A PROPOSED PURCHASE CYCLE AUDIT APPROACH USING BLOCKCHAIN TECHNOLOGY TO INCREASE AUDIT EFFECTIVENESS AND REDUCE FRAUD

Oluwaseun Latifat Salami

A Project

Submitted to the Faculty of Graduate Studies, Concordia University of Edmonton

in Partial Fulfillment of the Requirements for the Degree

Master of Information System Security & Assurance Management

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 8, 2020.

A Proposed Purchase Cycle Audit Approach Using Blockchain Technology to Increase Audit Effectiveness and Reduce Fraud

Oluwaseun Latifat Salami

Shaun Aghili (Approval on File)

Supervisor Date: April 20, 2020

Edgar Schmidt (Approval on File)

Dean of Graduate Studies: Date: April 20, 2020

ABSTRACT

Over the years, purchasing cycle fraud schemes have been the greatest risks of fraud for most organizations. Blockchain technology can maintain transactional data with full decentralization and reducing the growing number of cases of fraud in companies and organizations. This paper focuses mainly on the effectiveness of a blockchain-based system in enterprise procurement. It aims to create an audit template aimed at further preventing purchasing cycle fraud and enabling audit effectiveness in the purchase cycle sector through the implementation of triple entry accounting. This can be achieved by continuing previous research on blockchain accounting and discover how the technology if implemented, could influence the reduction of high audit cost and fraud detection in organizations. The literature review is carried out based on peer-reviewed publications and related professional literature. The current purchase cycle approach takes over 12 steps to complete a cycle that sometimes presents significant challenges such as insufficient lead time, management apathy etc. Blockchain's introduction into the purchase cycle will help standardize business processes, improve efficiency, and reduce operating costs. Blockchain network offers a confidential environment where transactions are not dependent on a centralized authority. The general assumption is that blockchain would help decrease fraud and errors, mitigate transit and delivery costs, reduce duplication and improve the management of purchases.

Keywords: Blockchain, Purchasing cycle, Auditing.

Contents

INTRODUCTION

Background

Purchasing cycle fraud schemes involving employees, such as over-billing, fictitious invoices and conflicts of interest are the greatest risks of fraud for most organizations. For instance, in 2017, a national retail chain contractor that's 61years of age defrauded a United States organization of more than $2 million, the contractor was an employee for over 15 years and had oversight of leasing buildings to house the stores of the company. Alteration of 22 contracts documentation, including forgery of letters for fictitious legal and maintenance services to the company, as well as a copy of the company's leases to match the bills incurred from services to those leases.

Over the years, organizations have tried different methods to discourage procurement fraud by introducing procedures to reduce the likelihood of its occurrence, but the problem of procurement fraud persists and is severely damaging to businesses. Using proper controls such as blockchain technology helps in the prevention of procurement fraud. When blockchain undermines a payment processing facility, the entire series of transactions can be traced. Organizations can minimize the likelihood of fraud through the implementation of blockchain.

According to the Association of Certified Fraud Examiners (ACFE), 2018 Report to the Nations (RTTN), Procurement fraud is the second most widely recorded type of economic crime behind misappropriation of assets, asset misappropriation scheme is the most common fraud on the fraud tree in 89% of its reported cases with median loss at an estimated $114,000 per occurrence, according to the survey. Furthermore, an article posted on the CPA Canada website

(Gordon, 2019) indicated that misappropriation of assets fraud makes up 85% of all reported employee fraud cases in Canada. A more effective purchase cycle control using blockchain technology may help further eradicate or prevent future incidents of falsified expense purchases or fraudulent billing schemes report.

This research project is focused on proposing a purchasing cycle audit template based on the triple entry (Debit, Credit, Blockchain) system to improve the effective detection of fraud such as fraudulent billing schemes and expense falsification as it pertains to an organization's typical purchase cycle. The implementation of such a triple entry accounting system and its accompanying proposed audit approach is also likely to help organizations in reducing their financial audit costs by reducing the amount of substantive testing required during financial audits.

The study consists of five sections; Section one encompasses of introduction, statement of the problem, objectives of the study, research methodology, significance and organization of the study. Section two of this paper focuses on a literature review comprising of: the theoretical background of blockchain technology, first-time adoption of blockchain technology for procurement, the definition of key concepts and how they interact with one another, the relationship between triple entry accounting and their current challenges, the perceived benefits of its implementation in the purchase cycle. The scope, research questions, procedures as well as limitations will be discussed in the Methodology section. The presentation of the results section introduces and discusses the final research deliverable. The research paper concludes with a discussion of conclusions and considerations, including recommendations for further studies of the exploratory and theoretical framework presented in this paper.

LITERATURE REVIEW

Triple Entry Accounting

Triple-entry accounting can be defined as an accounting system whereby a third variable is introduced according to the global standard (debit and credit), generally known as the double-entry principle. (Taylor, 2017). The third entry and triple entry accounting is cryptography, where there is a cryptographic account of the transaction stored permanently and immutably on the ledger. Ledger in this context is a distributed immutable record of a collection of transactions, which is owned by every participant in the blockchain.

The concept of triple-entry book-keeping, also known as momentum accounting, was first presented by Yuji Ijiri as the logical next step in accounting (Oden, 2018). In the double-entry accounting system, each organization keeps its collection of books. This process is time-intense and tends to increase audit costs because auditors take longer hours trying to reconcile the books (Taylor, 2017). An article on Systems innovation explained Triple entry accounting as' an upgrade to the standard double-entry method in which a third entry seals all accounting entries affecting outside parties cryptographically ", Therefore, put side by side, all parties ' bookkeeping entries and refer to the transaction. The third blockchain entry in the system is both a receipt and a transaction. For example, A seller reports a debit to account for cash earned while a buyer announces a cash loan spent on the same transaction with separate record sets. This is where the blockchain comes in: they take the form of a pool of permanent and accurate accounting records between wallet addresses in the same shared public instead of logging these entries separately in separate sets of ledgers. (Brett, 2018).

Triple-Entry Accounting characteristics include Tamper-proof Records, Distributed ledgers, Double-entry plus cryptography, Validated, Secure, Private as well as digitally Signed Receipts.

The merit of implementing a triple entry system is a reduction in the possibilities of falsified transactions. In the case of reconciliation, transparency, trust, and auditing, it provides an unchanging history of all device exchanges that could be analyzed using analytics and perfect audit trail. Auditors can quickly verify the data of the financial statement in lesser time and emphasis on greater risk sections such as internal control of the organization. (Ian G, 2018). Triple entry accounting also creates a level of validation and integrity due to the encrypted signature of the third party (Blockchain). (Taylor, 2017).

