Implications of Blockchain Technology

Ian Burke, Software Development, GMIT

***Abstract*—The term 'revolutionize' is being thrown around when it comes to Blockchain, the underlying technology of Bitcoin, a technology that has evolved beyond cryptocurrencies in recent years that offers potential capabilities such as smart contracts and decentralised applications that may or perhaps impact society and disrupt many industries in the future. Blockchain allows people to interact with each other whether it be exchanging digital currency or ownership of property by establishing trust without the involvement of a trusted intermediary in a secure manner using the highest level of cryptography. In this review, we will examine the functionality of blockchain and embark on the possibilities it can provide along with various obstacles it faces in the long run. Our conclusion is that blockchain shows great promise to businesses and society with decentralised applications, however it would take a considerable amount of time before we see the true power of the technology come into effect with many obstacles to overcome such as government regulation and adaptability of change for businesses.**

I. Introduction

Blockchain is the driving force behind the popular cryptocurrency Bitcoin which is a digital currency used for making transfers and payments on the internet. Basically, blockchain is a digital ledger that is distributed across a network of nodes, each node acquiring an updated copy of the ledger. The ledger contains a list of all transactions that have been executed on the network. Each transaction is verified and validated by consensus of multiple nodes on the network. In other words, the system maintains a self-audit trail [1]. The digital ledger is immutable. It can be updated by adding new sets of transactions but it cannot be changed, erased or mutated any further. Every transaction can be viewed on the public ledger, but the identity of participating parties behind every transaction is kept hidden. Blockchain uses a peer-to-peer network [2] meaning there is no central authority in control of the system. Therefore, creating a decentalised environment. E-commerce on the internet relies heavily on trusted intermediaries or third parties to process and mediate electronic transactions. This system is not ideal with growing problems like hacking, corruption and fraud. The whole security of the system is based on a trust model [2]. Blockchain allows parties to transact directly to each other without the involvement of a trusted intermediary or third party i.e. there is no middleman needed. This leads to fast, secure and cost effective transactions. The system is secured using the highest level of cryptography.

Since the emergence of Bitcoin, a lot of attention began to circulate around blockchain and the capabilities the technology can provide beyond cryptocurrencies. Blockchain is capable of disrupting industries like business and finance to state governance and giving empowerment to people in a decentralised fashion [3]. Blockchain applications such as distributed cloud storage, digital identity [4], digital voting and decentralised notary are currently being developed [5]. The introduction of smart contracts, another blockchain component, allow us to prove ownership of a digital property or any asset of value [6]. Physical assets such as a house, car or smartphone or non-physical assets such as company shares can be exchanged with smart contracts. Since the blockchain is a distributed ledger, it can also store a proof of existence of legal documents, health records, personal identity, notary i.e. document certification and private securities. A sense of anonymity and privacy can be achieved by storing the fingerprint of digital assets.

The paper is structured as follows: In section II, we will examine how blockchain works and the introduction of smart contracts. In section III, we will discuss the various possibilities of blockchain and how it can revolutionize the world. In the final section we will present our overall conclusion of the emerging technology.

II. How does it work

Blockchain was first introduced with Bitcoin to solve the double-spending problem [2]. A blockchain uses a peer-to-peer network which is comprised of interconnected nodes that share resources among each other without the use of a centralized administrator that controls the system i.e. a decentralised system. Instead of using a middleman to carry out a transaction, the Bitcoin blockchain uses cryptographic algorithms and protocols such as hashing and asymmetric private/public keys to secure and execute transactions [2]. For instance, a private key is used to create a digital signature for each transaction a user makes on the network. A digital signature is used to authenticate that the transaction belongs to the user and also prevents data corruption and manipulation from attackers. The private key is kept hidden while the public key is broadcast out to the network in which the receiver can obtain and use to carry out the transaction. Each transaction is broadcast to all nodes across the network and verified by a consensus i.e. majority of nodes agree on a transaction [2]. Basically the system is able to audit itself in a way.

Every ten minutes on the system, kind of like the heartbeat of the system, a block is created and within that block contains a set of transactions which are considered to have occurred within in the last ten minutes [5]. Once a block is validated through cryptographic proof-of-work, it is then

I. Burke is a student studying Software Development, Galway-Mayo Institute of Technology, Old Dublin Rd, Galway, Ireland e-mail: g00307742@gmit.ie

timestamped and giving a hash [7] i.e. a reference of the previous block. Each validated block is linked to each other like a chain in a linear chronological order, hence the name blockchain. This helps reduce the probability that a block will be generated more than once at a given time. Nodes that participate in generating proof-of-work are called miners [3]. The miners use their CPU power to solve these mathematical puzzles. Each miner competes with each other to complete the proof-of-work and add a newly mined block to the chain. The miner that solves the mathematical puzzle first is rewarded in cryptocurrency like Bitcoin [2]. Each block on the blockchain cannot be changed or manipulated without having to change the whole blockchain itself against the consensus of the majority of nodes. Transactions on the ledger can be seen publicly by anyone but information from both the sender and receiver is not linked to a particular transaction which makes them untraceable and anonymous by using a new key pair [2].

A. Security

If someone wanted to hack or attack nodes on the network to change or erase transactions, they would have to alter data in a block that contains the particular transactions. Each block is given a hash signature, which is generated by the miners, referencing the previous block. According to Bitcoin creator Satoshi Nakamoto in his original paper, ***"To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes"*** [2]. The attacker would also have to hack majority of nodes (over 50 percent) to agree on these changes. It would take enormous CPU power to hack over a million of distributed nodes simultaneously. The whole operation would take an excess amount of electricity to perform leading to high electricity costs for the attacker [6].

