Understanding Blockchain Technology

Kubeka Benedict Sizwe[1][217010763]

[1] University Of Johannesburg, Johannesburg, South Africa

Abstract. This research paper looks at how blockchain technology works at its core and looking at the blockchain systems present in our current society from permissioned which is seen as a private blockchain network technlogy, to permissionless viewed as a public blockchain technology. The paper further expresses the growth of blockchain technology from its roots in history to the modern-day. I will examine the central goal of its security feature and it's agility to be distributed forming a modular design. Smart contracts will be addressed, focusing on how they strengthened and how they function in everyday life and what we associate other mechanisms with smart contracts. I then look at how this technology has affect industries across the globe, indulging in the advantages of blockchain.

Keywords: Blockchain, Smart Contracts, technology, network,seystems, permissioned, permissionless.

1 Introduction

Blockchain grew out of a need to create digital trust where we had lost trust in institutions(Shrier, 2020) Blockchain has been a strengthening technology over the years, and the nature that drives the technology is it being digitally tamper-proof and its security adherent. Mainstream introduction into blockchain was introduced by, bitcoin a cryptocurrency. Since the introduction of the first Cryptocurrency (i.e. Bitcoin), Blockchain has been known as the underlying core technology for Cryptocurrency(Hossein Hassani, Xu Huang and Emmanuel Sirimal Silva, 2019).Before bitcoin, there was a similar blockchain concept (which Bitcoin advanced from) in the year 1991, when Stuart Haber and W. Scott Stornetta, research scientists worked on the first secure chain of blocks. The following year 1992, there was an advancement from this technology's design introducing Merkle trees, which efficiently stored manifolds of record.

In the early 2000s, there was another advancement of this technology, with the concept of decentralization of trust in the network file system brought forward by David Mazieres and Dennis Shasha. As the years progressed a figure by the name Nick Szabo, around the year 2005 proposed decentralized property names with the use of a protocol using a system like a blockchain, with features like timestamps and Proof-Of-Work this protocol was titled BitGold. The disadvantage with BitGold was that it introduced the double-spending problem, where a User could spend their coins twice.

When it was 2008, a paper called Bitcoin was first introduced by Satoshi Nakamoto(a person or group), as a peer-to-peer electronic Cash System using the foundation laid by Haber, Stornetta, Mazieres, and Szabo. The following year In 2009, Nakamoto's idea of a peer-to-network came into existence with the aid of several Computer Scientists like Hal Finney, who played a huge role in the development of the very first Bitcoin technology introducing a system called Reusable-Proof-Of-Work which solved the double-spending problem.

In 2013 a programmer by the name Vitalik Buterun, created a new blockchain-based platform called Ethereum which uses smart contracts, which is a scripting function that I will discuss in more details at a later stage. Over the years the technology became famous to the current time, where its viewed as a secure form of payment. In 2014, blockchain technology gained a lot of attention from the industry due to its security features which.

Blockchain is a system of records to transact value (not just money!) in a peer-to-peer fashion(Bikramaditya Singhal, Gautam Dhameja and Priyansu Sekhar Panda, 2018) In simple terms A blockchain is a distributed ledger, open to anyone, protected using cryptography. The structure of it is one like linked lists. A linked list, in its simplest form, is a collection of nodes that collectively form a linear sequence (Goodrich, Tamassia, & Goldwasser, 2014)
where data is stored in a container referred to as 'a block'. The content of the block is composed of a unique encrypted value (generated by complex cryptography algorithms) of that block and the encrypted value of the previous block. The encrypted value of a block can be defined as the identity of the block due to its uniqueness; an example could be the ID number of everyone in South Africa, it's never the same even for twins. The definition of the data stored in the block is subject to a blockchain.

