**EDINBURGH NAPIER UNIVERSITY SCHOOL OF COMPUTING**

**MSc INITIAL REPORT**

**1. Student details**

|  |  |
| --- | --- |
| Last (family) name | Nwosu |
| First name | Nnamdi |
| Napier matriculation number | 40224579 |

**2. Project details**

|  |  |
| --- | --- |
| Project title | Privacy Preservation of Blockchain in Healthcare |
| Summary of project (300 words)  Include a note of its aims, the main research questions, the methods to be deployed, deliverables, and means of evaluating the project work as a whole. | This dissertation aims to investigate and demonstrate Privacy Preservation of Blockchain in Healthcare.  For the sake of comprehension and simplicity, I will explain what blockchain means so that the reader may have an insight of what this project is trying to achieve. Blockchain refers to a type of data structure that allows tracking and identifying transactions digitally and sharing this information over a distributed network (Stroud, n.d.).  Blockchain technology is a game-changer with the possibility to impact not few industries, but entire sectors. Deloitte (2016) have identified that Blockchain has the potential to significantly disrupt the healthcare industry and put patient data in the hands of the patient. The ability of a distributed ledger for ensuring data integrity and immutability that makes it possible for different parties to share data and collaborate, this trend is vital to the revamping of healthcare globally.  Healthcare supply chain model is not structured, there is no body with overall control of the supply chain, though regulators have some oversight. Transactions are being made by different parties, it may take a while to access patient’s medical history as it is being scattered in various databases, and this can cause a grave disaster in medical world such as drug abuse, drug counterfeiting, administering of expired drugs. Right from manufacturing to prescription records are being segregated, thereby making it very difficult to unify the records and encourage easy access and interoperability. Using blockchain will eradicate any discrepancies and allow transparency of records amongst authorized parties (Unleashed, 2017).  Clinical trials are big medical challenges for present-day clinical research, the way they are being maintained currently make is difficult for an easy accessibility, sensitive data are being stored unstructured, no certainty in terms of privacy and decentralization. Experiments and trials should be preserved using more secure means that will not exposed them to vulnerabilities such as ransomware that will cause data loss or alterations (DrugPatentWatch, 2017).  This project is worth doing as it will address the aforementioned challenges in healthcare system. Blockchain will unlock the benefits of interoperability in healthcare, thereby making life easier for patients and medical worker. Data integrity, privacy and security will be assured with the help of decentralization and immutability, what this means is that records will not be stored on a central server, instead it will be scattered on different nodes making it impossible to manipulate records.   * 1. AIMS AND OBJECTIVES      1. AIMS  1. A literature review that will cover some essential blockchain platforms and smart contracts and relate them to healthcare system. 2. Comparison between Blockchain and Iota’s Tangle. 3. Demonstration of a blockchain application using a suitable smart contract.    * 1. OBJECTIVES 4. Based on the literature review a suitable smart contract will be used to develop a client application using ASP.NET that will consume a blockchain application that will demonstrate the application of private blockchain in healthcare. A decentralized application will be built and hosted. 5. A comprehensive whitepaper that explain how the entire system was developed. |

**3. Literature review**

**Chapter 2 Literature review**

2.1 Introduction

In this chapter we will review literatures that are related to privacy preservation of blockchain, we will look at the background of the blockchain itself, the topic will be incomplete if smart contracts are left uncovered, as it is the backbone of blockchain applications. This chapter will be divided in to five main sections, background of blockchain, smart contracts platforms, Iota's Tangle, healthcare data processing, and homomorphic encryption respectively.

The first section is dedicated to the background of blockchain, how it works, consensus and first crypto-currency (Bitcoin) that unveiled this state-of-the-art technology that will change the way things are done.

The second section will focus on smart contracts, which are used to develop DAPPS (Decentralised Applications). Such as Ethereum, NEO and LISK.

The third section will cover IOTA Tangle.

The fourth section will focus on healthcare data processing.

Finally, homomorphic encryption will be covered that will give us a clear picture on how privacy can be achieved in a public ledger system like the Ethereum.

