2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)
Amity University

Enhancing Privacy through "Smart Contract" Using Blockchain-Based Dynamic Access Control

Richa Gupta
Department of Management and Commerce
Amity University, Dubai, U.A.E.
rgupta@amityuniversity.ae

Vinod Kumar Shukla
Department of Engineering and Architecture
Amity University, Dubai, UAE
vshukla@amityuniversity.ae

Sindhu Suresh Rao
Department of Management and Commerce
Amity University, Dubai, U.A.E.
sindhu4s@outlook.com

Shaista Anwar
Department of Humanities, Arts and Applied Sciences
Amity University, Dubai, U.A.E.
shaista1046@gmail.com

Purushottam Sharma
Department of Engineering, Amity University, Noida, Uttar Pradesh, India
psharma5@amity.edu

Ruchika Bathla
Amity Institute of Information Technology, Amity University
Noida, UP, India
rbathla@amity.edu

Abstract: **Blockchain helps to deliver Computerized working, on spot verification, cost efficiency, enhanced work. One of the fast initiatives for the implementation of Blockchain is taken by financial sector. As more than 60% of the market percent of the market value focuses on new technology. In the coming time, blockchain will start into influence into many domain including accountancy on it auxiliaries. Smart contract can play a very important role in banking and insurance. This can be very vital tool for the auditing purpose, because all transactions can be updated without any third party interference. All the accounting standards can be evaluated through blockchain systems thus giving professional accountants such as Chartered Accountants and Certified Public Accountants to focus more on the company policies and how it can improve its operations ethically. To access any resource in blockchain network.This paper presents a framework which use Fair access using Dynamic Access control. All process of fair access is recorded in smart contract and token allocation can be done with the help of Digital Signature. This makes system more perfect. For the very purpose of Blockchain intervening into accounting policies is to ensure that auditors are working to the potential in terms of verifying the accounts and financial records in accordance to the International Accounting Standards. This step hopes to minimize minimal frauds that might happen in the workplaces which could halt to the end of the business life as the privacy of smart contract can be enhanced.**

Keywords—Blockchain, Smart Contract, FairAccess, Dynamic Access Control, Blockchain Auditing

I. INTRODUCTION

Block chain, as its name suggests, composed of numerous blocks suspended in series. May be defined as, "record-keeping technology, public ledger, distribution and decentralization" block chain is simpler to apprehend than the way it is defined. It is basically the digital information which is stored in the public database. Here, the digital information is Blocks and the database is Chain, which may be classified as: The blocks store information about the date, time and amount transactions made. Using a digital signature or user ID customer's details and information is stored in the Blocks. Selective information is stored by the Blocks that differentiate them from other blocks, exactly the way we all have different names for our identification. Every block stores a new code called a "hash" that makes it different from other Block. [1]

II. BLOCKCHAIN MARKET WORLD WIDE

The predictions propose that the blockchain technology will face gigantic growth in the years to come. The market growth as per the statistics shows that the hike will be more than 23.3 billion U.S. dollars in scope by year 2023 (Fig.1). One of the fastest initiatives is taken by the financial sector for investing in blockchains as more than 60% of the market percent of the market value focuses on new technology. [2]

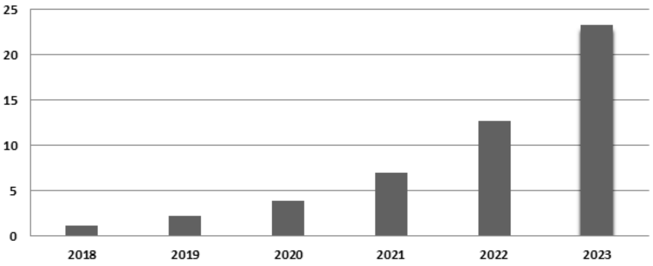

Fig. 1. Size of the Blockchain technology market in Billion US Dollars

III. WORKING OF BLOCK CHAIN

There must be a transaction against purchase to start the Block Chain. This transaction is then verified and stored in the next block. After the accurate verification it is highlighted with a green light and a unique identification code called "Hash" is issued to the recent Block. This block is then added to the chain. As soon as the block is added to the chain it can be viewed by everyone. Though block chain contents are visible to all, the consumers can connect their computers to the network of blockchain, this will automatically update the block chain whenever a new block is added. Every computer that is a part of Block Chain network has a copy of its own, which means there is an existence of millions of copies for

