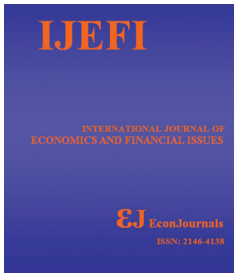


International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2020, 10(3), 166-173.

A Proposed System for Securing Cryptocurrency Via the Integration of Internet of Things with Blockchain

Atef Ghalwesh, Shimaa Ouf, Amr Sayed*

Business information system, Helwan University, Egypt. *Email: amriano92@yahoo.com

Received: 19 December 2020 Accepted: 12 March 2020 DOI: https://doi.org/10.32479/ijefi.9130

ABSTRACT

Nowadays the world discuss the problem of the cryptocurrency and shows several risks in dealing with this new investment or banning it by governments and the main issue of this paper is how can the third part ex: (exchange market for trading cryptocurrencies) avoid cybercriminal activities, In this paper, we will define only two of cybercriminals that related to the third part directly, First: Ransomware attacks and how the process of storing cryptocurrencies can be secured. Second: Black net in which many illegal trades could be done and how can the third part (governments) monitor the relationship between buyers and sellers to avoid this problem. In this paper, we propose a framework that proposed in anew exchange market by integrating blockchain technology and IOT (internet of things) to increase the security in the two processes that consider the main issues for the exchange market: first: storing the cryptocurrencies securely and avoid ransomware attacks, second: monitoring the transactions and avoid illegal business (black net) could happen through it. And we can implement this framework for special types of partially decentralized cryptocurrencies ex: NEO and Libra coin.

Keywords: Cryptocurrency, Hyperledger, Ransomware, Black Net, Blockchain, Internet of Things
JEL Classifications: E58, M15, K22

1. INTRODUCTION

This paper makes up a relatively new area which has emerged from countries which are beginners in the market of investing cryptocurrencies and they refuse it because of several reasons and specially the missing of security and the ability to be under cybercriminals attack threats. Although it's highly profit comes from investing cryptocurrency and its advantages in speed for transferring money and decentralization.

Because of this debate between accepting the cryptocurrency or denying it in many countries, the scientific research should have a big role in studying and analyzing cryptocurrency Issues.

This paper considers the field of securing the cryptocurrency as the main subject of its study and one of the major topics investigated in this field is how to monitor the relationship between the buyer and the seller and how to avoid money laundering through their transactions or black net.

Most of the theories of cryptocurrency focused on explaining the ransomware virus which can control your wallet or encrypt it and the user has to pay for hackers to get it back.

This seems to be a common problem in trading cryptocurrencies which called (cyber-criminal activities) and it comprises six types of hacking:

1. Ransomware.
2. Crypto jacking.
3. Ponzi schemes.
4. Exchange hacks.
5. Black net.
6. ICO frauds.

The main two problems are Ransomware and Black net. Because it consider the main issues for the third part and how can we store cryptocurrency securely and avoid ransomware attacks and how to monitor the relationship between investors and transactions and how to avoid illegal business.

This seems to be a common problem in storing the wallet which contains the cryptocurrencies for each user and this issue allowed the ransomware virus to appear that storing the wallet in the hardware of the PC could be encrypted by hackers with ransomware virus.

And also the main practical problem that we discuss is black net that in case of trading cryptocurrencies through the exchange market. Although you are playing the role of the third part between the buyer and the seller but you can't define any of them or know any personal information about the users.

1.1. Ransomware

Ransomware attacks are a kind of malware attack which encrypt all files in your computer. A key that needed to decrypt the files which provided only after a specific amount of "ransom" paid to the attacker. This "ransom" is the form of cryptocurrencies (Figure 1).

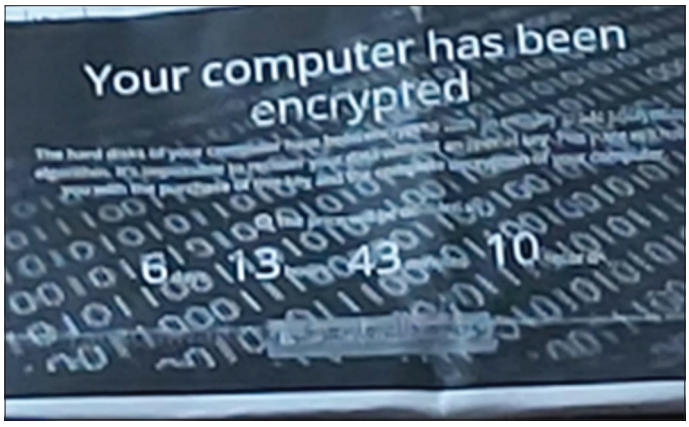
With cryptocurrency payments. These attackers get impossible to track down and might attack anyone in the world with ease (Paquet-Clouston et al., 2019).