Blockchain At A Glance

The term 'Blockchain' is a mixture of two words 'the block' containing batched transactions and a 'chain' representing cryptographically connected blocks (Natalia, 2018). NISTIR 8202 defined two categories of blockchain as permission-less and permissioned. The difference is that for a permissionless blockchain network, anyone can read and write without approval to the blockchain and is available to any future user (American Institute of CPAs, AICPA), while Permissioned blockchain networks, limits involvement in particular individuals or groups, which allows for finer controls. These blockchains overcome some of the public blockchains' drawbacks but still risk some of the potential benefits, such as decentralized transactions, Wide distribution of the ledger and a fully decentralized environment, with no intermediaries (AICPA). Understanding the differences between these two categories allows an organization to understand which subset of blockchain technologies may apply to its needs. There are different principles of blockchain, namely immutable, data distribution, efficiency, anonymity, etc. If the entire chain of blocks parallel to that transaction is also updated, a single transaction or record can be removed or amended (NISTIR 8202).

The hash is a one-way task, it can not be used to retrieve the initial data; it serves as a proof of data generated by the hash that corresponds to the original information. With regards to blockchain, it can function as an impartial, trustworthy, third-party mediator in practically any relationship or contract. (edX, 2019). Hashing is achieved by the 'n' number of networked computers. Every block has the same digital calculation and its unique signature. If a new block is registered, the participant will receive the same note. No information can be modified or altered on this block. Only the current old knowledge will add value to the participants. The participants also can only attach value to the old knowledge that already exists. (Chamria, 2018).

Merkle tree also identified as a hash tree is a code structure used for efficient data retrieval, data verification and synchronization. It is a structure of tree data, where each non-leaf node is a hash of its child nodes. All the nodes of the leaf are as wide as possible and as far left as possible. (Lakshita, 2018). By generating a root hash of that data, Merkle trees summarise the entire set of data in a block. To this end, it preserves data integrity and uses hash functions.

The blockchain can't be abused with this transactional data ordering scheme without invalidating the previous chain of hashes. One major issue is interoperability. Hash functions at the core of the Proof of Work (PoW) consensus, an algorithm is utilized as the cryptographic puzzle. (edX, 2019).

An article titled Blockchain Architecture Basics: Components, Structure, Benefits & Creation written by Anastasiia, Lastovetska summarized blockchain structures into three categories:

a) Public Blockchain Architecture

Public Blockchain Architecture is used according to the organization's needs. It ensures that the network information and exposure are open to anyone willing to participate (e.g. Bitcoin, Ethereum, and blockchain Litecoin networks are public). No authorization to join a public blockchain network is required; all participants can access, store and change the database by making their computing power available (PWC, 2017)

b) Private Blockchain Architecture

Private Blockchain Architecture is also designed to handle internal functions such as access control, mainly for audit purposes. Such networks are restricted to approved participants, with the owner or managing entity having the required permission.

The advantages of private blockchain include being fast, more efficient, making full internal control validation mechanisms more secure and trustworthy. The disadvantages include fewer developers, slow improvement and lack of flexibility.

c) Consortium Blockchain Architecture

This is regarded as a fusion of public and private blockchain platforms (Leonard T, 2017). Consortium Blockchain regulates the public blockchain's decentralized existence, and the private blockchain's permissible capability. Procedures are set up and controlled by the preliminary assigned users. Permission and access are managed by an entity and not by an organization. The blockchain network is a 'semi-private' framework with a managed user group that operates across different organizations. (Yafimava, 2019).

The difference is that in a public blockchain, there's potential to exchange most functions of ancient monetary establishments with a software system and essentially reshaping the approach

the national economy works while for Consortium blockchain, they don't permit any individual with access to the web to participate within the method of substantiating transactions (Yafimava, 2019).

Consensus of Blockchain

1) **Proof of Work (PoW) consensus**- According to Satoshi Nakamoto's blockchain innovation, POW consensus algorithm is potentially exposed to the 51% attack, where one network node had 51% of the network's total computing capacity, thereby having the ability to validate transactions and create new blocks on a one-handed basis Someone has to be chosen in a decentralized network to record the transactions. Random selection is the preferred way, however, is susceptible to attacks. When a node decides to publish a transaction block, a lot of work needs to be done to verify that the node is unlikely to attack the network. (Zibin Z, Shaoan X, Hongning D, Xiangping C, & Huaimin W 2017).
2) **Proof of Stake (PoS) consensus**- That means a person can mine transactions or validate them based on the number of coins they have. PoS is an energy-saving alternative Proof of Stake means that the farther a miner owns Bitcoin or altcoin, the more extractive power he or she has (Zibin Z et al., 2017).
3) **Delegated Proof-of-Stake (DPoS) consensus** - It is a core approach to a network of blockchains. In this consensus process, the stakes also known as tokens holders pick delegates who, in turn, confirm network transactions.
4) **Proof-of-Authority (PoA)** -It uses a collection of 'authorities' appointed nodes that allow new blocks to be generated and the ledger secured. This consensus algorithm is mostly used for permissioned ledgers. Ledgers using PoA require most authorities to sign for the development of a block. (edX, 2020). This leverages identity morals, implying that block

validators are not staking coins but have their credibility. POA is considered effective and efficient in the purchasing cycle sector alternative compared to POS and POW because it can perform many more transactions per second.

5) **Simplified Byzantine Fault Tolerance (SBFT)** – This consensus algorithm validates data, improves network throughput, and reduces the latency of transactions. It includes a single validator moving forward proposed transactions and creating a new block (edX, 2020) to prevent double-spending challenges. The goal of SBFT is to protect against catastrophic system failures by minimizing the impact these malicious nodes have on the network's proper operation and the appropriate consensus reached by the system's honest nodes.
6) **Proof of Activity** -is an algorithm that is used to ensure that all transactions that occur on the blockchain are legitimate and that all users achieve consensus on the precise status of the public ledger. (Frankenfield, 2020) It also avoids the possibility of a 51 percent attack as in POW and POS, as it is difficult to foresee who the signing peer will be in the future, and coin saving rivalry between signers will not allow the computational power to accumulate within the community.
7) **Proof of Capacity (POC)-** This method offers a much cheaper and safer source of block verification, thus more effective and viable with the use of hard drive and its storage. POC is a two-stage model (mining and plotting), This enables the blockchain network's mining devices (nodes) to use space on their hard drive to access the crypto coins available. Instead of continuously manipulating the numbers in the block header and repetitive hashing for the solution value, POC operates by storing a list of possible solutions on the mining system's hard drive just before mining operations begin. (Frankenfield, 2020). POC secures the

network using cheap low-power hard drives instead of highly costly power-hungry processors, graphics cards etc. (Kapoor, 2019).

Smart Contracts

IBM Blog defined smart contracts as computer code stored on a ledger, which in various circumstances execute actions. A smart contract can hasten business processes, decrease mechanical failure and increase cost-effectiveness. Since the blockchain retains the smart contract, the agreement can be accessed by managers and auditors, thereby removing the need to request duplicate copies. The system creates a hash string that provides visibility to all members as proof of work (PoW) in each block. Werbach and Cornell delineate a smart contract as "A digital arrangement which is self-executing and self-imposed". (Ramos, 2017). The uses of smart contracts are trust, irreversibility, autonomy etc. Utilizing the smart contracts purchasing process, where the terms are payable upon receipt, proof of delivery from a logistics provider would automatically activate automated programmed computerized invoicing and payments through the financial framework, with no traditional difference between customer and supplier. (Breuck, 2019).