978-1-7281-0666-3/20/$31.00©2020IEEE

same Block chain, in spite of millions of identical information; it is more difficult to hack or manipulate it. As every copy has to be changed in the Blockchain network. In spite of the information being visible to the public, block chain technology is secured and trusted, all new blocks created are stored in a sequential order i.e.; it is added at the end of the chain. After the block has been added at the end (Fig.2), it is not possible to go back into other blocks to alter the information as they have the "Hash" code, which is created by a mathematical algorithm that converts digital information into a string of alphabets and numerical digits. The hash code changes if any information is edited. However, as this is a complex equation, it is impossible to go back and reverse the process. Thus, Block Chain is secured, trusted and confidential. We have understood from the above Block Chains may support in storing data on monetary transactions [3].

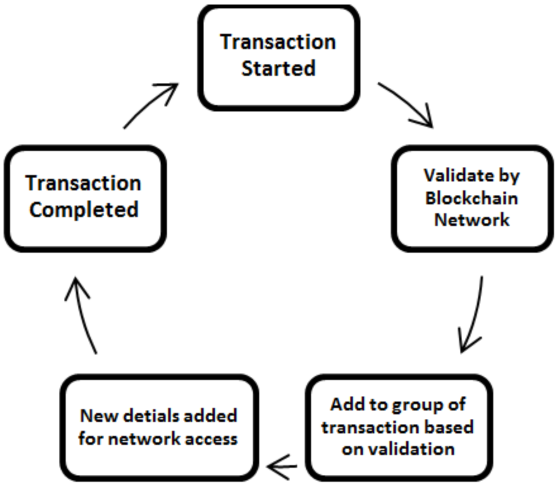
Transaction Started
Validate by Blockchain Network
Add to group of transaction based on validation
New detials added for network access
Transaction Completed

Fig. 2. Adding Transaction in Blockchain Network

The concept of blockchain innovations are the mix of many sub process, like Cryptography, computer science, Algorithm and monetary model, to make the one system of blockchain [4].

IV. Benefits of Blockchain

Tokenization: Any company's assets either liquidated or long-term can be paired corresponding to a token in the digital world. Simply means that, all assets are now identified by a digital token.

Supports audit trail: Audit trails are an IT feature which enables auditors to have a bird-eye view of all the transactions from its origination to the final statements. In the case of blockchain checking of audit evidences are done in real-time basis henceforth now auditors need not just limit to samples.

Smart contracts: A highlighting feature, executing transactions by itself on the basis of few pre-stated conditions and if and only of they were satisfied, the transaction would be automatically verified by miners of the network.

Eliminated red-tapism: Now that transactions happen on the real-time basis, related miners in the network can verify the transactions quickly and also check the figures from time to time to ensure a transparent trading.

*Economyshared***:** The peer-to-peer and decentralized nature of blockchain removes the need for centralized control of power such as Airbnb and Uber to facilitate the sharing economy.

V. Smart Contract

Blockchain systems have made professional life an ease for mediating in many fields. Especially in the field of accounting it aims at improving the efficiency, quality and assurance in the maintenance of records leaving no possible loopholes for criminal thoughts to execute. With the help of smart contracts, a unique feature of blockchain introduced by Nick Szabo the year 1994 helps in transferring assets, property, ownership rights and so forth through standalone orders when the pre-determined algorithm or the conditions are fulfilled.

