An Overview of Blockchain Applications and Attacks

Rahul Rao Vokerla[1], Bharanidharan Shanmugam[1], Sami Azam[1], Asif Karim[1], Friso De Boer[1], Mirjam Jonkman[1], Fahad Faisal[2]
rahul.vokerla@students.cdu.edu.au, {bharanidharan.shanmugam, sami.azam, asif.karim, friso.deboer, miriam.jonkman}@cdu.edu.au, fahad.cse@diu.edu.bd
[1] College of Engineering, IT and Environment, Charles Darwin University, NT, Australia
[2] Department of Computer Science and Engineering Daffodil International University, Bangladesh

Pre-print

***Abstract*—** In recent decades, Information Technology has contributed fundamentally to the development of financial markets, reforming the way in which financial institutions interact with each other. However, the established practices and norms of this sector may face an all-out overhaul as remarkable innovations such as Blockchain are maturing. The essence of Blockchain is that it is a public, shared and carefully designed record that allows mutually unknown individuals and institutions to share data in a reliable ledger and carry out all kinds of transactions. This ground-breaking technology is developed from cryptography and peer-to-peer network technologies. It is nearly immune to the majority of today's digital threats. Besides financial institutions, Blockchain based solutions have made it into other industries such as real estate, health care, the media as well as Government bodies. This paper will explain how Blockchain works, what it really is, types, its applications and threats and will offer a few ideas for prospective expansion of this technology.

***Keywords*—** *Blockchain attacks, Bitcoin, Public ledger, Distributed ledger technology, Double spending*

I. Introduction

Stuart Haber and W. Scott Stornetta first described Blockchains in early nineties [1]. Based on subsequent development in this area, Satoshi Nakamoto first conceptualized Blockchain in 2008, through the digital cryptocurrency known as Bitcoin. Other cryptocurrencies have also made it into circulation. Since the concept of Blockchain is still quite new, there are not many review papers yet; and as such this paper aims to fill the void.

Blockchain is a chain of blocks in which the information of transactions is registered and maintained in a distributed public ledger across a number of computers that are linked in a peer-to-peer network. There are a set of rules for confirmation of the legitimacy of a block and to verify that block has not been altered maliciously. The algorithms and the computational frameworks for creating, inserting, and utilizing the blocks are incorporated into today's Blockchain Technology [2].

This technology solved the problem of *Double-spending* (explained in more detail later) as the second transaction would be recognised as invalid. Blockchain uses public key cryptography, where every client is assigned a private key, and the respective public key is shared. By design, productivity is one of main concerns for Blockchain. Blockchain requires an exceptionally strict verification procedure to record a transaction, which leads to a delay due to the time necessary to conform and requires extensive use of resources.

At present, it takes around 10 minutes for a transaction to be confirmed. Many nodes are required to register and carry out such confirmation activities. These issues have limited the extent of Blockchain applications. For instance, current Blockchain strategies are by and large not feasible for the Internet of Things (IoT) network, because IoT devices often need to work with low computational power. Blockchain technology is still in an early stage of development. Further research in this field is needed to improve its efficiency.

II Building Blocks Of Blockchain

A. Public key cryptography

Public key cryptography is a crucial part of Blockchain structure and is utilized to guarantee the integrity of the messages and transactions incorporated with the blocks. The Blockchain convention utilizes what is known as the *Elliptic Curve Digital Signature Algorithm (ECDSA)* to make an arrangement of private keys and a related public key. The public key is used with the hash function to create a general address which is used by the public to carry out the transactions. The private key is kept secret and is utilized to sign a digital exchange to ensure exchange is genuine.

B. Digital Signature

Digital signatures are essentially like a signature on the document. These guarantee that the creator of an exchange indeed is the person who holds the private key. Digital signature is a key factor for Blockchain transaction; a sort of backbone for the transactions. Every transaction has a different digital signature which relies on the private key of the user. Additionally, given the message, the public key of the client and the signature, it is non-trivial to check if the signature is legitimate. Once the owner signs the exchange, the exchange is sent to the memory pool where it waits to be handled by the miners. The miner utilizes the sender's public key to guarantee that the digital signature is authentic which renders a hacker incapable of spending clients' assets without their consent. Once the ownership and digital signature is verified, the transaction is added to the next block and the money is exchanged from one wallet to another.