Other features of smart contracts are Digital Signature, Oracles and Self Execution, Decentralization, etc. (Sila, 2019). The key disadvantages are that a person can safely store and store data in smart contracts, and there are no inconsistencies, only if the code is correctly and accurately written with transaction time and cost. (Grybniak, 2017).

The agreement will reside on a decentralized blockchain in the form of the contract itself, which ensures both its validity and its execution. Each group would use cryptographic private keys as a digital signature (Sila, 2019). Forecasting their revenue as well as the assurance of faster payment is a major benefit of a smart contract.

Ethereum and Hyperledger Fabric are smart contract systems that use a Merkle tree called the Patricia tree to store their virtual machine's current state. Ethereum is a public protocol allowing anyone who accesses the Ethereum blockchain network to view the terms of each agreement unless encrypted. (Deloitte 2016, AICPA, 2017). Hyperledger framework can be described as an open-source, private blockchain system built for functions in enterprises.

Under the Linux foundation, Hyperledger Framework, was developed and managed by a few organizations. It uses a configurable architecture that provides a range of features including distributed ledger structures, smart contract engines, plug-in consensus protocols, user interfaces etc. (Zhang, Jian,2019).

Ethereum and Hyperledger Fabric use digital transactions and block signatures to check the creator's identity and that the signed data has not been changed since the signing date. Within the blockchain, public-key cryptography is used as a means of handling identities of users without exposing identities in the real world. (edX,2019).

Purchasing Cycle

The purchasing cycle is the procurement of goods and services in exchange for cash or commitments to pay cash. Auditing transactions in the purchasing process (e.g. raw material purchases, expenditures, accounts payable, and cash) usually consists of a mixture of quantitative monitoring and compliance check to support a management risk assessment that is at or below the limit. The procurement process is an integral aspect of supply chain management, identifying cross-company inventory and management of information flow. A purchase cycle flowchart in most organizations goes through five (5) steps, which are requisition, purchase orders, receiving the report, payment vouchers and checks. During auditing, the process is time-consuming, and there is a potential for fraud occurring as well as issues with a purchase error. The use of blockchain

in the process would help to reduce the costs of procurement, management, documentation and enforcement. (PwC, 2017). In developing countries, New entrants should be helping to join the market and new markets will expand and enhance customer satisfaction by simplifying the implementation and increasing accountability.

Purchase Cycle Fraud

Procurement fraud is an intentional deception designed to influence every stage of the purchasing lifespan to make a financial gain or instigate a loss. It can be carried out by suppliers or subcontractors within the organization (National Fraud Authority, 2011). Sources of fraud include bank account sharing employees and vendors, separate workers sharing bank accounts, multiple invoices from the same company, excessive overtime of employees, etc. (PwC, 2018).

Case Study

A finance director in a Nigerian supply organization, abruptly resigned, stating personal intent. His actions were reviewed to decide whether he acted outside of the organization's interests. Findings from the analysis of the supplier master files of the organization using an automated fraud detection system revealed that a 'bank account' section of several suppliers had been altered. The account information had been changed to a collective bank account information, with some transactions added to it. The account information was traced to the resigned Finance Manager.

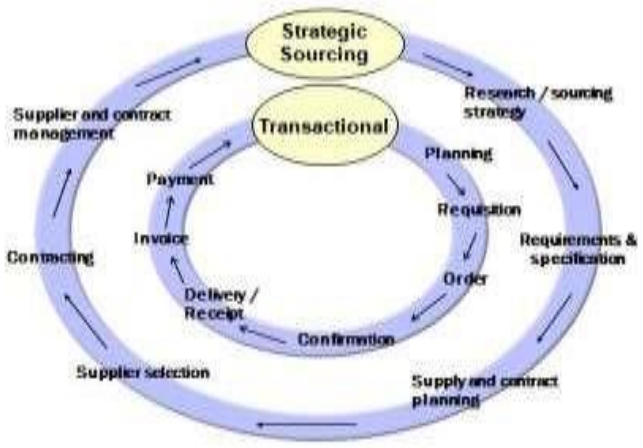

Fig 1- Fraud can take place at almost any point in the procurement cycle (Smith, P.,2015).

Few fraud schemes can occur in the purchasing cycle process in an organization.

1) **Kickbacks and Bribery**- Kickbacks or bribes are paid to decision-makers in exchange for manufacturing or non-commercial business contracts. A worker participates during a bribery theme once he or she accepts a vendor's payments reciprocally for a bonus. The charge should influence the competitive offer from the company. Bribery comes in a variety of forms; it may be monetary or in kind. Examples are expensive presents, credit cards, Greek gifts, sexual favors, etc. (PwC, 2018).
2) **Check Tampering**- Check tampering is a crime that is far more rampant in America than in other countries. (ACFE, 2018). Tampered checks scheme involves forging, modifying or producing fake checks that are rendered payable either to the perpetrator, the accomplice, the seller or "cash.".
3) **Conflict of Interest**- It involves overbilling a client for a supplier's products or services in which an employee has unknown ownership or financial interest. (ACFE, 2018). Referring

to the case study Where a member of the procurement team fails to notify the contractor or supplier of their plans, illegally communicates with the supplier or receives gifts or payments This is known as the purchasing cycle fraud scheme because the employee takes advantage of the organization's confidence in trusting the employee to act in the organization's best interest.

4) **Delivery Fraud**- Ways of fraud delivery include abuse of variance, abuse of contract specification and funds for misappropriating claims.
5) **Bid-Rigging Schemes** - Many bid-rigging schemes involve bribery during the bidding process between competing companies. It involves groups that agree to submit supplementary contract winning bids, sometimes on a rotational basis. Manipulation happens when a deal is handled to favor a preferred bidder, or circumstances surrounding him. (Clement, 2014).
6) **Billing Fraud**- This is the deliberate issuance by a manufacturer or contractor of false, duplicate or inflated invoices. This may also occur in collaboration with the buyer's representatives who will benefit from the scam in some way.
7) **Fake Invoicing Schemes**- Suppliers inflate invoices either on their own or by colluding with the project team, create false invoices or supply duplicate invoices for goods or services. (Deloitte, 2014). Fraudulent payment schemes can be complex and hard to detect, and those schemes can run for years before they are detected.

Implementation of a blockchain may help to reduce at least a few of these fraud schemes by implementing digital time-stamp documents to prevent manipulation of checks, the ability to keep a secure, cryptographic record of transactions. For example, transaction payment in a procurement

process is in' digital format' before the process is complete. There will be no avenue for tampering because the transaction is clear on both ends of the block.

The immutability of blockchain is also a characteristic that helps reduce fraud, the data can not be lost or altered as soon as a record is inserted into the system. Blockchain technology has the ability in a purchase cycle process to remove manual measures and roadblocks. It will minimize purchase order cycle time and invoice processing time, it will enhance first-time match rates for invoices for quicker processing of invoices, and boost supplier relationships.

Furthermore, Blockchain technology can enhance coordination and cooperation between the suppliers and the retailer through the lifecycle of each purchase. The blockchain has a great role to play in the purchasing cycle because fraud is often a matter of manipulating numbers or letters on paper. What better Preventive method than a system with which all kinds of information can be stored without altering it.