People throughout the decades have been performing transactions and recording them in a ledger which is a collection of records. Blockchain technology has made use of this concept, by keeping a record of each transaction, as there are time-stamped and immutable, meaning they are temper-resistance but can be reversed. By 2013, several proposals and companies were promoting the idea of using blockchain technology without a digital currency underpinning it. In these 'permissioned blockchains' only preapproved members may commit data to the blockchain, which exists as a shared ledger between all participating parties(Ammous, 2016) In a permissionless blockchain, Any user can join a public blockchain network, but their transaction is visible to other users on that network, this poses security concerns for groups such as organizations as they need to prevent unauthorized access to transactional data when transacting with other businesses. That's where a Permissioned blockchain comes into action, where only a few users have access to the private network and is usually used by a selective few organizations, granted access by an individual entity.

2 The Workings of Blockchain

Bitcoin completed the transformation by creating a single, universally accessible digital ledger, called a blockchain. It's called a chain because changes can be made only by adding new information to the end(Peck,2017). Blockchain results from the block's character, by going back to the structure of linked lists, looking at a single block whereby it has a direct link to the previous block's encrypted value, this then allows some linking between the blocks forming a 'chain.' In a typical block-chain, Like a link List The starting block(of index 0) doesn't have a reference to the previous block, so the encrypted value(for the previous block) would be, for example, 00, and its encrypted value would be '1AZY'. The next block of index 1 would have previous encrypted value of '1AZY', and its encrypted value would be '2Q1P'. The third block in the list at index 2, has a previous encrypted form of '2Q1P', and its encrypted value of 'B3AR' the figure below shows a visual representation.

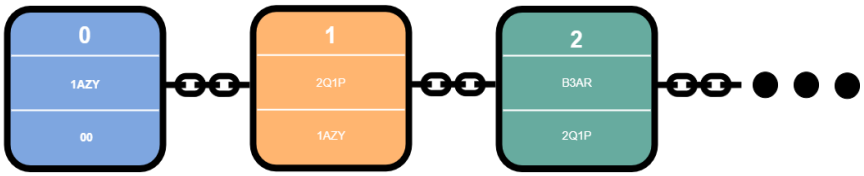

Fig. 1. A basic structure illustrating a blockchain.

2.1 Consensus & Security

When looking at different blockchain networks, A well know mechanism used in cryptocurrencies is proof-of-work. Individuals solve complex cryptographic algorithms to allow transactions, we'll look at how this happens later when looking uses of blockchain in the industry.

In a closed blockchain network which is defined as permission, the mechanism used is selective endorsement, the users or organizations involved with a particular transaction, can allow the transaction. This mechanism is faster than proof-of-work and has a modular design.

Encryption. One of the fundamentals of encryption is how many characters go into making the 'key' that is used to 'lock' and 'unlock' – encrypt and decrypt – the data(Shrier, 2020) .If the identity of a block is changed or altered the block following, that will no longer have a reference to the previous making it invalid, resulting in the following blocks invalid. Using Encryption alone does not enforce the best security, with an obstruction, alteration can occur with the use of IoT, all the invalid encryptions can be reconfigured and retrieved resulting in them valid again. Proof-of-work (Used in cryptocurrencies like bitcoin), decreases the rate at which each block is created, resulting in more time required to create a block and is cost consuming to. This feature

of blockchain adds on to the encryption function as a reliability feature, by adding more time required to decrypt a block when it's altered.

Distribution. The traditional approach was that there would be a centralized entity that would maintain just one transaction/modification history(Bikramaditya Singhal, Gautam Dhameja and Priyansu Sekhar Panda, 2018). A blockchain uses a Peer to peer network as another security feature, making it a decentralized system as it distributes resources. For instance, If I create a new block, it's distributed to each node within a network, the nodes individually check if it hasn't been altered and then adds it to their blockchain. This then creates a general agreement amongst the nodes in that network, regarding the characteristics of the block, such as if it has been altered or not, and if it is indeed, then the nodes within that network won't accept it as it's invalid. In an instance where a block is altered by a hacker hoping to get data stored in that block's chain, For them to succeeded in their mission, all the blocks must be obstructed, do the proof-of-work of each block and gain control of at least more than half of the network, and only then the nodes on the network can accept the compromised blocks.