C. Peer-to-peer Network

Peer-to-peer (P2P) network is a fundamental part of how Blockchain technology works and is one for the reasons for its solid security [17].

In a P2P network, the client not only employs the system for his or her own purpose, but simultaneously also provides the overall system with the air it needs for satisfactory functioning. Each 'Peer', often denoted as 'Node', a computing device, lends resources from its own capacity;

such as network bandwidth, disk storage or processing power, to the other participants or miners without a centrally coordinating server. All nodes are considered equal in a P2P network, but each node can take different roles at different times [18]. The identity and other private information of the participants usually remain encoded, safeguarding the participants' privacy.

III Blockchain Technology

A. Blockchain Technology

As mentioned before Blockchain contains its records in a distributed ledger which is visible to anyone in the network. Once the data is recorded in Blockchain it is quite hard to alter it. What data is stored in a block depends on the type of Blockchain. In case of Bitcoin, it stores the transaction information as a set, encompassing information regarding the sender, the receiver and the amount transferred. Each Block has a unique hash value, which can be compared to a fingerprint. When a block is created, its hash value is calculated simultaneously, and any changes of the information in that block will change the corresponding hash value.

Genesis Block: The first block created is called *Genesis Block*. It contains data and a unique hash value. In a chain of blocks all blocks except the Genesis block will use the hash of previous block to create its own hash value, along with a timestamp and the transactional data. For instance, when someone tampers block 2 in a chain of 5 blocks, the hash value of block 2 changes which this renders all the following blocks invalid because they no longer store valid hash values. The secure hashing algorithm-256 (SHA-256) is used to hash the blocks.

Miners will add new blocks to the chain whenever this is necessary or whenever a transaction is executed. When a new block is added to the chain, it is sent to everyone in the network and each node will check the block to verufy its authenticity. Blocks tampered with will be rejected by other nodes in the network. To successfully tamper a block, the attacker has to carry out a series of tasks including completing the whole proof-of-work and taking control of more than 50% of nodes in the network to make the tampered block acceptable in the peer-to-peer network. Needless to say, achieving these tasks are not only difficult, but also extremely time consuming.

B. Types of Blockchain

At present ther are three classes of Blockchain in use,.These are:

- *Private Blockchain*: Access to such Blockchains is tightly controlled. No one can join as a participant or a validator (who is able to perform transaction validation tasks) without the consent of the network administrator. Private companies may operate private Blockchains as an organization may not want public interaction on blocks containing sensitive company information.
- *Public Blockchain*: Contrary to private Blockchain, any momber of the public with an internet connection may join a public Blockchain network and carry out transactions and validations.
- *Consortium Blockchain*: Most often consortium Blockchains are semi-decentralized. Instead of one organization controlling access to it, multiple companies may take part in its operation and access control protocols.

C. How Miners work in Blockchain Technology

This section will discuss how a block is added in bitcoin Blockchain. Blockchain uses the concept of link-list based information structures which store transaction history of the whole system in blocks. In each block, the transactions are stored using *Merkle Tree*. A moderately secure time-stamp and a hash of the previous block is also stored. [3].

To effectively include a new block in the Blockchain, the miners need to confirm (mine) a block by performing a computationally difficult *Proof of Work* (PoW) puzzle. Tampering a block is not practicable, as it would change the hash of the block. The subsequent blocks would need to change in turn because each block in the network contains a hash value that is created by taking the hash of the previous block as an input.

The Blockchain continuously grows longer due to the constant mining process in the system. The procedure of adding a new block to the network is as follows: (I) once a miner confirms a valid hash value (i.e., a hash equivalent or lower than target) for a block, it includes the block in her own Blockchain and broadcasts the solution throughout the network and (II) after getting a solution for valid block, miners quickly check the solution and add the block to their Blockchain Non-valid blocks are discarded. Figure 1 shows the working approach that is being used for creating and maintaining Blockchain.