Plugging in the concept of "Provisions" into smart contracts will enhance this system very applicable to all range of firms operating, as accounting and finance is the heart of any firm.

VI. Literature Review

Uniqueness in Blockchain: Following characteristics(Fig.3.) makes blockchain more unique.

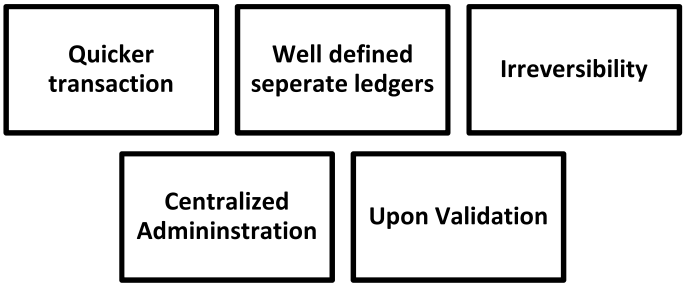

Fig.3. Uniqueness in Blockchain

Quicker transactions: Through blockchain systems monetary transactions can now happen in real time basis which means there is no loop hole for non-payment and the whole lump sum amount can now be transferred to the buyer at once.

Distinguished ledgers: In a system, in one blockchain unit, various parties who partake in the business of the firm are included. Each of these parties are responsible for at least one transactions. And when one transaction occurs all parties within the unit can view the transaction which makes it public history.

Irreversibility: Once the transaction is set into the blockchain a confirmation validation will pass on to all the parties who are in the block. This confirmation ensures that there is no repetition or changes in the figure for one's interest.

Centralized administration: There is no authorized body that controls the unit as it is just the digital system that leaves no power or authority to any entity present in. This prevents human errors or if the managing authority to falsify transaction figures.

Upon validation: Only when each party verifies the happening of the transaction that is through digital signature a block is created for the transaction.

Blockchain Based Smart Contract: Smart Contract is a digital agreement that pedals operator's digital resources, communicating the contributor's responsibility and rights, which will mechanically be performed by the system. Apart from it being a part of computer process, it can be also expressed as a contract contributor, which will respond to message what it receives and data is stored. Smart Contract is like an individual can be reliable and hold assets transitorily following the order which has already been programed. A smart contract is a self-implementing settlement installed in PC code directed by a block chain. The code contains a lot of instructions and guidelines under which the gatherings of the smart contract approve to connect with one another. Block chain Products brings results in investments to improve our world in many ways [6].

"Smart Contract" can defined as a transaction which is computerized that helps to execute the terms of a contract (Szabo, 1997). This proposal has been for a long time but has now come to practice along with blockchain. These days' smart contract podiums are evolving and becoming popular. This system could be used for many capacities like, IoT and banking services [7].Smart contract can be categorized in 2 types: evaluation and development where, evaluation is analysis of codes and performance and development is process of development of smart contract [8].

Smart contract manages agreements between users and also helps providing services to other treaties. It also helps to store information in regards to the application like, registration of territory and membership records.

According to H. Yining at el, stated that, smart contracts are getting into minds of many in the present era, introduced into public and private sectors as they give a feasible platform for them to operate in public and permissioned blockchains this in turn boost efficiency, encourage firms into transparent dealings[9].

Smart contracts, are still in the R&D stage and are currently being explored to its fullest potential and in the coming years, the future will be spun around the engineering of the smart contracts delivering a wide array of mutual benefits to its operators.

According to Maher Alharby, the functionality of smart contracts enables to execute standalone orders automatically upon the agreements also discusses the current status and its usage of smart contracts onto blockchain technology which encourages various unknown partners to enter into business dealings. (Eg; Ethereum Blockchain)

Revival of Smart Contract: The execution of smart contracts has been more feasible through the concept of blockchain over the beneficial functions that enables automated oversight administration of the agreements between the participating members (miners).
The miners then could transfer information and other assets through the smart contracts which would then verified by the smart contracts on basis of the agreements and release the output to the receiving party. On the other side if the stated agreements upon which the information of the asset has not been identified or if not compatible with the agreements, the output is not released.