1.2. Black Net

The dark –web is a part of the internet which has gained a mythical statues over the years. Almost every trading platform on the dark- web accepts cryptocurrency payments. these website are involved in everything from drug and weapon trade to even the sale of endangered animals and human organs cryptocurrencies have become the favorite means of payment on the dark – web because it allows the traders as well as the buyers to remain highly anonymous. Many governments have expressed their concern that cryptocurrency funding the drug trade or sponsoring terror activities (Brenig, 2015).

In practical no study to our knowledge has considered add a hundred of percent more than 49% of security.

Figure 1: A sample of ransomware attack



There has been less previous evidence for discussing how can the third part play his role and save keeping the decentralized and the privacy of cryptocurrency at the same time moreover, few studies have focused on implementing tokens in order to save the currencies in the wallets.

However, anti-money laundering control has rarely been studied directly. But only a few studies have shown how to follow the steps of previous transactions through a tangle in order to make a history of each wallet in order to give analysis of all trades and transactions to our knowledge, no study has yielded the integration of blockchain with IOT, and some of them used IOT and some used Blockchain but there is no previous research using the hyperledger approach to build up a new currency with a higher security that integrates IOT with Blockchain.

One way to overcome these problems is to implement an integration of blockchain and IOT interface which could be under control of the central bank to monitor the relationship between the buyer and the seller dealing with the currency but it wouldn't be implemented through cryptocurrency such as bitcoin or Etherum because of its nature which depend on data base distribution across a peer- to-peer network and without a central authority in this research, we will analyze two of cybercriminal activities that called (ransomware and black net).

And propose a system by integrating IOT with blockchain in order to achieve.

Security and monitoring the transactions to control the process of buying and selling cryptocurrencies.

To overcome this problem in section 3 we demonstrate a solution of 50% privacy and decentralized cryptocurrency which could be attractive to a large number of new investors who are afraid of cryptocurrencies risks and also could prevent problems occurred such as ransomware because of its highly security. And problem of black net because of the ability to monitor and control the relationship between all parties in the transaction.

1.3. What is Hyperledger?

Hyperledger is an open source development project to benefit an ecosystem of hyperledger based solution providers and users – it is focused on blockchain related use case that will work under a variety of sectors.

For this study it was of interest to investigate the integration of blockchain with IOT in order to achieve a higher security.

To illuminate this uncharted area, we examined currencies would be acceptable for this integration and alternative of bitcoin and etherum and we have investigated the effect of the integration between blockchain and IOT and found it would provide more security for storing the cryptocurrencies and monitoring the relationship between all parties through every transaction.

And it would be of special interest to encourage new investors to trade with this new cryptocurrencies through secured exchange markets and avoid a lot of risks.

We there for analyzed the nature of crptocurrencies such the privacy and decentralized, annominity and issues and investigate whether it could be traded under the umbrella of this integration or not.

And to examine the impact of these cryptocyrrencies, we tested sample of them such bitcoin and Etherum but found it could be difficult to change their nature of privacy.

One of the primary benefits of this integrated approach between blockchain and IOT is the authorization and authentication in the process of accessing and the highly security in the process of storing the cryptocurrencies and the ability to monitor the relationship between the buyer and the seller by the central bank as a third part between users through every transaction.

And this gives significant advantage because it can encourage many people to invest their money without high risks through this exchange market or this new kind of cryptocurrency.

The benefit of using the integration of blockchain and IOT is expected to be more secured to deal with cryptocurrency and solve several problems and avoid money risks.

The additional advantages of using this integration is that it results in a number of new investors of new investors will enter this field of cryptocurrency after increasing the security and the feeling of their money will be in safe through this new system.

2. RESEARCH METHODOLOGY

The following electronic scientific databases were searched to provide a full bibliography of research papers on cybercriminal activities and its role in attacking the cryptocurrency.