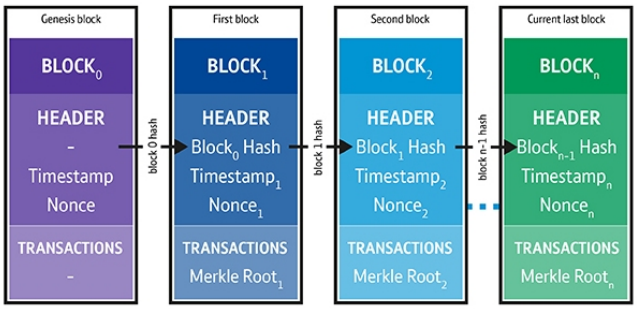

Fig. 1. Blocks in Blockchain [4]

Due to distributed nature of the block validation process, it is feasible that two valid solutions may be discovered simultaneously. This causes a delay in the distribution of a valid block. Another issue that may impede the validation of a block is the fact that miners are required to keep track of the global state of the Blockchain, comprising the completely ordered set of transactions. If there are two valid solution this is called a 'Fork' in Blockchain parlance.

When various forks exist, the miners can select a fork and proceed to mine over it. If the system has numerous forks and miners are extending different but valid versions of Blockchain based on their own Blockchain, miners working on one fork may communicate a valid block before miners working on another fork [5]. This results in a more extended version of the Blockchain in the system, and any miner can add new blocks on top of this longer Blockchain.

D. The Application of Blockchain

Some of the sectors where Blockchain is and eventually will contribute in a greater degree are described below.

- Financial Services

  I) *Assets Management:* The management of assets requires significant processing of sensitive and costly trading related transactions among multiple parties, often in a cross-border situation. Different parties such as the intermediary, the custodian or the settlement directorial keep their own copy of often similar records of transactions. This wastes valuable space and resources, and increases the chance of introducing human errors, affecting all other parties. Blockchain reduces such mistakes by encoding the records. In the meantime, it simplifies the procedure, while dropping the requirement for intermediaries [6].

  II) *Insurance Claims Processing:* Claims processing can often be a baffling and a difficult task for the claims processing officers. Insurance processors need to go through fake cases, staged incidents, difficult to deal with clients etc. which significantly increases the risks of errors and misclassifications. Blockchain in such a scenario can present an ideal framework for risk free administration and straightforwardness in processing cases. Its encryption [20] properties enable guarantors to ensure that processing is safe and reliable.

Apart from the points discussed above, *Cryptocurrency*, a digital currency system based on cryptography and Blockchain, has seen tremendous growth in recent times. Some of the notable Cryptocurrencies are Bitcoin, Ethereum, Litecoin and Ripple.

- Legal Services

Smart Contracts: A "Smart Contract" is a computer program for the automation of a promise, a self-executing digital contract that records and executes an agreement between two or more parties. Unlike a traditional contract, it is self-enforcing in nature, that is, a smart contract's outcome is inherently and directly coded into the contract itself [7]. A traditional Blockchain allows for a network of computers to build a trusted decentralized and automatic system that is an authority for such Smart Contracts. These digital contracts can be executed more efficiently and without human involvement, resulting in the potential for increased certainty of outcomes.

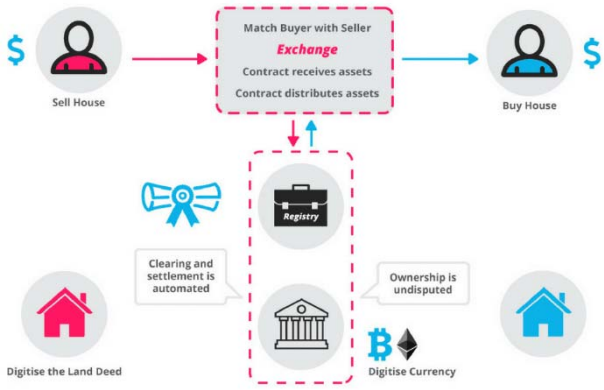

Fig. 2. Smart Contracts [8]

All kinds of contracts such as real estate, financial, intellectual property, employment etc. can take the form of Smart Contracts administered under a Blockchain network.