3 Smart Contracts

A Smart Contract is not a written contract on paper of the traditional kind, nor is it simply an online contract. It is described as "smart" because it can do more than both of these paradigms(Corrales, Fenwick and Haapio, 2019) In simple terms smart contracts, are scripts or programs stored on the blockchain, with automated execution based on conditions. These programs are deployed and executed on the Ethereum platform, and are written and compiled into byte code, and executed on the Ethereum Virtual Machine which is essentially a decentralized Turing-complete virtual machine. These smart contracts came with the second generation of blockchain technology as innovative technologies. In an effort to meet the objective, the core innovation of Ethereum was the Ethereum Virtual Machine (EVM)(Bikramaditya Singhal, Gautam Dhameja and Priyansu Sekhar Panda, 2018)

Blockchain can be used as a medium for these collusive agreements, or even be the subject of an agreement in itself, depending on the conditions of entry, use, and exit from the technology(Schrepel,2019). A contract in general is a binding between two entities, with certain conditions agreed upon, enforced by the law. In our society there are multiple contract agreements, enforced by law and curated by banks, insurance companies all dependent on the type of contract agreement. It is similar with smart contracts just that it does not require the third party to curate or enforce the law, since it is enforced by the program itself. This adds on the feature of a decentralized system in blockchain technology as the smart contracts form modular design across nodes as it distributes them, this allows users to create their own agreement and its managed by the program. Transactions between entities are then possible removing the reliance of third parties, when executed the entities involved in the contract require no engagement.

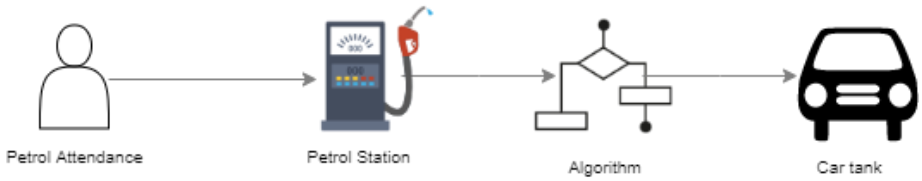

Fig. 2. An illustration of a contract between, a petrol attendance and a petrol station.

For this example, In fig. 2 above, the petrol attendants specifies the amount of petrol to be released to input on a keypad a certain amount of money like 500,00 ZAR, the petrol station then takes this input, and converts it to the equivalent amount of petrol to be released automatically using its algorithm and is poured to the car tank. This set of instructions will execute in any given case. There's no point whereby the petrol station will feel like not complying with the contract throughout its functionality.

This expresses how immutable the contract on a blockchain is, as it cannot be changed, this is a significant feature for security. The code governs how a particular contract acts, no government or entity can alter it.

There is a vast range of advantages associated with the use of smart contracts, such as them being incorruptible, and code being automatically executed. Another advantage is that there are less time-consuming resources since the whole process is fully automated, and there's a reduction of costs accompanied by managing them, making them efficient and execute optimally. Since the entire system of blockchain technology is decentralized, it is bound for smart contracts to have an advantage of Independency.

There exists room for uncertainty from the automated execution nature of smart contracts, the conditions of input data set for them are usually formal and thus leave less room for multiple resultants, whereby the rules may need to be altered due to unforeseen conditions presented at that moment.

3.1 Oracles

Oracles are an important component of the smart contract ecosystem (Bashir, 2018) Usually provided by external third-party entities outside the blockchain network and consensus, we can define an oracle as a data provider, used by smart contracts on the blockchain network. Smart contracts act upon certain conditions meeting satisfactory using input data, so if the data inputted is not enough or is false the overall processing of the smart contracts won't be good, and resultants will be as inefficient. This is where oracles come in handy, they assist by triggering the executing of smart contracts if certain pre-defined conditions are met. This reveals how Oracles give data to the blockchain to be utilized by smart contracts.