Benefits of Using Triple Entry in Detecting Purchase Cycle Fraud Scheme

1. Implementation of blockchain helps to shorten the steps in the purchasing cycle as well as the time frame of auditing (Meuwissen, S. (n.d.))
2. It increases efficiency and curbs issues of missing purchase transactions because of the traceability factor in the blockchain. (Deloitte)
3. Labour cost- audit cost reduces because there is less work to audit. Auditors can focus more on internal controls.
4. It means overreaching a company for a supplier's products or services in which an employee has unknown ownership or financial interest. (ACFE, 2018)
5. A Blockchain procurement platform can enhance the process of identifying and testing potential bidders. (Elegbe, 2018).

6. Another benefit is the prevention of fraud by real-time transaction processing and the immutability of the blockchain data.
7. Blockchain guarantees confidence between parties in cases where workers can falsify details about their business expenses and cause their employers to overcompensate in the form of reimbursements for inflated expenses. (ACFE,2018)

Blockchain technology is an emerging technology that promises to alter the way financial transactions are carried out. An article titled Blockchain - 7 Benefits for the Financial Industry by Michiel Mulders, stated the advantages of blockchain technology in the financial industry as prompt settlement, i.e. blockchain will take out the middleman in a transaction which will improve the swift settlement, creation of a better financial product such as crowdfunding mediums to provide a solution to the limitations of the blockchain (accessibility, transparency etc.), reduction of counterparty risks and improved contractual performance. (Mulder, 2019).

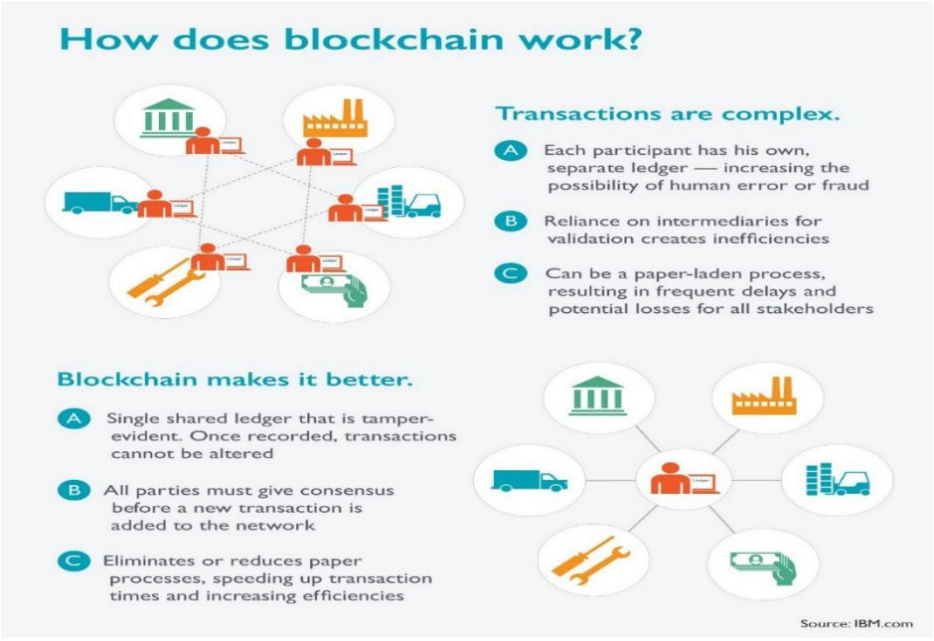

Fig 2- How does blockchain work

Source- IBM.COM

Blockchain technology is expected to decrease dependency on auditing to verify financial transactions and include an "automated third-party verification" (Spoke, 2015). The advantage of blockchain is that when the records are added to the database, there is a computer network that stores and verifies each new record as well as linking to the previous one, creating complete traceability and preventing any alteration of data. (Maltaverne, 2018)

The immutability of the data within a blockchain is highlighted " All members of a business network agree on the details collected in each transaction; once an agreement exists, it becomes a permanent record that cannot be modified" (Parnell, 2017). This ledger contains a record of all transactions, arranged in sequential "blocks," and it is public, or "distributed," to avoid fraud such as tampering; other users would quickly reject an altered version.

Unlike any previous technology, blockchain is changing the way related organizations come together and allowing for a new level of trust based on a common view of the truth. (F. Churchill, 2007).

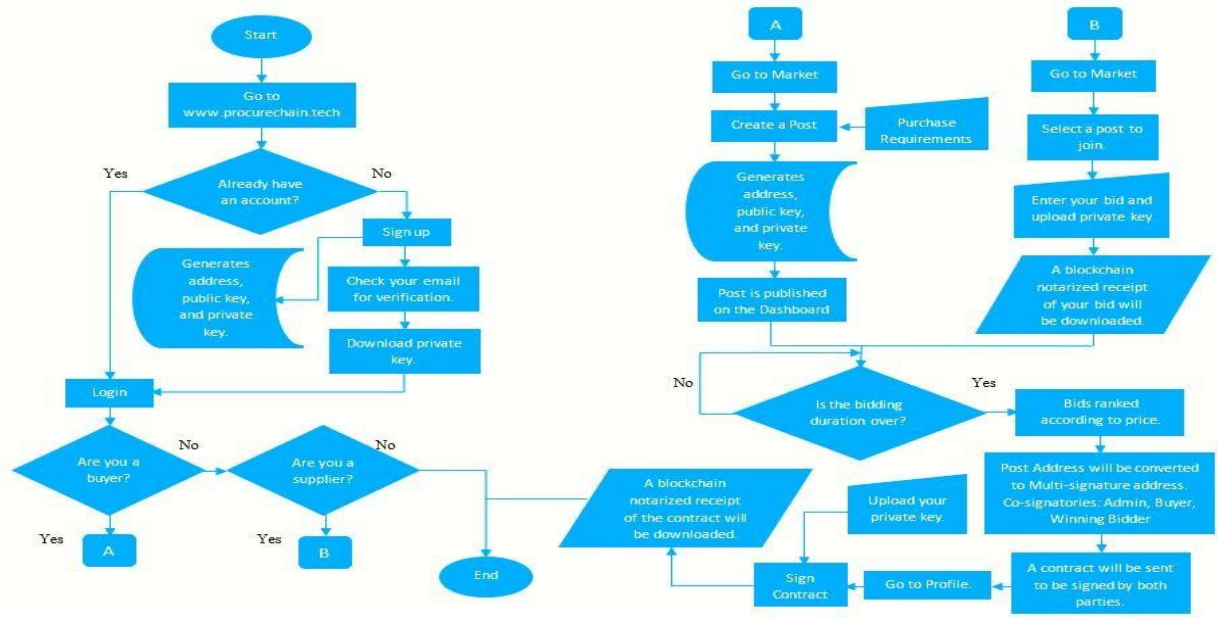

Fig 3**:** A blockchain model of a user joining the platform and acting as a buyer and a supplier. (August Thio-ac et al, 2019).