**2.2 Background of Blockchain**

According to (Marr, 2018), when the whitepaper of bitcoin was released in 2008 by the Satoshi Nakamoto, the creator of Bitcoin who is still unknown, Bitcoin was described as peer-to-peer version of electronic cash. This is where Blockchain made its public debut. Blockchain is the technology that runs Bitcoin. So, you cannot talk about Blockchain without starting the discussion of Bitcoin.

Since the evolvement of Bitcoin, more attention has been focused on the technology itself (Blockchain), and this has unveiled unlimited opportunities in our day-to-day digital activities. Blockchain has the potentials to impact every industry from educational institutions to financial to manufacturing such as making the supply chain decentralized and easily traceable (Marr, 2018).

Bitcoin was offered up to the open source community in 2009 after Nakamoto's whitepaper was released. Blockchain provided the solution to electronic trust because of the way it makes valuable information transparent in a public domain and makes it impossible to alter. It decentralises it so that copies of it will be scattered on different nodes (Marr, 2018).

Even today, some people believe that Bitcoin are blockchain cannot be decoupled, even though they are different. In 2014 some people started to realise that blockchain could be used for more than cryptocurrency and started investing in and how it can be used in various kinds1 of activities. At its core, it is a trusted decentralised ledger that permanently records transaction between two parties without the involvement of a third-party for authentication. It is an efficient way people believe that will dramatically reduce transaction cost (Marr, 2018).

According to (Marr, 2018) , when Entrepreneurs understood the capability of blockchain, this created a rush as people started investing and discovering how blockchain could impact supply chains, healthcare, voting, management, insurance, transportation and more.

**2.2.1 How Blockchain Network Works**

Instead of depending on a party, such as a financial institution, to act as a third-party between transactions, consensus protocol is being used by member nodes to agree on ledger content, and digital signatures and cryptographic hashes to ensure the authenticity of transactions (Perepa, Sloane Brakeville and Bhargav, 2016).

Consensusassures that the ledgers which are shared are uniform without any discrepancies, and lowers the risk of fraudulent transactions, because altering or tampering would have to be reflected on all the copies at the same time. Cryptographic hashes,such as the SHA256 algorithm, assures that a minuscule change to transactional input results in a different hash value being computed, which signifies potentially compromised input.Digital signaturesassure that transactions were initialized by senders and not imposters using a signed private key (Perepa, Sloane Brakeville and Bhargav, 2016).

The decentralized peer-to-peer blockchain network prevents a participant or group of participants from compromising the underlying infrastructure or controlling the entire system. Participants have equal right, adhering to the same protocols. They can be organizations, individuals, state actors, or a combination of all (Perepa, Sloane Brakeville and Bhargav, 2016).

(Perepa, Sloane Brakeville and Bhargav, 2016) further said, at its core, all transactions are recorded in chronological order with all nodes agreeing to the validity of transactions with a consensus model used. The result in transactions which are immutable and agreed on all the participants in the network.

**2.2.2 Consensus Protocols**

The lack of trust immanent in the blockchain system is notable to this section, as any entity, group, or individual can submit to the blockchain, it is crucial for the operators involved to agree on all "addenda" before they are permanently added to the blockchain. Because we cannot be sure of the honesty of the author, it is important to be reviewed for authenticity before being accepted (Hammerschmidt, 2017).

**2.2.2.1 Proof of Work**

A consensus algorithm, like proof of work used by bitcoin, does two things: It ensures the authenticity of the next block in a blockchain, it keeps malicious intruders from derailing the system (Castor, 2017) .

In proof of work, there is a competition among the miners to add the next block in the blockchain by solving a very difficult cryptographic puzzle. The first to solve it becomes the winner. The winner will be rewarded 12.5 newly minted bitcoin and a small transaction fees for solving the difficult puzzle (Castor, 2017).

(Castor, 2017), also included its common criticism, as it requires enormous amount of computational energy, and lack of scalability as it takes 10-60 minutes for transactions to be confirmed.