B. Smart Contracts

The concept of smart contracts was first introduced in 1994 by Nick Szabo [8]. The idea was never implemented until the emergence of the Bitcoin. According to Szabo, a smart contract is ***"a set of promises, specified in digital form, including protocols within which the parties perform on these promises"*** [8]. Basically, the terms and conditions of a contract can be written into code and embedded into software that can enforce them. Smart contracts do not necessarily have to be actual legal contracts but can also be programs that contain conditions which allows more interactions between parties if these conditions are met. They can be triggered by addressing an transaction to them [6].

Smart contracts can be programmed to ensure that all transactions adhere to the proposed agreements between participating parties and the records managed by blockchain are properly maintained with respect to the underlying agreements expressed by these records without the interaction by a third party [9]. Smart contracts can be paired with a blockchain to record changes of asset ownership under contract terms. A smart contract can act as a wrapper for any transaction that automatically executes the terms of a contract [1]. Government services can be improved efficiently and transparently with smart contracts via blockchain by automating laws and statutes. With a blockchain in place, systems can be resilient and operated on decentralised networks that do not depend on a central server which could lead to failure for the whole system. Blockchain systems can ensure accurate and identical records for contracting parties due to immutable and transparent system [5].

III. Possibilities with Blockchain

The Bitcoin blockchain is just one blockchain application. Another blockchain application is Ethereum, similar to Bitcoin but different in a way where it allows developers to use its blockchain as a platform to create decentralised applications [3]. Blockchain can be described as the next generation of the internet. Stock exchanges are currently experimenting with blockchain technology. Public companies can directly issue shares to investors via blockchain without the involvement of brokers. Shares can be purchased or sold directly through blockchain [5]. This would make stock trading more efficient and cost effective. Since the introduction of cloud computing, we have popular cloud storage services like Google Drive, Dropbox and One Drive that can store our documents, multimedia and any other files [5]. However, cloud storage services face many challenges in areas such as security, privacy and data control. We put our trust in these third parties over the handling of our personal files. Storj is a open source cloud storage project that is implementing blockchain technology to offer completely decentralised and encrypted cloud storage which will give users a sense of security and integrity [5]. Nonetheless, any person with spear disk storage could be become farmers on the site and host their own miniature data center to hold other peoples data in return for money. With the Internet of Things (IOT) becoming increasingly popular technology, there is still a centralised model being used on majority of IOT systems. In some situations, devices need to communicate and exchange data autonomously. Efforts have been made to implement decentralised systems to bring a level of security and trust for the exchange of data. Blockchain can keep record of messages and data exchanged between devices on IOT platforms. IBM and Samsung have teamed up to develop a Autonomous Decentralised Peer-to-Peer Telemetry (ADEPT) platform that uses blockchain components to establish decentralised IOT [5]. BitTorrent's file sharing, smart contracts and TeleHash (peer-to-peer messaging) are protocols being used to develop the platform [5]. Governments and large corporations control majority of DNS servers which can lead to censorship being enforced on users. Namecoin is an open sourced blockchain technology that implements decentralised version of DNS [5]. This lets every user to have the same DNS phone book data on their computers. Digital voting is another concept with blockchain technology where an election that implements a blockchain can prevent hackers from rigging the election with encrypted and immutable votes. This would also cut election costs for the government. Digital identity is a way in which people can store their personal records on the blockchain such as passports, birth certificates, health records, licenses, passwords and many more [9].

IV. Obstacles of Blockchain Technology

Blockchain shows great potential with a wide range of applications that can improve and benefit a number of sectors in various industries. However, with rapid innovation and change comes resistance. It is in people's behaviour to resist change. Blockchain technology brings a number of changes and disruption to businesses, governance and society [3]. One of these disruptions is the removal of trusted intermediaries and third parties like financial institutions. Customers will have to trust that their electronic transactions are safe, secured and completed. Government and politics may slow down the blockchain implementation by bringing in new laws and regulations due to such disruptions. It would take at least a decade or so before blockchain technology will take effect [10]. Blockchain offers anonymity which gives criminals an advantage to launder money, purchase weapons or buy illegal products online using cryptocurrencies like Bitcoin without being traced. This makes it very difficult for law enforcement to stamp down on criminal activity. With Future advancement of quantum computing, cryptographic keys may be easier to crack. Nonetheless, this argument is only valid until the hash keys become bigger and even more stronger. Mining in the Bitcoin blockchain is said to use massive amounts of electricity to keep the mining process going on a daily basis. Not only would it result in high electricity costs but it may create a carbon footprint if we take climate change into consideration [9].

V. Conclusion

In this review, we have briefly examined blockchain technology as a digital ledger that is distributed across a peer-to-peer network which enables people to establish trust without the involvement of a intermediary or third party. The whole system is decentralised with no central authority or single entity controlling the network. We have looked at how a blockchain works under the hood and then discussed the potential possibilities the technology can bring in the future along with obstacles it will face. With the vast capabilities of blockchain like immutability, transparency, security and smart contracts, we believe that this holds vast promise for every business, every society and people individually around the world. Overall, blockchain gives us a sense of hope when it comes to the concerns over privacy and trust when dealing with valuable assets. However, it will take some considerable amount of time, perhaps a decade or so, before we see the true potential of blockchain technology being implemented in many industries as with change comes resistance and such resistance would be government regulation.

References

[1] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges." *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.

[4] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[5] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[7] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in *Conference on the Theory and Application of Cryptography*. Springer, 1990, pp. 437–455.

[8] N. Szabo, "Smart contracts: building blocks for digital markets," *URL: http://www. alamut. com/subj/economics/nick_szabo/smartContracts. html (Letzter Abruf vom 31.10. 2016)*, 1996.

[9] J. Umeh, "Blockchain double bubble or double trouble?" *ITNOW*, vol. 58, no. 1, pp. 58–61, 2016.

[10] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.