- Health Care

Blockchain projects are already in use where decentralized Blockchain based patient records are being provided and patient progress is also being monitored [9]. In the field of disease outbreak, data can be recorded into Blockchain systems so that the effectiveness of disaster relief and response can be enhanced [9].

However, work is still in progress to strengthen the security of the framework for this sector.

- Manufacturing and Supply Chain

A number of manufacturing and logistics corporations around the world have adopted Blockchain to accomplish important tasks in a supply chain network. Blockchains are being used to ensure transparency in product supply chains, from origin to the customers' doorstep [19]. Product tracking and tracing within the nodes while in transport is also encoded in a Blockchain system [9]. Throughout a supply chain network, a number of intermediary payments may be involved for which Bitcoin or another similar cryptocurrency such as Ethereum can be used. For an instance, Maersk – The Shipping and Transport consortium, has broached forward propositions to streamline marine insurance through Blockchain. While manufacturing a product, Blockchain based approaches can be put into practice to ensure that standards are met and the environmental impact is acceptable. Records can also be shared with concerned clientele.

- Retail Services

Attempts are underway to establish decentralized Blockchain based market platforms where goods and services are traded without any middlemen. Blockchain derived payment methods, loyalty schemes and gift cards are also available.

- Intellectual Property (IP) Rights

Multiple companies in digital media, music and film industries are developing Blockchain based solutions to track

IP rights and payment for artists. Records of ownership and ensuring royalties are also being created.

- Transport and Tourism

Ride sharing and vehicle leasing are being developed to work with Blockchain technologies [9]. Empty hotel rooms can efficiently be tracked and traded through the usage of Blockchain based digital solutions.

- Governments

I) *United Kingdom:* The Department of Work and Pension (DWP) is looking into opportunities to apply Blockchain so that recording and administering benefits payments can be made more efficient and secure [9].

II) *South Korea:* The government of South Korea is building Blockchain solutions to be used in the area of public safety and transport.

III) *Dubai:* The government of Dubai is taking the initiative to develop digital solutions built upon Blockchain for multiple departments such as registration of business, health regulations, shipping and stopping the trading of 'Blood Diamonds'.

Apart from these countries, the adoption rate of several Blockchain technologies by governments of different countries is increasing rapidly as suggested by Figure 3.

Fig. 3. Blockchain in Public Sector as of March 2017 [10]

Estonia, by December 2017, had in fact managed to put 100% of Government data in a Blockchain system as illustrated in Figure 4 [11]. Countries like Australia, Canada and Indonesia have started to roll-out Blockchain based systems especially for cryptocurrency payment [12].

So it is apparent that the adoption rate and application of Blockchain will continue to grow worldwide.

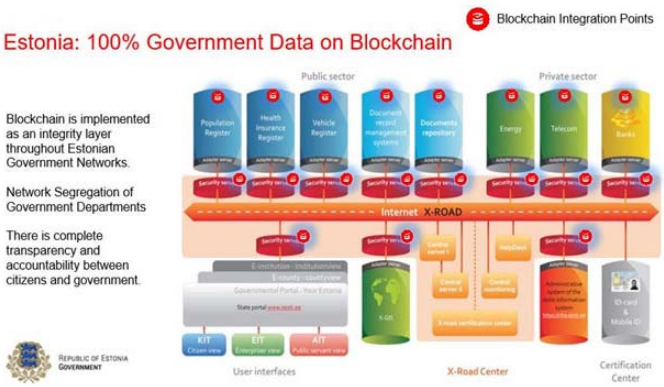

Fig. 4. Estonian Government's Blockchain Rollout [11]

IV. Attacks On Blockchain

Blockchain has stood the test of time against an array of different attacks. Due to the decentralized nature of its working environment, hackers and scammers have launched several versatile attacks over this technology. In this section, a detailed discussion on the topic will be given.