**2.2.2.2 Proof of Stake**

Proof of stake (PoS) According to (Manning, 2016), works in a different way from proof-of-work, it is a type of consensus algorithm, instead of investing in very expensive hardware just to participate, a miner or stakeholder puts up a stake or locks up an amount of their coins, for a block of transactions to be verified

Miners only need to prove they own a certain percentage of all the coins available in a given coin, and the cryptographic calculations in PoS are easier for computers to solve than that of Proof of Work (PoW) (Manning, 2016).

The Proof of Stake was created as an alternative to proof of work (PoW), for inherent issues to be tackled. The issue of PoW was solved by attributing mining power to the proportion of coins held by a miner. A PoS miner is restricted to mining a percentage of transactions depending on his or her stake (Investopedia).

**2.2.2.3 Delegated Proof of Stake**

According to (Kuster, 2017), delegated proof of stake (DPoS) was developed by Bitshares’ lead developer Daniel Larimer, also known as Bytemaster. He realized the energy that is being wasted through Bitcoin mining, and he also perceived that Bitcoin mining would become centralized considering the bitcoin network being in control of giant mining pools. Bitcoin’s system was not scalable and too slow because of its design and the system it uses.

(Kuster, 2017), also said that Delegated proof of stake and conventional proof of stake are not the same, and the difference is akin to the difference between representative democracy and direct democracy. In conventional PoS, every wallet that contains coins is eligible to ‘stake’. This implies that take part in validation process and forming the distributed consensus and earn some coins as a reward. In Distributed Proof of Stake system, any funded wallet is eligible to vote for delegates. Transaction validations are performed by these delegates, and they also maintain the blocks and are being rewarded in return using the traction fees.

According to (Buntinx, 2017),DPoS provides more decentralization than PoS in terms of issuing stake rewards to more people. Furthermore, DPoS uses a real-time voting and a reputation system to achieve consensus.

**2.2.2.4 Proof of Burn**

The way proof of burn works is quite different from aforementioned consensus algorithms. According to (Gill, 2018), in proof of burn coins are sent to an unspendable address, also known as an “eater address”, burning them effectively. Coins cannot be accessed or spent again once the are burned, as it has already been recorded in the blockchain, there is a proof that the coins can no longer be accessible or used, and the user may be rewarded for the burn.

(Gill, 2018), goes on to say that the objective behind proof of burn is that by burning a coin, a user is demonstrating preparedness for a short-term loss for long-term investment. Users stand a greater chance if they burn more coins, users may be rewarded in the process through proof of burn reward mechanism overtime when mining.

**2.2.2.5 Delegated Byzantine Fault Tolerance**

This consensus algorithm was developed by NEO for its platform. Neo holders can vote in order to decide who will be there consensus node, and consensus nodes decides who will be their speaker (A selected node that picks a block for delegated nodes to vote). Users have to communicate their transactions to the delegated consensus nodes, and it is being documented as a ledger which is being presented as a block. (Basic Crypto Coin, 2018).

(Basic Crypto Coin, 2018) further said, one of the selected consensus nodes is randomly selected to propose a block. The selected node will then send the block to the rest of the consensus nodes to confirm the accuracy, if it does not correspond with at least 66% of the consensus nodes, then the authenticity will be disregarded, then the said block will be discarded, and another consensus node will be selected among others, this process will continue until at least 66% of the consensus nodes agree on the authenticity of the block, and it will be added to the blockchain. A node must have at least 1000 (At the time the source document was published) “GAS” to qualify for delegation (Being a consensus node.).

According to (CryptoGraphics, 2018), delegates (Consensus nodes) can determine if a delegate is dishonest, or if it received a corrupted block from a dishonest speaker (The randomly selected delegate that proposes a block) by comparing their blocks. Dishonest delegates will be replaced by a new one if more than 50% of the delegates find the block to be valid.

According to (Castor, 2017) there are other types of consensus algorithm such as proof of activity, proof of capacity, and proof of elapsed time.

**2.2 Smart Contracts**

This section will focus on blockchain platforms such as Ethereum, NEO and LISK which are used for developing decentralised applications (DApps). Ethereum, NEO and LISK, reader will be able to understand their basic functionalities.