Public blockchains like Ethereum give room for a permanent and immutable collection of code, called a smart contract, that runs on the blockchain that entails an account balance, executable code and private storage. Such services assist in fostering, implementing and executing the terms of the agreement. The contractual state includes the storage and balance of the contract that is stored on the ledger, which is updated whenever the contract is cited. Types of smart contracts are wills, trusts, insurance plans, proprietary content, lending and escrow etc. Only when the consumer is satisfied with the product or service, can smart contracts release payment to the vendor. This also provides identity verification while preserving anonymity. Private blockchains in the network, such as intranet; there are nodes made of protocol collections. That blockchain has its own set of protocols that not only identify the nodes but also reveals how these nodes interact with each other (Peer network). It can help alleviate many of these issues and create a truly common organizational technical infrastructure. It allows participants in a supply chain or procurement to track data and exchange the data on how goods and services are generated, developed, consumed, and sold to the open market, which we have been unable to do technologically before. (edX, 2019)

According to Shala, Trick et al (2019), key advantages of using blockchain include maintaining data integrity, safe access, non-repudiation, and identity management options. Consequently, it offers tremendous potential for making the Machine-to-Machine (M2M) system more efficient. The Peer to Peer overlay (P2P) is used to manage M2M application services. By saving the service's interface description (IDS) and related personal temporary contact information, the end-user providing the service will register it using the P2P overlay network.

(Shala, Trick, Lehmann, Ghita, & Shiaeles, 2019). The downside of the decentralized M2M service platforms, there is no centralized body that controls the end-user service creation process. Blockchain can also improve human to human (H2H) cooperation as trust is also behind such collaboration. This is especially the case if partners do not know each other, and this often happens with new business transactions. H2H blockchain is cryptographic, hence identity and reputation are ensured that users are said to be who they are. Business to Consumer (B2C) can be defined as a business or direct transaction amongst businesses and customers who are the end-users of its products or services. (Belasy, 2017). Blockchain technology brings transparency to the customers through ethical sourcing validation, labour verification and immutable shared view.

The public key infrastructure (PKI) security is used to execute strong authentication, digital signatures, data encryption, and to provide a public key that represents the identity of the user. The private key is stored in a wallet and the user credentials list is a wallet.

Challenges of Blockchain Implementation in The Purchase Cycle

This section focuses on the challenges that could happen if organizations adopt blockchain:

1. **Control, Security and Privacy**: Bitcoin blockchain is not following the immutability feature in blockchain, Bitcoin was a public distributed ledger, visible to any account holder; Anyone could show the balance and complete transaction history in that wallet with the wallet number. Recently, Microsoft revealed the Confidential Consortium Framework, a method for businesses using Ethereum more privately and not influencing scalability. The solution includes off-chain settlement, using edge hardware and trustworthy execution environments such as Intel's." (Forbes, 2017). Such security issues need to be resolved before the general public entrusts a blockchain solution to their data.

2. **Regulatory Status**: National governments have both developed and controlled modern currencies. Cryptocurrencies face difficulties in widespread adoption by pre-existing financial institutions if their legal position in government remains unsettled. (Meuwissen, (n.d.))
3. **Cultural Adoption**: Change is a more significant challenge amongst humans. To achieve an adaptation challenge it requires time, commitment and excellent knowledge transfer.
4. Due to the scalability compared to other transaction processing systems, blockchain networks have seen a decline in transaction speed and increased fees per transaction. However, Deloitte said work is being done to create a more efficient model that can increase the speed of transactions. New consensus structures are being used by companies in the industry such as Hyperledger, Stellar and Ripple to accelerate this process.
5. **Implementation Cost**: It is costly to set up the initial Blockchain infrastructure. The investment costs could be daunting on a smaller scale. (Sreeperambudur, 2019).
6. The lack of interoperability between blockchains and the lack of friendly UI results in low user adoption, which is detrimental to the blockchain industry's development.

Overview of ISO Standards Governing Purchase Cycle

ISO 20400:2017 Sustainable Procurement Guidance- This standard focuses on the crucial role the supply chain plays in managing environmental risks and capitalizing on opportunities for sustainability. This addresses the key principles of sustainable procurement, the fundamental principles of accountability, integrity, respect for human rights and ethical conduct, and their vital importance for organizational success.

ISO 28000:2007 (Specification for security management systems for the supply chain): Requires management of security system requirements involving those aspects which are essential

to supply chain security. This includes all activities controlled or influenced by organizations affecting security within the supply chain. More considerations would be deemed explicitly, how they affect security management, including transportation in the supply chain. The ISO does not set specific purchasing procedures for companies, but only allows companies to identify their procurement processes, decide who is eligible to approve purchases, ensure that the procedures of the company are properly controlled and that those procedures are enforced.

According to an article on ISO 9001 purchasing procedures by Markgraf, it stated companies apply ISO 9001 to mitigate the issues with their goods and services to their purchase, problems such as minimizing waste and enhance customer relationships (the purchaser and the final customer). Companies are also encouraged to implement this standard to improve its operations and appoint a staff that it must report to the top management about its quality assurance on purchasing procedures. (Markgraf, B. 2016).

METHODOLOGY

The purpose of this research is to help create an audit template aimed at further preventing purchasing cycle fraud and enabling audit effectiveness in the purchase cycle sector. This paper builds on previous ideas widely used in procurement research and demonstrates how they can be applied to issues related to blockchain. Utilization of various search strings for the keywords consisting of 'Blockchain' and 'Procurement' to ensure wider coverage of research domains, search engines such as IEEE Explore, Web of Science, ACM Digital Library and Google Scholar among others were used to find information. The key goal was to include mainly high-quality papers published in conferences, journals, seminars, symposiums and books. Findings from the research questions will be examined, and relevant guidelines will be discussed with a strong emphasis on audit effectiveness for the implementation of blockchain technology. However, the scope of this

research paper is limited to the benefits, capabilities of blockchain technology concerning purchase cycle fraud prevention.

Furthermore, an important limitation of this study related to the fact that this research is highly theoretical in nature, there are several kinds of research carried out on blockchain technology already, there are very few that discussed the triple entry accounting and auditing. Also, the research team lacked the platform to test the effectiveness of the proposed project

Relevant question concerning the purchase cycle sector addressed by this study is:

- What are the best practices and controls to be adopted and implemented for the mitigation and/or prevention of fraud schemes in the purchase cycle sector?
- How will the implementation of Blockchain technology be used within the purchase accounting cycle and come up with an Audit template Checklist for mitigating and/or preventing Fraud Scheme?

The following procedures were followed in the conception of the proposed purchase cycle audit approach; determine the various fraud schemes related to the purchase cycle based on the literature review, identify the benefits associated with using a triple entry accounting system to detect purchase cycle fraud schemes. Identification and compilation of best practices and controls from frameworks and standards such as ISO 28000, ISO 20400, ISO 9001:2008, COBIT 2019 and NIST 8202. Recommendations for setting up an enhanced purchase cycle audit checklist based on implemented blockchain technology.

PRESENTATION AND DISCUSSION OF RESULT

When incorporation of findings on procurement fraud systems, internal control elements and contract management processes, a better image of procurement fraud emerges.