Every detail of the contract between parties is clearly embedded into the blockchain systems therefore preventing fraud from either side of the transaction [10].

According to Konstantinos Christdis and Michael Deventsikiotis in their research paper state that, the concept of smart contracts resides in the world of blockchain, because smart contracts is functionality that operates for blockchain to enchance inter-miner dealings, aided by crypto-signatures verifiability. With the mandatory digital signature verifications, business can transfer assets and information between distrustful companies. Since this feature of blockchain enables prevention of fraud, therefore leads to much lesser scope to corporate disputes in conclusion, gives no disagreeability from the participants in the future [11].

According to Martin von Haller Grønbæk, Partner, Bird & Bird Copenhagen, his published article points out that theoretically, blockchain can be fully implemented and explored to the extreme limits but implemented in reality can be a sophisticated affair. At the same time, other manual costs can be avoided such as, trust-gaining time cost between the parties of the business dealing, decreases transaction costs.

Though smart contracts are can be driven out of few agreements and possible situations of a business transaction but he highlights the point that all business dealings do not go as per scripted or benchmarked conditions. The occurrence of various contingencies that happen in a transaction may leave this system without a solution or a response [12].

According to the article published by smart contracts alliance in partnership with Deloitte enumerate various benefits such as, monitoring letter of credit, fraud prevention and reduction due to proper accounting and transfer of financial assets, enables companies to pay out dividends and stock splits more accurately, removal of intermediaries and various operational risks attached with this conventional business, huge businesses with numerous transactions can now be easily traceable and its auxiliary information can also be reviewed.

These functions will include various companies of all nature and types to be a part of such a system which will operate the future of business [13].

VII. Issues and Challenges with Blockchain-based Smart Contract

Performance: A clear restriction of using smart contracts for digital agreement is that low operation output effects in great underdevelopments within the interval that it takes to complete a contract.
Privacy: as the nature of the device is public blockchain which means anybody can access or view these transactions the privacy of the transaction is no there [14].
*Impact of Bugs in Smart Contracts:*When compared to the conventional software, smart contracts cannot be directly mended once installed which brings an exceptional set of limitations while smart contracts are designed[15].
Ethereum: This is an open cradle blockchain podium in combination with Smart Contract which offers distributed computer-generated mechanism to handle the contract, with the use of its digital currency called ETH, individuals can produce many various services, contracts or applications on this podium [16].In spite of the fact that blockchain has become very popular, it has a few points we have to see, a few issues has just been improved alongside new method's creating on application side, getting increasingly develop and stable. The administration need to make relating laws for this innovation, and endeavor should prepared for grasp blockchain advancements, forestalling it carries an excess of effect to current framework. When we appreciate in the upside of blockchain advances bring to us, in a similar time, despite everything we need to remain careful on its impact and security issues that it could be have [17].

VIII. IOT enabled Smart Contract

IOT enabled blockchain-based smart contract is one of the most informative techniques of communication in the recent years. IoT is projected to assimilate the smart contracts into the internet and offers consumers with innumerable services [18]. It has in recent world grabbed the attention of stakeholders across a many businesses, finance, healthcare, utilities real estate and many more. The transformation to decentralized network may not be always easy and positive or even at times blockchain is not able to fulfill the requirements of the applicants. Smart contract and blockchains bring in bags of adavantages along with limitations.A regionalized construction for the extensive IoT scheme is to support the ecosystem and be sustainable.

The incorporation of IoT with blockchains permits for a like to like options where technologies can buy and sell mechanically [19].Use of blockchain in financial transaction tracking: Different highlights of Blockchain, for example, decentralization, changelessness, and straightforwardness make it engaging for business divisions and spaces all over the world. One such industry that is driving the route in investigating the capability of blockchain is the financial transaction tracking. [20].