A. Double Spending

A customer could potentially achieve double spending (i.e., send two conflicting transactions in quick succession) in the event where customer can spend a set of the same bitcoins in two different transactions. For example, a dishonest customer (C1) could make a transaction (T1) at time t1 utilizing a set of bitcoins (B) with a recipient address of a merchant (V) to buy some item from V. The client broadcasts transaction T1 to the bitcoin network at time t2 where t1 and t2 are very close. The customer also creates and broadcasts another transaction T2 at time t2 using the same coins with as recipient address the customer himself or a wallet which is under the control of customer. If the customer would manage to deceive the vendor with the type of transaction, the merchant would deliver the purchased products to the customer, without ever receiving the payment, as visualized in Figure 5. However, research has indicated that to carry out such attacks over large Blockchain networks such as Bitcoin would require a very large amount of computational power, which is unlikely to belong to any individual.

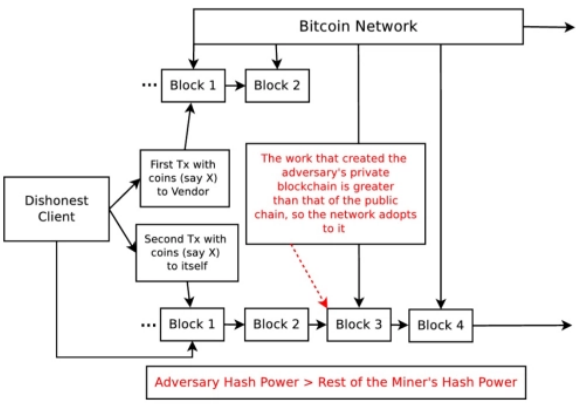

Fig. 5. Double Spending Attack [14]

Even if anyone would possess such computational power, his identity would get revealed at some point. The risk is larger for smaller networks is larger [9]. If a two transactions are proposed from the same bitcoin wallet address, the transactions initially move to the unconfirmed transaction pool. If this happens sequentially, the first transaction is approved via the confirmation mechanism and verified into the subsequent block. The second transaction would be recognised as invalid by the confirmation process and would therefore not be verified. If both transactions are pulled from the pool for confirmation simultaneously, the transaction with the highest number of confirmations will be included in the Blockchain, while the other will be discarded. Merchant should therefore be holding off the delivery of goods until multiple confirmations of the transaction have been recorded in the Blockchain.

B. Finney Attack

A Finney attack is a variation of double spending. Here a dishonest customer (Cd) pre-mines (i.e., secretly) a block which contains the exchange T2, and after that it makes a transaction T1 utilizing the same bitcoins as for a merchant (V) [15]. The mined block is not informed to the system, and ***Cd*** holds it back until the exchange T1 is acknowledged by the merchant, V. V just acknowledges T1 when it gets an affirmation from miners indicating that T1 is valid and can be incorporated into the existing Blockchain. When ***Cd*** gets the item from V, the attacker releases the pre-mined block into the system, and makes a Blockchain fork (say **B0** fork) of equivalent length to the existing fork (say **B** fork). At this point of time, if the following mined block in the network expands the B0 fork Blockchain rather than fork **B**, other miners in the system will continue to expand over the B0 fork. As the Blockchain B0 fork progresses towards becoming the longest chain in the system, the miners will disregard fork **B** and subsequently the top block on fork **B**, which contains the transaction, making T1 invalid, resulting in the customer getting back his or her coins through while merchant V still loses the item.

C. Brute-Force Attack

An advancement of the Finney assault is called a Brute-force attack in which a clever attacker has control over **n** nodes in the network, and these nodes by and large work on a private mining plan which aims to utilize them for a Double-Spend attack [14]. An attacker presents a double spend exchange in a block similar to earlier attacks, while continuously working on the expansion of a private Blockchain (i.e., B0 fork). Assume that a merchant waits for x affirmations before accepting an exchange, and sends the item to the customer once he gets the x affirmations. The attacker can mine the x number of pieces ahead (i.e., secretly) and can release these blocks in the network. Due to its excess length this Blockchain fork will then be extended further by the other miners in the system. This causes the same delayed consequences as the Finney attack, effectively causing a double spending attack using a different method.

Table 1 tabulates the practicality of several attacks against a number of Blockchain based application domains.