A smart contract is a computer program that runs on top of a blockchains that contains some conditions under which the participants to that smart contract accept to interact with each other. Agreement is automatically enforced if a predefined rule is met. Negotiation or performance of an agreement is being facilitated by smart contract code without any third party (BlockchainHub).

**2.2.1 Ethereum**

For the sake of limited time allocation for this research, I will not cover the full details and functionalities of Ethereum. I will concentrate on its comprehensive review for basic understanding.

Ethereum is a decentralized platform that allows the running of smart contracts: An application that runs without any possibilities of failure or third-party being involved (Ethereum, n.d.).

These apps operate on a custom blockchain, this makes it possible for developers to store registries of debts, transfer future funds according to agreed condition (like a futures contract or will) and other things that will be invented in future, all will be done without a middleman that sits in-between the two parties (Ethereum, n.d.).

**2.2.1.1 Ethereum Smart Contracts**

I assume readers are familiar with “Smart Contracts”. Ethereum is not just a payment-system platform where money is transferred among users, it provides the interface for users to write wallet-based programs using its smart contracts (Malanov, 2017).

Wallets can send money to these programs automatically, the amount to send, where to send, and so forth are decided by these programs, with an important condition: The programs runs according to rules that are predictable, immutable, equal and transparent to its users. And it operates homogenously for all users (Malanov, 2017).

(Malanov, 2017) further said that these programs, also known as smart contracts, are added to the blockchain where they are stored forever, and parties involved have a copy of it, with equal execution for every network user that uses it.

Ethereum current uses proof of work (PoW) consensus algorithm for now, but it is planning to move to proof of stake (PoS) in 2018 (Castor, 2017).

Ethereum’s creator, Vitalik Buterin, recently released an approximate implementation guide that shows the will first start with a ‘hybrid’ system that merges bitcoin’s proof-of-stake with its much anticipated proof-of-stake system called Casper, created by Vitalik (Hertig, 2017).

The plan simply means that Ethereum will start alternating between PoW and PoS, so that some transaction blocks are secured through PoS and the others remain on PoW (Hertig, 2017).

Ethereum uses Solidity which is contract-based, high-level programming language, which has a very close syntax to the scripting language of JavaScript. Solidity is statically typed language which is responsible for enforcement and verification of constraints at compile-time as opposed to run-time. As a programming language of Ethereum, it is made for enhancement of Ethereum Virtual Machine. (Sharma, 2017).

To move Ethereum between accounts, miners have to calculate the new blocks, to compensate them for their efforts, transaction sender must pay a fee(Gas which is also known as Ether), which depends on the complexity of the transaction sender wants to make. (Zuchowski, 2017).

**2.2.2 NEO and its Smart Contracts**

Neo is a cryptocurrency framework which was developed by Onchain, a company based in Shangai, which started as “Antshares” and rebranded recently to become NEO. The platform encompasses smart-contracts and has been referred to as the “Chinese Ethereum” as it has similar functionality with Ethereum, such as support for Decentralised Applications (DAPPS), and Initial Coin Offerings (ICOs). It is different from Ethereum as you have multiple choices of programming languages such as Java, C/C# and GO, while Ethereum you are restricted to using only Solidity language. Next to the coin “NEO” is another one called “GAS” which is the currency for the apps on the system, which is same as Ethereum’s Ether (Dale, 2017).

NEO has a focus on digital assets, identity and smart contracts, and it is designed as a distributed network for “Smart Economy”. Digital identity on the NEO platform will take control of identity information of organizations, individuals, and other groups that digitally exist. Method to link digital and physical representation of assets. NEO offers additional features such as cross-chain interoperability, peer-to-peer networking and digital certificates. NEO could possibly achieve infinite scalability with its efficient Virtual machine (Warner, 2017).

**2.2.3 LISK**

According to (Adams, 2017), LISK is a blockchain application platform built to allow programmers to develop decentralized applications(Dapps) like NEO and Ethereum. Javascript developers can build Dapps using its “sidechains”.