IX. Disruption - Blockchain in Banking

The blockchain technology can possibly disturb the banking and fund division of recent times. A couple of manners by which blockchain can change the present face of the financial business are as per the following:

Reduction is fraudulent Activities: wherever there is involvement of cash chances for fraudulent activities may arise. This leads to the practice of money management through more reliable systems. Blockchain system can be secured and non- corruptible system which is distributed and no casual disaster. Every transaction made is stored in the form of block with the cryptographic device which is challenging to destroy [21].
Know Your Customer: Costs for Banks and financial institutions are increasing which is a concern for them. When they adopt the blockchain system, the autonomous proof of for each customer by one bank or financial party would be reachable by other financial groups to practice so that the Know Your Customer process need not be restarted or done again [22].
Smart Asset: Professional finance sometimes become really challenging when trades and transactions which is in the state of asset has to stamped with clear date and time. Globally Supply involve a lot countless bodies and constituents that are traded endlessly. This involves loads of paper documentation and time. This can be easily maintained and stored through Blockhain which can hold these records of smart assets in digitized format easily updated when required [23].
Smart Contracts: These contract applications are significantly viable for the banking and finance sector. This smart contract is a piece of code which can be self-executed and runs at the point when certain conditions composed on it are finished. It also helps in speeding and simplifying the financial transactions ensuring the information in the transaction is accurate and approved only when the codes meet. [24]

Trade Finance: Blockchain can be one of the most useful applications for the trade finance in the banking sectors. All difficult transactions can be worked on the blockchain network and can be shared easily with the importers and exporters. When certain predefined states of the arrangement are met, the keen contracts will consequently execute themselves and the particular gatherings can see every one of the activities performed [25].

X. Framework for Securing Smart Contract using Dynamic Access Control

FairAccess: This is a token based access model for accessing resources by using Blockchain technology. Digital Signature, act as tokens which are used to define access rights of a resource. It is difficult to forge the digital signature, in Blockchian network, as it creates a database of requesting person, requested resources, token used, token issued, which also helps in auditing process. The entire process of allocating a resource is done by using Smart Contract. [26]

Transaction is added in network, only when this is validated by blockchain network. And Finally added to Blockchain network so that this can be access by everyone available in that network, based on allocated permission.

*Dynamic Access Control:*While accessing the resources, smart contact need to be regularly checked and validated every time on each request (Fig.4). Once a new request has been made, this is immediately sent for validation by blockchain network. Blockchain Network checks for multiple things inducing request validation, policy which is already available related to resource requested. Once validation is successfully completed, then relevant updates are done in smart contract and which is further updated to user who has requested. In case any policy to access the resources is modified, also get recorded in Smart Contract [27].

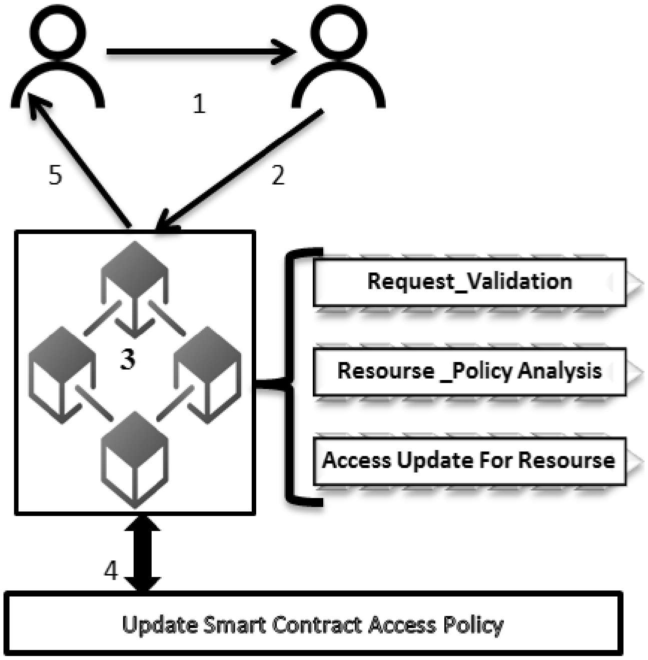
1
5
2
3
Request_Validation
Resourse _Policy Analysis
Access Update For Resourse
4
Update Smart Contract Access Policy