The search process to find research papers that related to cyber-criminal activities problems. And its role in cryptocurrency was performed on the top 3 scientific databases. The search was performed based on five keywords: ‘‘cryptocurrency + cybercriminal activities + IOT + blockchain” We take only papers that were truly related to our research.

By searching on the following scientific database: by refined years only from (2015 to 2019)

And (Articles only)

IEEE Library: Found about 75 results only 7 of them in the scope.

Science Direct: Found about 40 results only 15 of them in the scope.

Springer Link: Found about 35 results only 4 of them in the scope.

In addition to 4 other articles which related to cryptocurrency in Banking. From 2012 to 2016. By searching in Google scholar for references with key words (Banking + cryptocurrency).

We selected 30 articles on cryptocurrency’s problems from 3 libraries published between 2015 and 2019. And the results were analyzed to identify the solutions and limitations that covered the cybercriminal activities and different models and algorithms they used to solve these limitations.

And made lots of analysis about the different types of cryptocyrrencies and how can the third part play his role in the processes of storing and monitoring and found that NEO and Libra coins could be suitable to deal with the proposed exchange market.

3. LITERATURE REVIEW

In this session we categories the previous studies into two ways:

1. Researches discussed the problems of cybercriminal activities and their proposed solutions for missing of security.
2. Researches discussed the problem of accepting the cryptocurrency legally or banning it.

3.1. Cybercriminals in Related Work

Bray in (2016) showed that cyber-crime has increased and anonymity plays a big role in acts of cyber-crime and how it could allow the user to bounce their IP address over multiple users and access the black net and how cryptocurrency could use a medium of exchange online that allow buyers and sellers to remain anonymous when completing transactions and recommended that analyze all cyber issues must and understood this will allow for policy makers, low enforcement, and the intelligence community to better combat cyber-crime and cyber terrorism (Bray, 2016).

Steven David Brown in Romania (2016), talked about cybercriminals and how its distinctive characteristics of decentralization and pseudo-anonymity are also attractive to criminal actors and it had assessed as represented only a low money laundering risk and showed an example of public electronic payment console in which requires longs in at least once every 3 weeks or the account would be locked and also registration requires a minimum of personal information and the machine prints out a paper receipt showing the date and time but it would be workable to launder much larger sums using different consoles and different email addresses (Brown, 2016).

Christian Brenig in Germany (2015), discussed the problem of money laundering (Black net) in cryptocurrency and explained money laundering process such as drug trafficking, kidnapping and arms smuggling and how can anti money laundering controls implemented and compared its related factors and the percentage of acceptability of it and the roles of intermediaries administration and its authentication level with blockchain and its flexibility with transaction fees and the role of trusted third part in payment processing but it needs extra research to be conducted in the light of the interconnections in the other disciplines such as computer science and legal studies (Brenig et al., 2015).

Fabio Spagnolo in London (2019), used amarkov-switching non-linear specification to analyze the effects of cyber-attacks on returns with cryptocurrency (Bitcoin, Etherum, Lite coin and stellar) over period 2015-2019 and suggested the existence of

significant negative effects of cyber-attacks on the probability of cryptocurrency staying in law volatility regime (Caporale et al., 2019).

Conti (2018), presented a study of twenty recent Bitcoin ransomware cases along with their renamed re-banded versions and proposed a framework to identify, collect and analyze Bitcoin addresses that belong to cybercriminals behind the ransomware and reported the characteristics and functionality of the ransomware and suggested other future research to extend the identification to other cryptography–based cryptocurrency and investigate the ransoms extorted via other payment options (Conti, 2018).

Masarah Paquet Clouston in Canada (2019), showed a data-driven method for identifying and gathering information on Bitcoin transactions related to illicit activity based on foot-prints left on the public blockchain and implemented this method on-top-of the graph sense open-source platform and applied to analyze transactions related to 35 ransomware families. And found that the market skewed with only a few numbers of players responsible for most of the payments and helped policy makers and law enforcement agencies to use this statistics to understand the size of the illicit market and make informed decisions to force this threat (Paquet–Clouston et al., 2019).

Poon and Dryja in (2016), discussed the Bitcoin protocol payment system showing its Blockchain scalability problem and a network of micropayment channels could solve scalability with its hashed time lock contract (HTLC) and key storage and showed the predicted blockchain transaction fees for bidirectional channels and the payment to contract and how could the lightning network be in the Bitcoin and its risks with a network of instantly confirmed micro payment channels whose payments are encumbered by time locks and hash block outputs (Poon and Dryja, 2016).