LISK is just like Nxt, Bitcoin or Bitshares in terms of network decentralization, but it does not utilize Proof of Work like Bitcoin or Proof of Stake like Nxt. It utilizes Delegated proof of stake like Bitshares (Which was covered previously). You can develop your own blockchain applications on top of LISK sidechains using the LISK App SDK. You can also develop social media apps, games, exchanges, contract execution platforms, IoT applications, that are decentralized without any complications (Kordek, 2016).

**2.2.3.1 LISK’s Sidechain**

LISK’s sidechain allows its users to fully customize its blockchain, which makes it to be decoupled from the mainchain, and free from pollution or spam on the other sidechains or the mainchain itself. You can create parameters that are only applicable to your blockchain application without affecting other sidechains or the mainchain (Kordek, 2016).

According to (Cointelegraph, 2016), sidechains do not affect the speed, security or scalability of the mainchain as it is an independent cryptographic ledger that is being attached to the mainchain. Sidechains are important as they reduce the load off the mainchain making it faster and efficient.

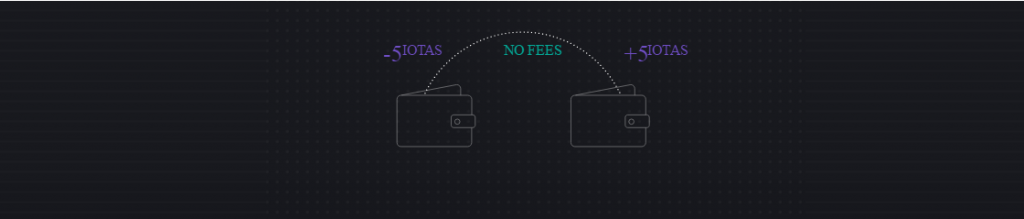
**2.3 Tangle**

I wish to cover all about “TANGO” in this section, unfortunately, I will focus on its basics, as detailed explanation that encompasses its underlying technology is broad, and the allocated time for this research will not be enough for it.

For the last six years the evolvement and progress of Bitcoin really proved the value of blockchain technology. Nevertheless, the platform has some drawbacks which prevent it from being adopted generally by cryptocurrencies, for instance, the idea of transaction fee irrespective of the value of the transaction involved is a notable drawback. Due to the need for inclusion of IoT devices will make Bitcoin not to be the best, as paying a transaction fee higher than the actual value is not logical. This drawback cannot be worked around due to the nature of Bitcoin’s consensus algorithm (POW), miners are being paid some fees for validation of transactions(IOTA Whitepaper, 2017).

According to (The Tangler, n.d.), IOTA uses “TANGLE” was born in 2014, and it is the backbone of Internet of Things (IoT), and the only technology of its kind, but a distributed ledger that is scalable, quantum resistant and decentralized. IOTA is the very first technology that allows Nano payments without a need for transaction fee. Below features make TANGLE different from blockchain:

* IOTA is based on Direct Acyclic Graph (DAG) also known as TANGLE, not blockchain.
* It cost nothing to transact using IOTA (No transaction fee).
* Unlike blockchains, IOTA is scalable.
* Nothing like mining, blocks in IOTA.
* IOTA supports the machine economy.
* IOTA is an interoperable protocol that solves the problem of Internet of Things (IoT).



**Figure 1: Above image from (IOTA, n.d.) demonstrates IOTA’s no fee feature.**

**2.4 Healthcare Data Processing**

The healthcare sector has generated huge amount of data known as “Big Data” over time, as a result of compliance and regulatory rules, record keeping, and patient care. The current trend is to digitize these huge data as some of them are still in hard copy form, the need to improve the quality of healthcare, and the reduction of cost will be beneficial to healthcare industry, as it will aid in medical and healthcare functions, including other clinical decision making, population health management, and disease surveillance ( Raghupathi & Raghupathi , 2018).

**2.4 Homomorphic Encryption**

Homomorphic encryption is the process by which calculation can be done on encrypted information (cyphertext) without being decrypted. It is essential as it helps in making cloud computing more secure, as trust is always an issue when it comes to storing data on cloud provided by third-parties (Greenberg, 2014).