4 Role of blockchain Technology in industry

Due to its complex security, this technology is widely used around the world in many industries. Let's look at the role blockchain systems have played in industry.

4.1 Business Sector

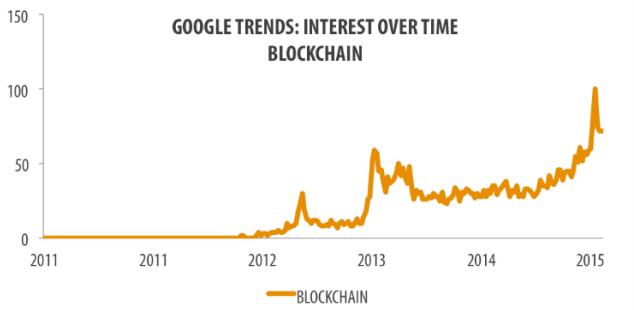

Fig. 3. Growth of blockchain (Anz.com, 2020)

There plenty of advancement made by blockchain in industries today, and its forever growing daily. In South Africa, A company with efforts of assisting and dealing with current issues like animal poaching which affects the country's wildlife has devised a system alongside with tech giant IBM. This system titled is StudEx, which uses blockchain technology and the IoT to verify ownership of animals, by tracking animal's characteristics such as heart rate, making it difficult to get animals. Which is also an investment platform.

Create smarter, more efficient supply chains, reduce fraud, verify transactions more quickly, and create disruptive new business models with Azure blockchain services(Microsoft.com, 2019) Introduced by Tech giant Microsoft, Ethereum technology, which works with Azure a cloud computing service provided by Microsoft, allowing developers using Microsoft services to integrate blockchain technologies into their projects. A company based in the USA called chronicled is shaping the way blockchain can be used in logistics with the use of IoT by cutting out the middle as it can add on occurring costs for a logistics company. Their system specifies the authentication of each product's origin, which adds as an advantage in the transportation of a product, preventing the exchanging of a product with wrong or a faulty one, throughout the whole transporting process.

4.2 Financial Sector

Financial services has been at the epicentre of blockchain experimentation and, increasingly, blockchain deployments. (Shrier, 2020) With the rise of the fourth industrial revolution, came about many ways of banking such as using cryptocurrencies, which are

virtual currencies' that are digital. Before we can examine its uses in finance, we first must look at how these cryptocurrencies function on block chain technology. There is a wide range of cryptocurrencies in the market today, from Litecoin, Ethereum, Tezos, XRP, and the first to use this blockchain technology, bitcoin. Bitcoin is the first application of blockchain technology(Bashir, 2018)

Besides the complex encryption security feature, these currencies have vast benefits one of which is that they cannot be counterfeited as its exclusive, digital and decentralized. As seen earlier in Fig.1, we have an overview of how a typical bitcoin transaction can be processed, where at block 0, data stored would be the specific transaction details between a sender and a receiver.

Users executing transactions on the bitcoin network have access to a public key and private key, a public key is a well-known address within the bitcoin network, and a private key is an address known by a specific user only and not everyone on the network. The details of a transaction contain the amounts of bitcoins being sent/received and the addresses of the sender and receiver, all of this is encrypted using the sender's private key as identification of the source via a hashing algorithm known as SHA256. It then transfers using the receivers public key, allowing the transaction to be restricted to the receiver and only decrypted by their private key. We refer users who verify these occurring transactions to as miners and earn as they mine, they add the verified block to the chain, and this process is called mining. This has increased demand in semiconductors over the years, as the need for faster problem-solving computers rises.

In the banking sector, there's been a huge interest in blockchain, technology, In Italy, most of the banks use a blockchain system called Corda, whereas in before there were physical transactions between the banks in efforts to reintegrate transfers between these banks, and this process could take up to, months cause they were using physical drives. With the aid of this new system, Corda they could speed up the overall process that took months now could happen within a day.