Huideny in China (2018), discussed the cyber-criminal issue of initial coins offering (ICOs) and provided anon-exhaustive classification of the legal statues of ICOs, and analyzed ICOs benefits in low costs and how requirements and profit liquidity with efficiency reliability and anonymity, investor protection and risks found it unclear about the Chinese government investors against fraudulent projects (Deng and Huang, 2018).

Jain Lin in Finland (2016), explored the solution space of enabling the fair exchange of cryptocurrency payment for a receipt and identified the timeliness of the exchange for a fair payment-for-receipt protocol imitations that leverage functionality of the block chain to achieve strong timeliness and compared security and efficiency of the two protocols and tested the results and found that the fair payment protocol based on blockchain–based is more cost and time effective than the protocol–based signatures otherwise it had any exceptions (Liu et al., 2018). Summary of previous studies are presented in Table 1.

3.2. Researches about Accepting the Cryptocurrency or Banning it

Winston Moore and Stephen in Barbados (2015), examined the potential role of cryptocurrencies as part of the portfolio of the external assets held by a central bank by using historical performance of the various exchange rates and using a relatively small portfolio composition of Bitcoin and found that digital currency is not likely to exceed 10% of all transactions in the short run and recommended that if Bitcoin incorporated into the portfolio for foreign balances of the central bank of Barbados that its share be relatively small (Moore and Stephen, 2015).

Joseph Bonneau in USA (2015), analyzed the perspectives and challenges for Bitcoin and cryptocyrrencies and provided a systematic exposition Bitcoin and the many related cryptocyrrencies and identified three key components of Bitcoin's design and properties and future stability, and found that there is no scientific model with sufficient predictive power to answer questions about how Bitcoin or related systems might fare with different parameters or in different circumstances (Bonneau et al., 2015).

Charles Evans (2015), analyzed the compliance of distributed autonomous block chain management systems (BMS) like Bitcoin also related to as (virtual–currencies) and its role in Islamic banking and central banks and it realized anew unit of XBT in exchange for the provision of services to maintain the security and stability of the Bitcoin network (Evans, 2015).

DeVries (2016), analyzed strengths, weakness, opportunities and threats of Bitcoin and compared it with other cryptocurrencies for 2014, 2015 and 2016 and predicted that it might hold a place for cryptocurrency as major currency solution and Bitcoin would help to pave the way for those currencies to flourish and also the blockchain technology that acts as Bitcoin's backbone has potential in other ways such as smart contracts (DeVries, 2016)

Andrew Philip (2017), motivated by the unique characteristics found in cryptocurrency data, which are drawing media and academic attention. And showed cryptocyrrencies exhibit long memory, leverage, stochastic volatility and heavy to validness in data analysis and also contributed deeper understanding surrounding cryptocyrrencies for the upcoming regulators and governments (Phillip, 2018).

Caporale in London (2017), examined persistence of the four main cryptocyrrencies and its evaluation overtime by using R/S analysis and fractional integration long-memory techniques and found that cryptocurrency market is still inefficient most times and advised that trend trading strategies can generate abnormal profits in cryptocurrency market (Caporale et al., 2018).

In other hand, Jousha Hendrickson in USA (2017), used a monetary model with endogenous search random consumption preferences to consider the extent to which a government can ban an alternative currency, like Bitcoin and defined a ban as a policy whereby government agents refuse to accept an alternative currency and met out punishments to private agents caught using (Hendrickson, 2017).

Mohamed Rabiul in Malaysia (2018), compared between cryptocurrency and fiat currency in both Architecture, algorithm, cash flow and ledger technology on the emerging economy focused