Fig. 4. Logical diagram for Dynamic Access Control
1= User Request | 2= Sent to Blockchain network
3 = Blockchain network (Check for request validation, Check for resources related policy, update Access policy
4 = Update Smart Contract Acess | 5 = Update user

XI. Limitation of blockchain

Complexness: The story is not just limited to easy creation of blocks and a simple validation, the prior application of these systems, decisions and implementation of the technology to be adopted into organizations must also equip its employees to cope up with the same. Along with this, the working of this system requires heavy digital connections and technical aspects making this system quite a headache.

Vast networks: Huge corporate can have several miners with the permissioned blockchains, this implies that, several transactions would lead to several public and private keys to remember. If one is lost, the transaction will be incomplete.

*Human error:*Manual entry of figures and the nature of the transaction could invite human errors and intentional errors while uploading it into the network. This is cannot be easily eliminated as it is human nature and manual entry must be audited carefully.

*51% Attack:*This a problem notified by the founder of bitcoins, Satoshi Nakamoto, stating that, a miner holding more than 51% of the share of power in the network, he can therefore look after the transactions in his way according to his will and therefore this power might soon serve him as his advantage over the network. In other words, Someone who holds majority of percentage in participation within the network also holds authority and there could manipulate records according to their will.

*Pricely affair***:** Though the transaction costs are nearly less, the implantation, adoption and training could cost pricy and might consume time as well. Although many firms are moving towards adoption and it is estimated that the transaction costs could also move up.

XII. Conclusion

In conclusion of above study, privacy of smart contractsa help to reduce corporate frauds, which can further result for:

1. Better internal audit control, introduction of Blockchain
2. Enhancing business ethics of the organization’s climate
3. Random inspection and government intervention in intervals to prevent such frauds
4. Data analytics and predictive analysis for risk assessment.
5. Cyber security measures fraud awareness training program for employees.
6. Cryptocurrency- Paper money less transactions to ensure digital traces of transactions.

Block chain is a growing system emerging into industries assuring the trust of a transparent operation by keeping in loop of all members related to the organization by the way of crypto signatures.

References

[1]. Rechtman, Y. (2017). Blockchain: The Making of a Simple, Secure Recording Concept. CPA Journal, 87(6), 15-17.

[2]. Statista, "Blockchain technology market size worldwide 2018-2023", L. Shanhong, [Online]https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/

[3]. Lin. I. and Liao.T, "A Survey of Blockchain Security Issues and Challenges", "International Journal of Network Security 19(5):653-659", September 2017

[4]. Garay. J, at el., “The Bitcoin Backbone Protocol: Analysis and Applications”, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[5]. Gervais. A.,at el., “Is bitcoin a decentralized currency?,” IEEE Security Privacy, vol. 12, pp. 54–60, May 2014

[6]. Kosba. A,,at el., “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,”in 2016 IEEE Symposium on Security and Privacy(SP’16), pp. 839–858, May 2016.

[7]. Governatori, Guido; Idelberger, Florian; Milosevic, Zoran; Riveret, Regis; Sartor, Giovanni; Xu, Xiwei (2018). "On legal contracts, imperative and declarative smart contracts, and blockchain systems". Artificial Intelligence and Law. 26 (4): 33.