Blockchain technology has paved the way for introducing decentralized finance, allowing anyone with a smartphone to have access to banking services without the need of signing a contract or speaking to any bank consultant. Decentralized applications work by depositing funds into your app, and thereafter it's automatically converted to a cryptocurrency of your choice, depending on the volatility of the digital currency it'll either appreciate or depreciate, thus earning you interest, if volatility is low. Decentralized apps are built on Ethereum, using smart contracts. Under the strong challenges from Cryptocurrency and construction of decentralized market infrastructures, banks have been embracing FinTech innovations and are closely cooperating with FinTech companies to stabilize their essential role in the financial market.(Hossein Hassani, Xu Huang and Emmanuel Sirimal Silva, 2019)

5 Conclusion

It is now clear, how blockchain technology works alongside its systematic integration, from when it was just an idea on paper to a full-on working ecosystem. Blockchain technology provides many ways of providing a service for the people and not having one central owner of that service. Like any service, it is a reliance on its users, without us using this blockchain technology it might as well be useless.

The security features discussed helps this blocking technology keep a market competitive edge than any other service. It is interesting to see blockchain will continue to make life easier as a technology, reaching and touching every industry as we emerge out of the current fourth industrial revolution.

References

1. Goodrich, M. T., Tamassia, R., & Goldwasser, M. H. (2014). *Data structures & algorithms in java 6Th Edition*. New Jersey, Estados Unidos: John Wiley & Sons, Inc.

2. Shrier, D.L, 2020. *Basic Blockchain: what it is and how it will change the way we work and live* Great Britan: Robinson, p.20,p.33.

3. Anz.com. (2020). [online] Available at: https://bluenotes.anz.com/media/402955/googletrends-blockchain.png [Accessed 01 Aug. 2020].

4. Hossein Hassani, Xu Huang and Emmanuel Sirimal Silva (2019). *Fusing big data, blockchain and cryptocurrency : their individual and combined importance in the digital economy*. Cham: Palgrave Macmillan.

5. Bikramaditya Singhal, Gautam Dhameja and Priyansu Sekhar Panda (2018). *Beginning Blockchain : a beginner's guide to building Blockchain solutions*. New York: Apress.

6. Ammous, S. (2016). Blockchain Technology: What is it Good for? [online] papers.ssrn.com. Available at: https://ssrn.com/abstract=2832751 [Accessed 03 Aug. 2020].

7. Peck, M. E. (no date) '*Blockchains: How they work and why they'll change the world*', IEEE Spectrum, 54(10), pp. 26–35. doi: 10.1109/MSPEC.2017.8048836.

8. Schrepel, T. (2019) '*Collusion by Blockchain and Smart Contracts*', Harvard Journal of Law & Technology, 33(1), pp. 117–166. Available at: https://0-search-ebscohost-com.ujlink.uj.ac.za/login.aspx?direct=true&db=lgs&AN=142243758&site=eds-live&scope=site (Accessed: 04 August 2020)

9. Corrales, M., Fenwick, M. and Haapio, H. (2019). *Legal tech, smart contracts and blockchain*. Singapore: Springer.

10. Bashir, I. (2018). *Mastering blockchain : distributed ledger technology, decentralization, and smart contracts explained*. Birmingham - Mumbai Packt March.

11. Microsoft.com. (2019). Blockchain Technology and Applications | Microsoft Azure. [online] Available at: https://azure.microsoft.com/en-us/solutions/blockchain/ [Accessed 19 Aug. 2019].

12. Roets, A. (n.d.). Entering a different digital world with Tumelo Ramaphosa. [online] The Citizen. Available at: https://citizen.co.za/news/south-africa/1997333/entering-a-different-digital-world-with-tumelo-ramaphosa/ [Accessed 19 Aug. 2020].