Table 1: Summary of some previous studies used IOT or block chain

Rekated work	Used IOT	Used blockchain	solution
Cryptocurrency and criminality: The Bitcoin opportunity (Brown, 2016)	✓		Machine of cryptocurrency
Economic analysis of cryptocurrency backed money laundering (Brenig et al., 2015)		✓	Aml control program
Bitcoin and money laundering for aneffective solution (Bryans, 2014)		✓	Centralized cryptocurrency
The regulation of intial coins offering in china (Deng and Huang, 2018)	✓		Internet protocol
Ransomware payments in the bitcoin ecosystem (Paquet-Clouston et al., 2019)		✓	Identifying information of bitcoin on top graph sense
Securing the blockchain against hackers {13}		✓	An algorithm
Strengthing the bitcoin safety (ur Rehman et al., 2018)	✓		Hardware tokens
Blockchain tokens and the potential democratization of entrepreneurship and innovation (Chen, 2018)		✓	Tokens
The proposed framework	✓	✓	Intergration between bolckchain and IOT

on most influential facts behind the economical elements like the applicable operation via successful blockchain algorithms, architecture and mining operation based on contents from journal publications, online publications, new reports, seminars and workshops and found it possible to track Bitcoin transactions which triggers money laundering. Terrorism financing, trading drugs and illicit products and if the private key lost, all Bitcoin lost forever, and it's not real money and the risk is always there (Islam et al., 2018).

Niranjan Sapkota in Finland (2019), retrieved asset of 143 cryptocuyrrencies for a sample spanning 2014-2018 and investigated the popular momentum strategy implemented in the cryptocurrency market and this research didn't find any evidence of significant momentum payoffs in the cryptocurrency market. And recommended a future research to clarify why momentum appears to be unprofitable in cryptocurrency market (Grobys and Sapkota, 2019).

Caporale in London (2019), analyzed over 1000 GPACH models to select the best model for volatility the four most popular cryptocurrencies, are Bitcoin, etherum, Ripple and Litecoin and predict the value–at-risk and expected shortfall on a rolling window basis and found that using standard GRACH models may

yield incorrect predictions and led to ineffective risk-management, portfolio optimization and pricing of derivative securities and advised using two-regime GRACH models could produce better predictions than single-regime model (Caporale and Zekokh, 2019). Summary of the debate of dealing with the cryptocurrency in some countries are presented in Table 2.

We can summarize the advantages and disadvantages of the currncies machanism as follows:

For the digital currency, although the transaction is opened and transparent for all customers but it is unstable, theft, fraud and stealing money could be amajor problem.

For the centralized cryptocurrency, Although this makes to any displine of financial sectors but customers are unauthorized to access core transaction and are focused to trust financial company ex: NEO coin, the process of mining can only done by seven trusted nodes controlled by asingle party.

For the decentralized cryptocurrency, although it is more stable due to large amount of nodes in p2p network but it's trustless nature can be destroyed by vulnerablility attack. ex: Bitcoin and Etherum.

For Blockchain tecnology without any integration, although Hash function makes secure tranaction with out supervision but much energy customing and slowing issues are faced by customers (Islam et al., 2018).

And according to this analysis we found the partially centralized cryptocurrency would be more sutable for our proposed exchange market launching, and it can be NEO vs Dollars trading.

Based on the previous studies, we found that some studies focus on applying IOT to solve the cryptocurrency problems, other use blockchain to overcome these problems. most studies ignored to integrate blockchain with IOT to maximize the security.

Table 2: Summary of the debate of dealing with the cryptocurrency in some countries

Country	Accepting or banning the cryptocurrency	The reasons
USA	Two papers accepted the cryptocurrency	To achieve the highest profit and the speed of Blockchain management systems
USA	Two papers rejected the cryptocurrency	Because of weakness and threats of Bitcoin
Barbados	One paper accept it	The profit of holding it in the portfolio of the international reserves
London	Two Papers accept it	High invests in its market
Malaysia	One paper reject it	Risks of losing the private key and money laundering
Finland	One paper reject it	Analyzed 143 cryptocurrencies and found it will be great risk
Egypt	The launching of the exchange market was cancelled	Risks of ransomware and Black net

The proposed framework is implemented to solve the two issues of ransomware and blacknet by integrating blockchain with IOT.

And the proposed framework consists of three layers:
1. The blockchain.
2. IOT.
3. The user inerface.

Depending on the hyperledger project because of its benefits in integrating the Blockchain with IOT, In order to maximize the security in the two processes of monitoring and storing.