[8]. Buterin, V. (2014) A Next-Generation Smart Contract and Decentralized Application Platform, White Paper

[9]. H. Yining at el., "Blockchain-based Smart Contracts - Applications and Challenges", Project: Towards Digital Paradise (TDP)

[10]. Andrea M. Rozario and Miklos A. Vasarhelyi, "Auditing with Smart Contracts", "The International Journal of Digital Accounting Research", Vol. 18, 2018, pp. 1-27, ISSN: 2340-5058
[12]. KONSTANTINOS CHRISTIDIS and MICHAEL DEVETSIKIOTIS, "Blockchains and Smart Contracts for the Internet of Things", "SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN INTERNET OF THINGS (IoT)", IEEE Access

[11]. Martin von Haller Grønbæk,"Bird & Bird Copenhagen", "Blockchain 2.0, smart contracts and challenges" [Online] https://www.twobirds.com/~/media/pdfs/in-focus/fintech/blockchain2_0_martinvonhallergroenbaek_08_06_16.pdf

[12]. "Smart Contracts Alliance — In collaboration with Deloitte", "Smart Contracts: 12 Use Cases for Business & Beyond A Technology, Legal & Regulatory Introduction — Foreword by Nick Szabo" [Online] https://www.perkinscoie.com/images/content/1/6/v2/164979/Smart-Contracts-12-Use-Cases-for-Business-Beyond.pdf

[13]. Cai Y, Zhu D (2016) Fraud Detections for Online Businesses: A Perspective from Blockchain Technology. Financial Innovation

[14]. Lemieux V (2016) Trusting records: is Blockchain technology the answer? Rec Manag J 26(2):110–139

[15]. Watanabe. H., at el.,“Blockchain contract: Securing a blockchain applied to smart contracts,” in IEEE InternationalConference on Consumer Electronics (ICCE’16),pp. 467–468, Jan. 2016.

[16]. Divyakant Meva, “Issues and Challenges with Blockchain: A Survey”, “International Journal of Computer Sciences and Engineering”, Vol.-6, Issue-12, 2018,

[17]. Atzori, L., Iera, A. and Morabito, G. (2010) ‘The internet of things: a survey’, Computer Networks,Vol. 54, No. 15, pp.2787–2805.

[18]. Konstantinos Christidis ; Michael Devetsikiotis Block chains and Smart Contracts for the Internet of Things Publisher: IEEE; PP 2298.

[19]. Georgia State UniversityScholarWorks @ Georgia State UniversityBusiness Administration Dissertations Programs in Business AdministrationSummer 8-1-2018 The Impact of Blockchain Technology on FinancialTransactions pp; 24-25

[20]. December 2017, Volume 59, Issue 6, pp 441–456| Cite as A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services Authors Authors and affiliations Hissu HyvärinenEmail authorMarten RisiusGustav Friis

[21]. Preventing Money Laundering or Obstructing Business?: Financial Companies' Perspectives on ‘Know Your Customer’ Procedures Martin Gill, Geoff Taylor The British Journal of Criminology, Volume 44, Issue 4, July 2004, Pages 582–594, Published: 08 April 2004

[22]. Yoo, S. (2017), "Blockchain based financial case analysis and its implications", Asia Pacific Journal of Innovation and Entrepreneurship, Vol. 11 No. 3, pp. 312-321. https://doi.org/10.1108/APJIE-12-2017-036

[23]. Lawrence J., TrautmanPrairie, “The Consumer Finance Law Quarterly Report 232 (2016)”, View A&M University - College of Business

[24]. Blockchain based financial case analysis and its implications Soonduck Yoo Asia Pacific Journal of Innovation and Entrepreneurship ISSN: 2398-7812 Publication date: 4 December 2017;(3.2.2)

[25]. A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy-preserving access control model based on blockchain technology in IoT,” in Europe and MENA Cooperation Advances in Information and Communication Technologies, Springer, 2017, pp. 523-533.

[26]. A. Outchakoucht, E. S. Hamza, and J. P. Leroy, "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things," in International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 7, 2017, pp. 417-424.

[27]. Tsai, W.-T., Blower, R., Zhu, Y., & Yu, L. (2016). A System View of Financial Blockchains. 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), 450.