(Greenberg, 2014) further said that a search engine which is homomorphically encrypted could take encrypted parameters and compare them with the ones on the web using the index. Or data in cloud database that are homomorphically encrypted would allow users to know how much money an employee earned in a specific period time. However, it accept an encrypted name and also output an encrypted result, this protects the data from privacy problems that usually afflict the internet.

**2.4.1 Fully Homomorphic Encryption(FHE)**

Instead of being limited to a specific computation, with fully homomorphic encryption, you can perform computational operation on encrypted data using any function, without being decrypted or exposed (Experts, n.d.).

According to (Gentry, 2009), fully homomorphic encryption has many applications, such as allowing search engine for querying encrypted data, it also makes it possible for encrypted data to be searched. Encrypted data can be stored on a remote server, and allows the server to fetch the query result based on the input parameters without the server knowing the content of the data.

**2.4.1 Partially Homomorphic Encryption(PHE)**

Computations on encrypted data is either additions or multiplications in Partially homomorphic encryption unlike fully homomorphic encryption. This has existed for many years. With partially homomorphic encryption you can build exciting apps. Below are examples of applications which can be built with PHE.

* Electronic voting: A tally can be computed from the encrypted votes without each vote being decrypted, except the result.
* Data mining: Mean, variance and linear regression of simple statistics can be computed.
* In voice/image processing: Liners functions like matrix multiplications and fast Fourier transformations can be performed efficiently with partially homomorphic encryption.

**2.5 Conclusion**

The first part of this literature review covered the background of Blockchain technology and the consensus algorithms. Based on the algorithms covered, it shows that proof of work is less efficient as it consumes a lot of resources such as electricity, finance, and high computing power. According to (Young, 2016), a malicious attack can be launched on small proof of work network, if the attacker has up to 51% of the computing power. Though other consensus algorithms may have their own flaws such as centralization problem, in the case of proof of stake, major stakeholders could control the entire network and become decision makers thus creating a major “monopoly”.

Based on the reviewed literature, Tangle is faster and more efficient than blockchain, as you do not pay a transaction fee to miners, and it scales faster than Bitcoin’s blockchain. IOTA is also quantum resistant but bitcoins’ blockchain is not. I believe when IOTA project is finalized, it will have a better use case than the blockchain considering its outstanding features.

# References

Raghupathi, W., & Raghupathi , V. (2018). *Health Information Science And Systems.* Retrieved from Big data analytics in healthcare: promise and: https://www.biomedcentral.com/track/pdf/10.1186/2047-2501-2-3?site=hissjournal.biomedcentral.com

Adams, C. (2017, December 5). *Invest In Blockchain*. Retrieved from Understanding Lisk (Part 1): The Lisk Platform Explained: https://www.investinblockchain.com/lisk-platform-explained/

*Basic Crypto Coin*. (2018, January 26). Retrieved from NEO’s Delegated Byzantine Fault Tolerance explained: https://cryptowizard370887289.wordpress.com/2018/01/26/neos-delegated-byzantine-fault-tolerance-explained/

*BlockchainHub.* (n.d.). Retrieved from Smart Contracts: https://blockchainhub.net/smart-contracts/

Buntinx. (2017, April 20). *Merkle.* Retrieved from What is delegated proof of stake: https://themerkle.com/what-is-delegated-proof-of-stake/

Castor. (2017, March 4). *A (Short) Guide to Blockchain Consensus Protocols.* Retrieved from Coindesk: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/

*Cointelegraph.* (2016, May 22). Retrieved from Lisk to Move Developers from Blockchain to Sidechain: https://cointelegraph.com/news/lisk-to-move-developers-from-blockchain-to-sidechain

*CryptoGraphics*. (2018, February 7). Retrieved from The Byzantine Generals’ Problem: https://cryptographics.info/cryptographics/blockchain/consensus-mechanisms/delegated-byzantine-fault-tolerance-dbft/

Dale, O. (2017, December 21). *Blockonomi.* Retrieved from A beginner's Guide to Neo: https://blockonomi.com/neo-guide/