Based on the findings, the Private-Permission Blockchain will be recommended as the best for organizations. In the smart contract, purchase orders from the department are paid with funds from the general ledger to local bank suppliers as soon as the delivery is completed. There's no allowance for bribes or gifts in cash. Private blockchains allow users to have different permissions levels so that access can be restricted, and data can be encrypted to protect privacy. The blockchain must cut across all nodes so that the other nodes will disallow the transaction if any node is compromised. Private blockchains are faster, more cost-effective and more stable than public blockchains, which requires a lot of energy and time to verify transactions. A private blockchain would allow accountants and auditors to automate audit processes and audit transactions in real-time. If implementing blockchain into the purchasing cycle, the mechanism of Consensus Proof of Stake (POS) is much more resource-friendly than POW. In a Proof of Stake system validators have a much greater incentive to manage the network as they possess the blockchain coins they validate on. Research shows that Ethereum plans to move from Proof of Work to the Proof of Stake consensus soon. Proof of stake will virtualize the entire mining process and will replace miners with validators. Many of the bid-rigging, bribery, billing schemes and conflict of interest fraud occurred during the source selection process. It is during source selection that contract proposals are reviewed, costs are negotiated, and decisions are taken on contract awards. An auditor needs to determine that reasonable and reliable audit evidence supports the reported transactions. The auditors would also need to gain confidence over the consensus algorithm of a blockchain and perform a risk evaluation over the IT security climate. In the first step, based on the literature

review, the researcher studied and identified a major fraud scheme that has been suffered by the organization's purchasing sector.

Diagram 3 shows a flowchart blueprint of blockchain implementation into the purchase cycle.

Next, we compiled a total of 30 best practices and controls derived from a few information security frameworks and standards which included ISO 28000, ISO 20400, ISO 9001:2008, COBIT 2019 and NIST 8202. Table 1, this includes the purchasing stages, fraud schemes and related control account.

This step outlined the mapping of the 17-fraud scheme with the best practices and controls concerning purchase cycle manual steps. Table 1 below provides the reader with a partial view:

Table 1: *The Mapping of Seventeen Recent fraud scheme Experienced by the organisation purchase cycle Sector with thirty Best Practices and Controls*

The Mapping of Seventeen Recent fraud scheme Experienced by the organisation purchase cycle Sector with thirty Best Practices and Controls

/N	STAGES IN THE PURCHASE CYCLE	FRAUD SCHEME	BEST PRACTICES AND CONTROLS
1	ORDER REQUISITION	1. BILLING SCHEME 2. UNNECESSARY ORDERS.	1. The auditor should ensure that authorization is done by the right personnel 2. Ensure checking the material, quantity and required delivery date 3. The auditor should ensure that evaluation was done on order with budget 4. Are approval limits covered in written procedures?
2	SELECTING SUPPLIER	1. PRICE FIXING 2. CONFLICT OF INTEREST	5. Confirm the list of approved or registered suppliers 6. Ensure the suppliers and staff are aware of the organization's policies on code of conduct, gifts and entertaining 7. Will all resources, equipment, and services demand need authorisation from the supervisor? 8. If catalogue or advertising rates are not available, do the buyers receive price quotes or bids from two or more suppliers on large purchases?
3	QUOTATION AND TENDERING	3. BID RIGGING 4. PRICE FIXING	9. Are the right suppliers selected? 10. Accuracy of quotation with the price, compliance to specification, terms of the condition of sale, delivery and payment terms 11. Precision of quotation with the price, compliance with specification, conditions of sale, delivery and terms of payment.

The Mapping of Seventeen Recent fraud scheme Experienced by the organisation purchase cycle Sector with thirty Best Practices and Controls can be found at: Google doc address: https://drive.google.com/open?id=1aw2XwKt3jWdi_iQhnUKldSYm0Hg7AQYu (Sheet 3)

The last step in constructing the research deliverable which is the creation of an audit checklist template that auditors can use in a company that has blockchain technology implemented in its purchase cycle.

The audit template entails 2 categories; firstly, purchase cycle checklist and secondly checklist for when an organization implements blockchain technology. The purchase cycle template cover from access rights, security, approvals, checks for accuracy etc. while triple entry accounting involves governance, consensus, hashing, data validation, procedures for security of data collected and areas that cannot be modelled into blocks.

The figures below provide the reader with a glimpse of the audit template for both the purchase cycle and blockchain implemented the purchase cycle. Readers interested in reviewing the entire template may retrieve it at Google doc address:

https://drive.google.com/open?id=1aw2XwKt3jWdi_iQhnUKldSYm0Hg7AQYu

(Sheet 4 & 5).

PURCHASE CYCLE AUDIT CHECKLIST

Check "Yes" or "No" or "N/A" (where not applicable). Where a No is indicated, some action may be required to rectify the situation.

N	Purchasing Cycle risks to consider	Yes	No	N/A	Comments / Action Required
1.	Is collection of transactional data (purchase) properly documented?				
2.	Are there procedures in place to validate correctness of invoice against the corresponding purchase order?				
3.	When errors are identified, are there prompts required to make adjustments &approvals required?				
4.	Do you ensure that disbursements are recorded completely and accurately?				

Fig 4: Purchase Cycle Audit Checklist Template.

	A	B	C	D	E	F	G	H	I	J
		BLOCKCHAIN- PURCHASE CYCLE AUDIT CHECKLIST								
		Check "Yes" or "No" or "N/A" (where not applicable). Where a No is indicated, some action may be required to rectify the situation.								
		Blockchain- Purchasing Cycle risks to consider	**Yes**	**No**	**N/A**	**Comments / Action Required**				
1		Does creation of blocks have documented approvals? If yes; What level of authorization exists for creation of block or initiation of transaction?								
2		Is there a blockchain control mechanism in place between initiation and approval?								
3		Is the hashing algorithm robust enough? Ex: SHA256 or better?								
4		Is there a blockchain's consensus protocol used in selecting a block creator?								

Fig 5: Purchase Cycle - Blockchain Implemented Audit Checklist Template

The result of the above purchasing cycle audit template will determine what percentage of control testing as against substantive testing will be carried out if the auditor is not satisfied which happens in very rare cases.

RECOMMENDATIONS AND CONCLUSIONS

In terms of financial loss, reputational damage, and complexity, procurement fraud can be one of the most important types of fraud faced by organizations within the region. This project aims to provide a timely but brief overview of the role and potential of blockchain technology in the purchasing process sector and related impact on the reduction of fraud within an organization. The research deliverable shows the conception of an audit checklist framework to be used by auditors in an organization with blockchain technology applied in its procurement cycle; with the implementation of Blockchain technology use in auditing, there is a great potential to reduce audit cost because a larger amount of time is reduced when maintaining and reconciling ledgers. Furthermore, Blockchain also provides ownership of assets by ensuring transparency, Blockchain ledgers are immutable, and all legitimate transactions are followed by a timestamp that can aid in

auditing and avoid fraud and counterfeits. This use case will boost compliance with laws, reduce paperwork and dramatically cut audit costs.

