legitimate agreements drafted today use customized layouts containing normalized lawful languages which accommodate different terms and conditions. These agreements generally depend on the third-party for their execution and implementation. This cycle is excess and tedious, also costly, and unpredictable. This can be bypassed through brilliant agreements which contain a code that is equipped for executing the terms and conditions. The agreement code characterizes the terms and conditions as a lot of arguments in a manner like that of an authoritative document (Wang, et al., 2019).

Governance, deployment, risk management these are potential dangers that can be developed using evolving smart contracts. A governance system will need to execute and operate blockchain as a lawful application and necessities to consider oversight and observing functions, rule setting, and acknowledgment and change control management. When all is said and done, governance will be a necessity for lawful as well as for all advancements that oversee data. This change to some common guidelines for data administration is not just basic to blockchain yet to different interests like network safety. Governance norms around the blockchain will inevitably add to showcase trust in the innovation, the lawful and administrative condition. This will quicken the reception and accomplishment of the smart contract.

The existence of smart contracts it is not immune to risks and challenges just to name a few, the performance potential and computer assets needed to approve, measure, and identify misrepresentation will be a deciding element for appropriateness of smart contracts to different administrations. Example, banking, money related and installment administrations. In its present structure, blockchain is not equipped for taking care of thousands of exchanges with a similar degree of proficiency that does not forfeit on the security and decentralization parts of it. Another challenge, every node in the specific blockchain network must know about each transaction that happens all around the world, which may make a critical delay the network. The objective is to play out all transaction with higher productivity, yet in a way that does not forfeit the decentralization and security that the network gives (Wang, et al., 2019). If parties want to information to be private that will be difficult to preserve the contract and still attain the benefits of a blockchain.

5. Use of blockchain in industry

In healthcare Blockchain will change medical services and increment quality of care by empowering new biological systems and new business models to develop. Medical services data stored on a blockchain can change the way you store clinical data just as how you share data inside your organization, with medical services accomplices, payers and with patients. Blockchain decentralizes medical services data, expanding information accessibility, efficiency, transparency, and trust, likewise requires cautious planning to capitalize on the focal points it brings.

Travel and transportation industry have a lot of moving parts. Blockchain innovations can help everyone move in the safe, secure, productive and friction less ways for business success and consumer loyalty. Looking into the aircraft business' act of interlining. Numerous business-to-business transaction happen between booking operators, air transporters, Visa organizations and air terminals. The outcomes regularly lead to multifaceted nature, blunders, or disputes in transactions. In any case, when all parties utilize a similar information in a blockchain environment, regular data visibility and sharing can remove out irregularities.

Within the retail industry the customers confidence to shop online increases, as blockchain check and verify the legitimacy and safety of goods. Suppliers within the industry are guaranteed in meeting the consumer’s demand. With all this information stored in a blockchain, retailer can now have insights to what consumer prefers. In doing so will lead retailers promoting preferred products and in return earn loyalty from consumers.

Blockchain can easily replace two of these roles, evading transactions copies and enlisting and approving budgetary exercises. With blockchain it is anything but difficult to prevent, for instance, a customer from performing out numerous installments with a total amount that surpasses what they owe. All things considered; it is conceivable to wrongfully perform out this demonstration with customary cheques. In any case, it is difficult to accomplish this with blockchain as all money related activities must be confirmed before they are performed. Simultaneously, blockchain can go about as a safe library for the directed money related transactions. This vault cannot be altered by any substance required in the wake of being affixed to the chain. It can likewise be utilized to approve the directed transactions through collective checks and confirmations. These two highlights empower numerous monetary applications. for example, the digital currencies, stock trading, insurance marketplace and financial settlements (Al-Jaroodi & Mohamed, 2019).