Deloitte. (2016). *Opportunities for Blockchain in Healthcare.* Retrieved from Deloitte: https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html

DrugPatentWatch. (2017, November 8). *Medium.* Retrieved from How Will Blockchain Revolutionize The Healthcare Industry?: https://medium.com/drugpatentwatch/how-will-blockchain-revolutionize-the-healthcare-industry-6821b1e6ffe6

Ethereum. (n.d.). *Ethereum*. Retrieved from Build unstoppable applications: https://www.ethereum.org/

Experts, C. (n.d.). *CRYPTO EXPERTS* . Retrieved from Fully Homomorphic Encryption: https://www.cryptoexperts.com/technologies/fhe/

Gentry, C. (2009). Retrieved from A fully homomorphic encryption scheme: https://dl.acm.org/citation.cfm?id=1834954

Gill. (2018, January 16). *99bitcoin.* Retrieved from What is Proof of Burn: https://99bitcoins.com/what-is-proof-of-burn/

Greenberg, A. (2014, 03 11). *WIRED.* Retrieved from HACKER LEXICON: WHAT IS HOMOMORPHIC ENCRYPTION?: https://www.wired.com/2014/11/hacker-lexicon-homomorphic-encryption/

Hammerschmidt. (2017, Jan 9). Retrieved from Medium: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe

Hertig, A. (2017, May 5). *Coindesk.* Retrieved from Ethereum's Big Switch: The New Roadmap to Proof-of-Stake: https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/

*Investopedia.* (n.d.). Retrieved from Proof of Stake: https://www.investopedia.com/terms/p/proof-stake-pos.asp

*IOTA*. (n.d.). Retrieved from https://iota.org/

*IOTA Whitepaper.* (2017, October 1). Retrieved from The Tangle: https://iota.org/IOTA\_Whitepaper.pdf

Kordek, M. (2016, July 26). *Lisk Community Update.* Retrieved from What Is Lisk? And What It Isn’t.: https://blog.lisk.io/what-is-lisk-and-what-it-isnt-e7b6b6188211

Kuster. (2017, November 3). *Captain Altcoin.* Retrieved from What is Delegated Proof-of-Stake? – A Complete Beginner’s Guide: https://captainaltcoin.com/delegated-proof-stake/

Malanov, A. (2017, October 18). *Kaspersky.* Retrieved from Explainer:Smart contracts, Ethereum, ICO: https://www.kaspersky.com/blog/ethereum-ico/19846/

Manning. (2016, November 2). *EthNews.* Retrieved from EthNews: https://www.ethnews.com/proof-of-work-vs-proof-of-stake-explained

Marr, B. (2018, February 16). *Forbes.* Retrieved from A Very Brief History Of Blockchain Technology Everyone Should Read: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#354551537bc4

O’Byrne, R. (2016, October 24). *Logistic Bureau.* Retrieved from Nursing Hospital and Healthcare Supply Into a New Age: https://www.logisticsbureau.com/nursing-hospital-and-healthcare-supply-into-a-new-age/

Perepa, Sloane Brakeville and Bhargav. (2016, May 9). *IBM.* Retrieved from Blockchain basics: Introduction to distributed ledgers: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

Sharma, T. K. (2017, September 2). *Blockchain Council.* Retrieved from What is Solidity, Programming for Ethereum Smart Contract: https://www.blockchain-council.org/ethereum/what-is-solidity-programming-language-for-ethereum-smart-contracts/

Sharp, N. (2017, November 16). *JJSManufacturing*. Retrieved from Blockchain for manufacturing: what are the opportunities?: http://blog.jjsmanufacturing.com/blockchain-for-manufacturing-what-are-the-opportunities

Stroud, F. (n.d.). *webopedia*. Retrieved from blockchain: https://www.webopedia.com/TERM/B/blockchain.html

*The Tangler*. (n.d.). Retrieved from IOTA- WHAT IS IT, WHO IS IT?: http://www.tangleblog.com/what-is-iota-what-is-the-tangle/