An employee may prepare and submit a fraudulent check along with legitimate checks. This often happens when the check signer is busy or maybe out of office. Since the check signer is relied upon to provide some form of prevention, additional controls could be offered by implementing blockchain technology. Blockchain technology provides transparency and accountability; ensuring companies are accountable for their actions creates a compliant mechanism and trustworthy relationships. Optimistically, procurement teams will be able to see the larger picture and be open to distributing blockchain networks beyond their organizations and developing/joining cross-organizational blockchain information networks.

The implementation of blockchain technology into the purchase cycle could reduce the competitive edge in the organization as well as eliminating untrustworthy merchants within an entire industry sector. Blockchain technology is recommended to function as a genuinely secure repository of public records and transactions, removing thereby the need for a centralized record management authority. Integrating this technology into the processes of an organization would result in performance, trust and protection. though, blockchain is still in its early stages and therefore only suitable for pilot projects. Automated blockchain audits would also allow users of the financial statements to access information better, more effectively and at the acceptable level of detail.

In the digital world, the procurement industry recognizes the need for creativity and is becoming less afraid to look out of the box. This will increase corporate value as a creative incentive by combining considerable external knowledge and expertise with internal business partners while ensuring technology and market leadership for its goods amid the reduction of

private incremental audit costs. As earlier stated, most work is in pilot stages, blockchain technology would need more time to reach the desired scalability, decentralization and security for justifying it to be able to reach the commercial side of this sector. Only additional projects can prove the commercial feasibility to be able to be adopted in the mainstream.

REFERENCES

(PDF) Using Blockchain Technology for Business Processes in Purchasing − Concept and Case Study-Based Evidence. Available From: Https://Www.Researchgate.Net/Publication/325787549_Using_Blockchain_Technology_For_Business_Processes_In_Purchasing_-_Concept_And_Case_Study-Based_Evidence (Accessed Oct 29, 2019).

ACFE, "Report to The Nation on Occupational Fraud and Abuse," The Association of Certified Fraud Examiners, 2010. Www.Acfe. Com

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017, November 15). Blockchain Technology in Business and Information Systems Research. Retrieved from Https://Link.Springer.Com/Article/10.1007/S12599-017-0505-1.

Belasy, Samir Ibrahim. "What Do You Know about the Marketing Types B2C, B2B & B2H? - Bayt.com Specialties." Bayt.com, 13 May 2017, specialties.bayt.com/en/specialties/q/360616/what-do-you-know-about-the-marketing-types-b2c-b2b-amp-b2h/.

Bitcoin Magazine. (2018). Triple Entry Bookkeeping with Bitcoin. (Online) Available At: Https://Bitcoinmagazine.Com/Articles/Triple-Entry-Bookkeeping-Bitcoin-1392069656/

Blockchain: Understanding Its Uses and Implications. (2019). Retrieved from https://www.edx.org/course/blockchain-understanding-its-uses-and-implications

Brett, C. (2018, April 19). Track. Capital Triple-Entry Accounting Built on Blockchain -. Retrieved October 24, 2019, From Https://Www.Enterprisetimes.Co.Uk/2018/04/19/Track-Capital-Triple-Entry-Accounting-Built-On-Blockchain/.

Breuck, F. D. (2019, August 12). Get ready for blockchain in the supply chain – part 2 : FUJITSU BLOG. Retrieved from https://blog.global.fujitsu.com/fgb/2019-08-07/get-ready-for-blockchain-in-the-supply-chain-part-2/

Browne, R. (2018, October 1). Five Things That Must Happen for Blockchain To See Widespread Adoption, According to Deloitte. Retrieved from *Https://Www.Cnbc.Com/2018/10/01/Five-Crucial-Challenges-For-Blockchain-To-Overcome-Deloitte.Html*.

Chamria, R. (2018, August 2). How Can Blockchain Put an End to Fraud In Financial Transaction? Retrieved from https://www.sofocle.com/how-can-blockchain-put-an-end-to-fraud-in-financial-transaction/

Churchill, F. (2017, August 24). Unilever, Nestlé and Tyson join blockchain pioneers. Retrieved from https://www.cips.org/en/supply-management/news/2017/august/unilever-nestle-and-tyson-join-blockchain-collaboration/

Corda Enterprise - Blockchain Platform for Business. (2020). Retrieved from https://www.r3.com/corda-platform/

D, Yaga,P. Mell,N. Roby, And K. Scarfone, "Blockchain Technology Overview (NISTIR-8202)," October 2018. Published by The National Institute of Standards and Technology. Downloaded September. 5, 2019.

Deloitte. (2016). Blockchain Technology: 9 Benefits & 7 Challenges. (2017, January 12). Retrieved October 30, 2019, From Http://Blog.Deloitte.Com.Ng/Blockchain-Technology-Benefits-Challenges/.

Delvecchio, L. (2019, May 24). The Purchasing Cycle Explained. Retrieved from Https://Www.Purchasecontrol.Com/Blog/Purchasing-Cycle/.

Elegbe, W. (2018, October 28). Williams-Elegbe Delivers Inaugural Lecture on Public Procurement, Corruption and Blockchain Technology. Retrieved from Https://Africanprocurementlaw.Org/2018/10/25/Williams-Elegbe-Delivers-Inaugural-Lecture-On-Public-Procurement-Corruption-And-Blockchain-Technology/.

Frankenfield, J. (2019, October 5). Smart Contracts: What You Need to Know. Retrieved from Https://Www.Investopedia.Com/Terms/S/Smart-Contracts.Asp

Frankenfield, J. (2020, January 29) "Proof of Activity (Cryptocurrency)." Investopedia, Investopedia, www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp.

Gordon, D. (2019, October 1). Know the red flags of occupational fraud to protect your business. Retrieved from https://www.cpacanada.ca/en/news/atwork/2019-01-10-fraud-signs

Greene, Craig L. "McGovern & Greene Llp." EMPLOYEE FRAUDS - PURCHASING - McGovern & Greene Fraud Archives; Chicago, Las Vegas, 2019,

www.mcgoverngreene.com/archives/archive_articles/Craig_Greene_Archives/Focus-Employee_Frauds-Purch.html.

Grybniak, S. (2017, December 28). Advantages and Disadvantages of Smart Contracts in Financial Blockchain Systems. Retrieved from Https://Hackernoon.Com/Advantages-And-Disadvantages-Of-Smart-Contracts-In-Financial-Blockchain-Systems-3a443145ae1c.

Hamoni, R; McLaughlin, R; and Rice, F (November 2019). Building Canadian Consensus: Our Maturing Blockchain Ecosystem. Information and Communications Technology Council (ICTC). Ottawa, Canada

Iang.Org. (2018). Triple Entry Accounting. (Online) Available At: Http://Iang.Org/Papers/Triple_Entry.Html

Kamalia, A. (2019, November). (PDF) Blockchains Potential to Combat Procurement. Retrieved from Https://Www.Researchgate.Net/Publication/334524231_Blockchains_Potential_To_Combat_Procurement.

Kapoor, Shivaansh. "What Is PoC(Proof of Capacity)?" Medium, Medium, 4 Jan. 2019, medium.com/@shivaanshkapoor02/what-is-poc-proof-of-capacity-c85febb5d18e.