3.3. Layer 1: (Build the Blockchain)

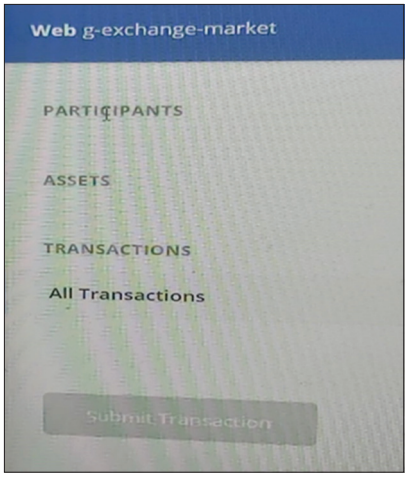
- Model file: File which we can

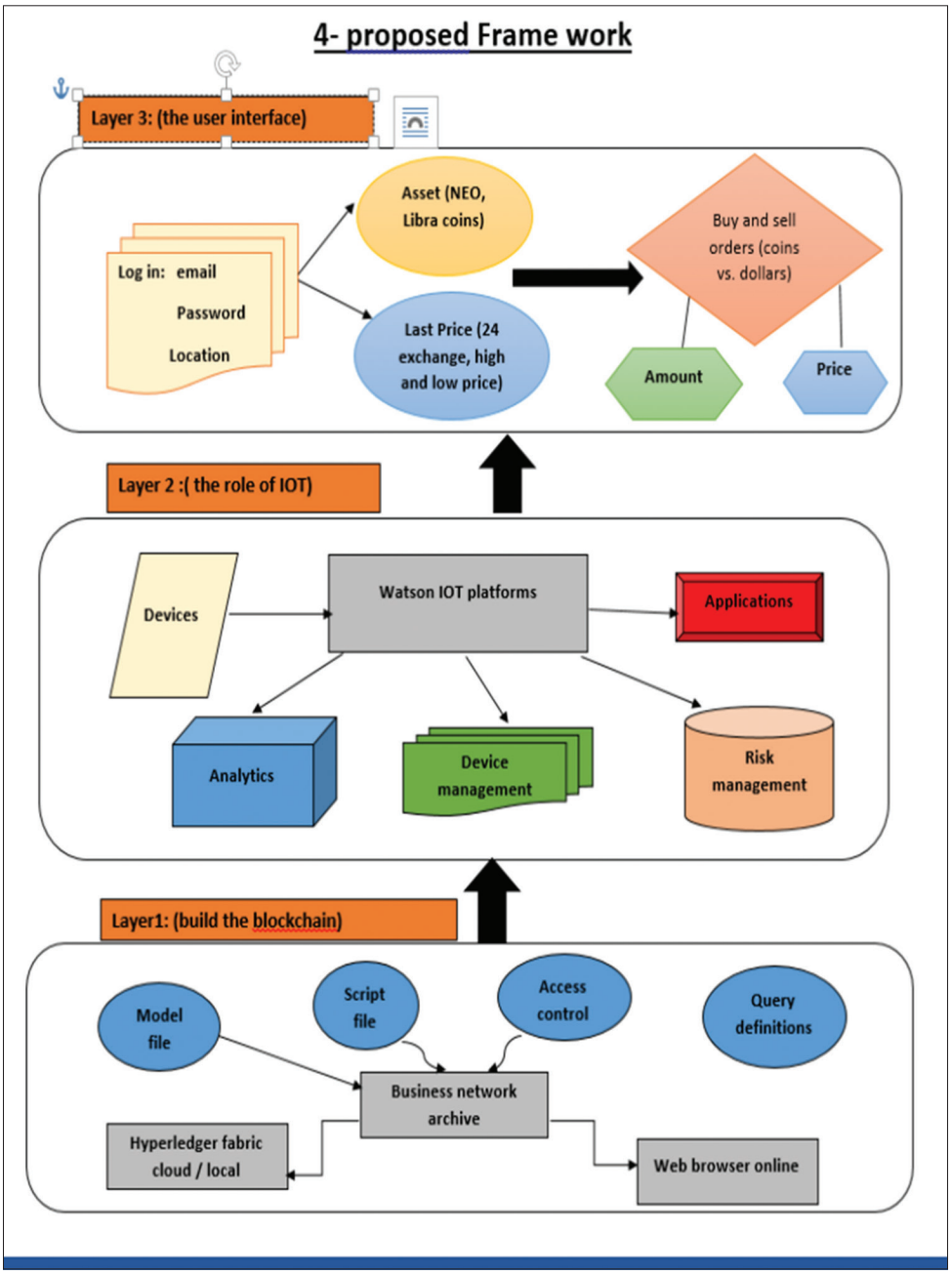
Make an extension of it named (CTO) file that we declare our models of participants, assets, transactions and events (Figure 2).