*tutorialspoint*. (n.d.). Retrieved from SDLC - Waterfall Model: https://www.tutorialspoint.com/sdlc/sdlc\_waterfall\_model.htm

*UKcryptocurrency.* (n.d.). Retrieved from Introduction : What is IOTA?: https://ukcryptocurrency.com/iota/introduction-what-is-iota/

Unleashed, I. B. (2017, October 30). *Blockchain Unleashed: IBM Blockchain Blog*. Retrieved from Blockchain in healthcare: Patient benefits and more: https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/

Warner, M. (2017, December 30). *Medium.* Retrieved from Smart Contracts and Scalability on NEO Blockchain: https://medium.com/@blockpass/smart-contracts-and-scalability-on-neo-blockchain-f86c8dae82fb

*XB Software*. (n.d.). Retrieved from Software Development Life Cycle (SDLC). Waterfall Model: https://xbsoftware.com/blog/software-development-life-cycle-waterfall-model/

Young, J. (2016, September 14). *Eligma.* Retrieved from Proof-of-Work vs Proof-of-Stake: merits and disadvantages: http://www.coinfox.info/news/reviews/6417-proof-of-work-vs-proof-of-stake-merits-and-disadvantages

Zuchowski, L. (2017, November 14). Retrieved from Ethereum: Everything you want to know about Gas: https://blog.softwaremill.com/ethereum-everything-you-want-to-know-about-the-gas-b7c8f5c17e7c

**4. Annotated contents list for the dissertation**

[INTRODUCTION](#_Toc509739350)

[*1.1* PROJECT MOTIVATION](#_Toc509739351)

[1.2 AIMS AND OBJECTIVES](#_Toc509739352)

[1.2.1 AIMS](#_Toc509739353)

[1.2.2 OBJECTIVES](#_Toc509739354)

[Chapter 2 Literature review](#_Toc509739355)

[2.1 Introduction](#_Toc509739356)

[2.2 Background of Blockchain](#_Toc509739357)

[2.2.1 How Blockchain Network Works](#_Toc509739358)

[2.2.2 Consensus Protocols](#_Toc509739359)

[2.2 Smart Contracts](#_Toc509739360)

[2.2.1 Ethereum](#_Toc509739361)

[2.2.2 NEO and its Smart Contracts](#_Toc509739362)

[2.2.3 LISK](#_Toc509739363)

[2.3 Tangle](#_Toc509739364)

[2.4 Healthcare Data Processing](#_Toc509739365)

[2.5 Homomorphic Encryption](#_Toc509739366)

[2.5.1 Fully Homomorphic Encryption(FHE)](#_Toc509739367)

[2.5.2 Partially Homomorphic Encryption(PHE)](#_Toc509739368)

[2.5 Conclusion](#_Toc509739369)

[Chapter 3: Methodology](#_Toc509739370)

[3.1 Introduction](#_Toc509739371)

[3.2 System Development](#_Toc509739372)

[3.2.1 Requirement Analysis](#_Toc509739373)

[3.2.2 Design](#_Toc509739374)

[3.2.3 Development](#_Toc509739375)

[3.2.4 Testing](#_Toc509739376)

[3.2.5 Maintenance](#_Toc509739377)

[Chapter 4: Design and Implementation](#_Toc509739370)

[4.1 Introduction](#_Toc509739371)

[4.2 Proof of Concept](#_Toc509739372)

[4.3 Testing](#_Toc509739372)

[Chapter 5: Conclusion and Recommendations](#_Toc509739370)

[5.1 Conclusions](#_Toc509739371)

[5.2 Recommendations](#_Toc509739372)

[5.3 Further System Development Considerations](#_Toc509739372)

5.4 Further Research

**5.  Work plan**

|  |  |  |
| --- | --- | --- |
| **MILESTONE** | **DATE** | **TARGET** |
| Milestone 1 | 06/04/2018 | Finish Design |
|  |  | Finish Development |
|  |  | Finish Testing |
|  |  |  |
| Milestone 2 | 13/04/2018 | Finish Chapter Five |
|  |  |  |
| Milestone 3 | 17/04/2018 | Finish, print report, and put together documents. |