Kenton, Will. (2020) "Proof of Burn (Cryptocurrency) Definition." Investopedia, Investopedia, 5 Feb. 2020, www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp.

Lakshita L. (2018, December 6). Introduction to Merkle Tree. Retrieved from https://www.geeksforgeeks.org/introduction-to-merkle-tree/

Lastovetska, A. (2019, January 31). Blockchain Architecture Basics: Components, Structure, Benefits & Creation. Retrieved from https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

Little, S., & High, M. (2019, November 13). Blockchain Technology: What Internal Auditors Should Know. Retrieved from Https://Www.Crowe.Com/Events/Iia-Members-Only-Blockchain-Technology-What-Internal-Auditors-Should-Know-12-12-19.

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 254-269). ACM.

Maltaverne, B. (2018, April 25). Blockchain: what are the opportunities for Procurement? Retrieved from https://medium.com/procurement-tidbits/blockchain-what-are-the-opportunities-for-procurement-d38cfd5446fa

Mardus, Randall. “Blockchain Consensus Algorithms: An Early Days Overview.” Medium, Coinmonks, 22 Jan. 2020, medium.com/coinmonks/blockchain-consensus-algorithms-an-early-days-overview-2973f0cf49c6.

Markgraf, B. (2016, October 26). ISO 9001 Purchasing Procedures. Retrieved from https://smallbusiness.chron.com/iso-9001-purchasing-procedures-40107.html

Maslova, Natalia. "BLOCKCHAIN: DISRUPTION AND OPPORTUNITY." Strategic Finance, July 2018, P. 24+. Gale Academic Onefile, Accessed 2 Oct. 2019.

Meuwissen, S. (N.D.). The Impact of Blockchain Technology at Purchase to Pay. Retrieved from Https://Www.Academia.Edu/30176340/The_Impact_Of_Blockchain_Technology_At_Purchase_To_Pay?Email_Work_Card=Interaction_Paper.

Mulders, M. (2019, October 14). Blockchain-7 Benefits for The Financial Industry. Retrieved from Https://Hackernoon.Com/Blockchain-7-Benefits-For-The-Financial-Industry-E51f67a5cc05.

N. Szabo, "The Idea of Smart Contracts," 1997

Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-To-Peer Electronic Cash System" (PDF). Archived (PDF) From the Original On 20 March 2014.

National fraud Authority (2011, October). Procurement Fraud in the Public Sector - gov.uk. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118460/procurement-fraud-public-sector.pdf

Oden, C. (2018, October 3). The Impact of Triple Entry Accounting System on Financial Reporting. Retrieved from Https://Www.Projecttopics.Org/Impact-Triple-Entry-Accounting-System-Financial-Reporting.Html

P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz. Metrics for assessing blockchain-based healthcare decentralized apps, in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), 2017, pp. 1-4. https://doi.org/10.1109/HealthCom.2017.8210842

Parnell, G. (2017): How Blockchain Can Strengthen Supply Chain Links. Https://Theloadstar.Co.Uk/Guest-Blog-Blockchain-Can-Strengthen-Supply-Chain-Links

Pinkasovitch, A. (2019, September 12). Detecting Financial Statement Fraud. Retrieved from Https://Www.Investopedia.Com/Articles/Financial-Theory/11/Detecting-Financial-Fraud.Asp.

PwC now audits crypto companies. (2019, June 26). Retrieved from https://www.accountingtoday.com/articles/pwc-now-audits-cryptocurrency-companies

PWC, (2017) Blockchain: A catalyst for new approaches in insurance. Retrieved from https://www.pwc.com.au/publications/pwc-blockchain.pdf.

Ramos, J. (2017, June 29). Why Smart Contracts Won't Replace Contract Law. Retrieved from https://thedailycpa.com/2017/06/29/why-smart-contracts-wont-replace-contract-law/

Rosic, A., & Blockgeeks. (2019, August 23). Proof of Work vs Proof of Stake: Basic Mining Guide. Retrieved from https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Sandro Psaila (2017). Blockchain: A Game Changer for Audit Processes? Deloitte Malta Article

Shala, B., Trick, U., Lehmann, A., Ghita, B., & Shiaeles, S. (2019, May 11). Novel trust consensus protocol and blockchain-based trust evaluation system for M2M application services. Retrieved from https://www.sciencedirect.com/science/article/pii/S2542660519301234

Smith, P. (2015, April 24). Procurement and Supply Chain Fraud - OFS Portal. Retrieved from https://ofs-portal.com/wp-content/uploads/2016/04/OFS-Portal-White-Paper-on-Fraud-April-2015.pdf

Spoke, M. (2015). How blockchain tech will change auditing for good. Available at: https://www.coindesk.com/blockchains-and-the-future-of-audit/

Sreeperambudur, S. (2019, March 11). The Challenges Involved in Implementing the Blockchain Technology in Financial Industry. Retrieved from Https://Medium.Com/Datadriveninvestor/Challenges-Involved-In-Implementing-The-Blockchain-Technology-In-Financial-Industry-C87e5e9c9d9e.

Staff, S. (2019, July 3). What Are Smart Contracts and How Do They Apply to Fintech? Sila: Simple Banking and Payments API. Retrieved from Https://Silamoney.Com/What-Are-Smart-Contracts-And-How-Do-They-Apply-To-Fintech/.

Taylor, B. (2017, November 28). Triple-Entry Accounting and Blockchain: A Common Misconception. Retrieved from Https://Www.Forbes.Com/Sites/Forbesfinancecouncil/2017/11/28/Triple-Entry-Accounting-And-Blockchain-A-Common-Misconception/#4b608632190f

Timothy Leonard, Blockchain For Transportation– EVP Operations and Technology 2017 Data Visionary Americas Data Heroes Awards by Hortonworks WHITE PAPER

Triple-Entry Accounting. (2019, September 17). Retrieved from Https://Systemsinnovation.Io/Triple-Entry-Accounting-Articles/.

Wiatt, R. G. (2019, January 1). From the Mainframe to The Blockchain. Retrieved from Https://Sfmagazine.Com/Post-Entry/January-2019-From-The-Mainframe-To-The-Blockchain/.

Wikiwand. (2018). Single-Entry Bookkeeping System | Wikiwand. (Online) Available At: Https://Www.Wikiwand.Com/En/Single-Entry_Bookkeeping_System

Wu, J., & Xiong, F. (2019, July 23). Application of Internet of Things and Blockchain Technologies To Improve Accounting Information Quality. Retrieved from Https://Ieeexplore.Ieee.Org/Document/8769831

Yafimava, D. (2019, August 14). What Is Consortium Blockchains, And What Purpose Do They Serve? Retrieved from Https://Openledger.Info/Insights/Consortium-Blockchains/.

Zhang, Jian. "Deploying Blockchain Technology in the Supply Chain." IntechOpen, IntechOpen, 28 May 2019, www.intechopen.com/online-first/deploying-blockchain-technology-in-the-supply-chain.

Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, And Huaimin Wang (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends Conference Paper.