Table 1: List of Attack against Different Applications

	IoT	Government Services	Smart Contracts	Identity	Financials
Attacks					
Double Spending	✗	✓	✓	✗	✓
Finney	✗	✓	✓	✗	✓
Brute Force	✗	✓	✓	✗	✓
Vector 76	✗	✓	✗	✗	✓
Selfish Mining	✓	✓	✓	✓	✓
Block Withholding	✓	✓	✓	✓	✓
Bribery	✓	✓	✓	✗	✓
Sybil	✗	✓	✓	✗	✓
Eclipse	✗	✓	✓	✗	✓
Tampering	✗	✗	✗	✗	✗

D. Selfish Mining Attack

In truth, every one of the miners in Bitcoin could be called 'Greedy' as they are mining for the reward that is related with each block. However these miners are also legitimate and reasonable, while the Selfish Mining Attack, described here refers to the malicious miners only. In the selfish mining, the dishonest miners perform data hiding (i.e., withholding a mined block) and damage other honest miners using a two-fold thought process: (I) acquire an unfair compensation which is greater than their offer of processing control spent, and (ii) confuse other miners and lead them to waste their assets in fruitless courses. This attack affects all applications because blocks are added to Blockchain by miners. When miners are adding invalid blocks, or withholding valid blocks, it becomes difficult to add genuine blocks.

D. Sybil Attack

A Sybil Attack is a type of attack where the attacker installs dummy software and tries to compromise part of the Blockchain network. A Sybil attack is a community-oriented attack performed by a group of comprised nodes. Moreover, an attacker may change its character and may launch an intrigue attack with the partner nodes. An attacker tries to detach the client and disconnect the exchanges started by the client or a client will be made to use blocks, which are operated by the attacker. If no nodes in the system confirm an exchange, that info can be utilized for Double Spending attack. As Sybil is a network-based attack, there is a possibility of this type of attack in applications such as government services, smart contracts, financial services etc.

E. Block Withholding Attack

In this case, the attacker generates a valid block but refrains from broadcasting it, and instead broadcasts transaction X as a payment for a goods or services. A merchant may eventually observe transaction X and accept this 0-confirmation transaction. Immediately after that, the attacker will start broadcasting the previously generated block with transaction Y, conflicting with transaction X, the Bitcoin network will accept his block and invalidate transaction X [13].

This attack is quite costly to launch. Figure 6 illustrates the attack comprising of two attackers.

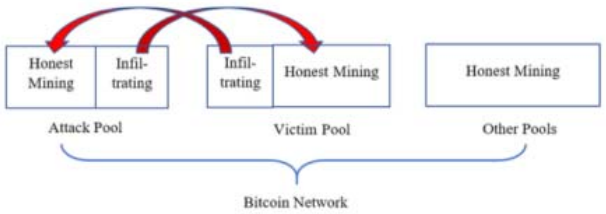

Fig. 6. Block Withholding Attack

Besides the above discussed attacks, there are more variations such as the Bribery Attack, the Eclipse Attack, Tampering, 51% Attack etc. to name a few. Botnets [16], can also affect Blockchain networks.

V. Conclusion And Ideas For Prospective Growth

In this paper, the possible applications of Blockchain technologies and associated risks have been highlighted. Its contribution includes identifying and listing the applications and mapping them with possible attacks. However, to make the growth of Blockchains smoother and faster, some proposed solutions could be quite effective, such as:

I) Building Blockchain based frameworks where it will be possible to involve the general public directly in achieving some tasks. This will greatly enhance their understanding of the procedure, as it is still quite esoteric to most of the general public.

II) Setting up more ATMs citywide so that it becomes easier to use cryptocurrencies to exchange Fiat money.

III) Unload or distribute the computational powers to a greater degree than what is possible nowadays so that IoT devices can be a part of Blockchain. This will indeed exponentially increase its applicability in daily live.

IV) Building effective programming solutions to integrate AI and Biometrics with Blockchain systems so that the regulatory requirements for financial services can be fulfilled with strict certainty.

V) If the field of *Quantum Computing (QC)* further matures it could overcome the slowness of the processing of Blockchains of with current computing technology. However, QC could also be a threat to public-key cryptography, thereby potentially putting the Blockchain technology at risk.