In the logistic management industry, they are systems that help deal with the conveyance of crude material, items, and administrations between the producers or merchants and the customers. These would all be able to be important for a solitary organization or various organization and elements. Blockchain can offer ground-breaking help to empower these applications. One of the challenges in logistics is the inclusion on many organizations in the

activities. This may likewise incorporate various synchronized sub-exercises performed by various organizations, for example, industrial facilities, stockpiling organizations, transporting organizations, and consistency specialists. It is significant for any logistics the executive's application to give a lot of capacities to design, plan, arrange, screen, and approve the performed activities. Such capabilities can be effectively and safely upheld by blockchain. Utilizing the common disseminated records in blockchain to confirm, store and review logistics transactions will help lessen time delays, the management expenses, and human errors. Furthermore, applying smart contracts will encourage arrangements between the organizations in question and make restricting contracts quicker and with lower costs (Al-Jaroodi & Mohamed, 2019).

in the robotics industry, robotics has numerous potential modern applications including material transport and accuracy cultivating. In any case, there are numerous difficulties blocking such innovations from being basically evolved and utilized including self-governing abilities, decentralized controls, and community practices. As blockchain innovation can be utilized among various conveyed substances to agree without the requirement for a controlling power, it tends to be utilized in swarm robotics technology applications for a similar reason and to include security, independence, and adaptability highlights. This helps fabricate safer multitude mechanical technology applications that can-do better dynamic in a distributed way for productive activities.

Conclusion

What I have come to learn, is that blockchain technology goes further than money. The ability of this technology to allow a network to operate reliably without a central point of control, it is mind blowing. Blockchain decentralizes control which helps us shift society from which has limited room at the top, to a web with more access to opportunity and more consensus to what is valuable. With the emerging of this technology, one could say it is the solutions to almost every problem. Given time for this technology to grow, with what I have read and came to understand I believe blockchain technology has great potential to change the way in which this world has be functioning for so long and make it a better place to live for everyone.

References

Al-Jaroodi, J. & Mohamed, N., 2019. Blockchain in Industries: A Survey. *IEEE Access,* Volume 7, pp. 36500 - 36515.

Beck, R., Avital, M., Rossi, M. & Thatcher, J. B., 2017. *Springer.* [Online]
Available at: https://link.springer.com/content/pdf/10.1007/s12599-017-0505-1.pdf
[Accessed 10 09 2020].

Cong, L. W. & He, Z., 2019. Blockchain Disruption and Smart Contracts. *The Review of Financial Studies,* 04 04, 32(5), pp. 1754-1797.

Frankenfield, J., 2020. *Investopedia.* [Online]
Available at: https://www.investopedia.com/news/cryptographic-hash-functions/
[Accessed 10 09 2020].

Golosova, J. & Romanovs, A., 2018. *ResearchGate.* [Online]
Available at:
https://www.researchgate.net/publication/330028734_The_Advantages_and_Disadvantages_of_the_Blockchain_Technology
[Accessed 11 09 2020].

Mingxiao, D. et al., 2017. *IEEE Xplore.* [Online]
Available at:
https://ieeexplore.ieee.org/abstract/document/8123011?casa_token=ez1hW84hjF0AAAAA:SIuZM-BQb-WphY8Qhj5Ky837upeR-W-AQACOxoQou5Wb1YclrL8qgnGb6soVOX8Z7qdgBtA
[Accessed 10 09 2020].

Oldenbourg, D. G., 2018. Application of blockchain technology. *it - Information Technology,* 60(5-6), pp. 249-251.

Trade Finance Global, 2020. *tradefinanceglobal.* [Online]
Available at: https://www.tradefinanceglobal.com/blockchain/history-of-blockchain/#:~:text=Blockchain%20began%20with%20a%20man,as%20a%20medium%20of%20exchange.
[Accessed 10 09 2020].

Vasin, P., 2014. *BlackCoin.* [Online]
Available at: http://bitpaper.info/serve/AMIfv96zY1Qy1kHDkKj-0P5_SZMG5ffHm8EyOVwBzPTtqbINPo-R3femZWkzk08i-ISg5ZgACMrdCMHH-jovVKeXoXlrSy-zF7NZt7NMWRpT-gmWDrW-Qz6NdOUdmOvYLXOreooL3-YK8mf6rYFHGQR6Vn5aFwZSAm625XNYpjoCc0OuuIMzCsc.pdf
[Accessed 11 09 2020].

Wang, S. et al., 2019. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems ,* 49(11), pp. 2266 - 2277.