On a positive note, several of the abovementioned ideas are being evaluated at present by some of the major players in this field. Blockchain with all its potential, could indeed bring about a major change in our daily lives in the not so distant future.

References

[1] Haber, S. and Stornetta, W.S., 1990, August. "How to time-stamp a digital document". In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.

[2] Zhao, J., Fan, S. and Yan, J. (2016). "Overview of business innovations and research opportunities in blockchain and introduction to the special issue". Financial Innovation, 2(1).

[3] D. Kraft, "Difficulty control for blockchain-based consensus systems," vol. 9, no. 2, 2016, pp. 397–413.

[4] Fromm, K. (2017). "How blockchain and serverless processing fit together to impact the next wave" [online]. https://read.acloud.guru. [Accessed 31 January 2019].

[5] Szabo, N. (2018). "Secure Property Titles with Owner Authority". Satoshi Nakamoto Institute. [online] Nakamotoinstitute.org. Available at: nakamotoinstitute.org/secure-property-titles/ [Accessed 31 August 2018].

[6] BlockchainHub. (2018). "Blockchain Explained - Intro - Beginners Guide to Blockchain". [online] Available at: https://blockchainhub.net/blockchain-intro/ [Accessed 31 August 2018].

[7] Legalwise. (2019). "Rise of Smart Contracts with Blockchain Technology in Australia and New Zealand". [online] Available at: https://www.legalwiseseminars.com.au/news/smart-contracts-and-the-law/.

[8] Blockgeeks. (2019). "Smart Contracts: The Blockchain Technology That Will Replace Lawyers". [online] Available at: https://blockgeeks.com/guides/smart-contracts/.

[9] Marr, B. (2018). "35 Amazing Real World Examples Of How Blockchain Is Changing Our World". [online] Available at: https://www.forbes.com/sites/bernardmarr/2018/01/22/35-amazing-real-world-examples-of-how-blockchain-is-changing-our-world.

[10] White, M., Kilmeyer, J., Chew, B. (2017). "Will blockchain transform the public sector?". Deloitte.

[11] GlobalBankingAndFinance (2018). "Every week more Governments are announcing Blockchain adoption". [online]. Available at: https://www.globalbankingandfinance.com/every-week-more-governments-are-announcing-blockchain-adoption/. [Accessed 31 January 2019].

[12] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452. doi:10.1109/comst.2018.2842460.

[13] Heusser, J. (2018). "SAT solving - An alternative to brute force bitcoin mining." [online] Jheusser.github.io. Available at: jheusser.github.io/2013/02/03/satcoin.html. [Accessed 31 August 2018].

[14] Bitcointalk.org. (2018). "Best practice for fast transaction acceptance - how high is the risk?" [online]. Available at: https://bitcointalk.org/index.php?topic=3441.msg48384#ms g48384 [Accessed 31 August 2018].

[15] Blockchain Unleashed: IBM Blockchain Blog. (2018). "Blockchain for Government: IBM Blockchain Blog." [online] Available at:https://www.ibm.com/blogs/ blockchain/ category/ blockchain-for-government/ [Accessed 31 August 2018].

[16] Shanmugam, B., Azam, S., Yeo, K.C., Jose, J. and Kannoorpatti, K., (2017), January. "A critical review of Bitcoins usage by cybercriminals". In Computer Communication & Informatics (ICCCI), 2017 International Conference on (pp. 1-7). IEEE.

[17] BlockchainCouncil (2018). Blockchain-council.org. "How Does Blockchain Use Public Key Cryptography?" [online] Available at: https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/ [Accessed 31 August 2018].

[18] Lisk. (2018). "Peer to Peer Network" [online] Available at: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-a-peer-to-peer-network [Accessed 31 August 2018].

[19] Provenance (2015). "Blockchain: the solution for transparency in product supply chains". Whitepaper.

[20] Mota, A.V., Azam, S., Yeo, K.C. Shanmugam.B, and Kannoorpatti, K., (2017). "Comparative analysis of different techniques of encryption for secured data transmission", IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017.