1. 1- Participant: A person w can own something or platform an action, in the exchange market this could be the bank and the users.
2. Asset: an item of value, it could be the cryptocurrency.
3. Transaction: When some participants trade assets (coins).
4. Event: When an asset changes value, we can edit events every time new Coins traded with the new price.

- Script file (transaction function): some java script code that will carry out the logic for actions as a parameter (which defines fields in the transaction model variable in the CTO file, (adding the new numbers to assets we have).
- Access control file: a file extension (file name. ACL) where we can put some rules For what participants can or can't access for example, the third part (bank) can allow the new transaction but the user can't
- Queries: it has made SQL statements written to find how many assets a participant has? Written in separate file (file name Query) mainly used to APIS that written to find things on the chain.

Figure 2: An example of the model file creationss





- Business network definition: you bandle all your files (models, scripts, permissions and queries) into a business network archive.

3.4. Layer 2: (The Role of IOT)

- Devices: should have GPS in order to log in and determine their location.
- The Watson IOT platforms: have sensors and connected with Google maps.
- Applications: only previewed for the third part to monitor the relationship between users.
- Analytics: shows the duplication happened of buying or selling for A and B devices in each transaction.
- Device management: describe how many times the same device access with the same location and what orders it did.
- Risk management: can alert in cases of buying and selling for the same devices (every time) and that may be money laundering cases.

3.5. Layer 3: (the Web Browser Online)

- Log in process: Should contains email, password and device location.
- The user can see the cryptocurrency and the change of price in dollars (old and new price).
- And the user can make order of buying or selling the asset.

4. CONCLUSION

Finally, we can summarize this analysis of several types of cryptocurrencies and identifying its risks such cybercriminal activities and specially ransomware attacks and black nets, we found its great issue in monitoring and storing the cryptocurrency

and how can the exchange markets play the role of a third part between buyers and seller and about the world legal situation of the cryptocurrency (refusing or accepting it) and how can central banks deal with it.

We found that the solution is to integrate blockchain with IOT to build up a strong, secured system for an exchange market and it could deal with partially decentralized cryptocyrrencies (centralized) such as Libra, NEO, IOTA, NEM which could differ from the known cryptocyrrencies like; Bitcoin or Etheruem because of its highly of privacy and decentralized that could be very hard to be under control by any government.

And it's predicted to increase the security of trading cryptocurrency in safe and encourage governments and investors to deal with it and avoid several risks.

REFERENCES

Banerjee, M., Lee, J., Choo, K.K.R. (2018), A blockchain future for internet of things security: A position paper. Digital Communications and Networks, 4(3), 149-160.

Boireau, O. (2018). Securing the blockchain against hackers. Network Security, 2018(1), 8-11.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W. (2015), Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: Paper presented at the 2015 IEEE Symposium on Security and Privacy. Washington, DC, United States: IEEE Computer Society.

Bray, J.D. (2016), Anonymity, cybercrime, and the connection to cryptocurrency. Available from: https://www.encompass.eku.edu/etd/344.

Brenig, C., Accorsi, R., Müller, G. (2015), Economic analysis of cryptocurrency backed money laundering. Sweden: Paper presented at the ECIS.

Brown, S.D. (2016), Cryptocurrency and criminality: The Bitcoin opportunity. The Police Journal, 89(4), 327-339.

Bryans, D. (2014), Bitcoin and money laundering: Mining for an effective solution. Indiana Law Journal, 89, 441.

Caporale, G.M., Gil-Alana, L., Plastun, A. (2018), Persistence in the cryptocurrency market. Research in International Business and Finance, 46, 141-148.

Caporale, G.M., Kang, W.Y., Spagnolo, F., Spagnolo, N. (2019), Non-linarites, cyber-attacks and cryptocurrencies, Working Paper No. 19-14. England: Brunel University London.

Caporale, G.M., Zekokh, T. (2019), Modelling volatility of cryptocurrencies using Markov-switching GARCH models. Research in International Business and Finance, 48, 143-155.

Chen, Y. (2018), Blockchain tokens and the potential democratization of entrepreneurship and innovation. Business Horizons, 61(4), 567-575.

Conti, M., Gangwal, A., Ruj, S. (2018), On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers and Security, 79, 162-189.

Deng, H., Huang, R.H., Wu, Q.J.E. (2018). The regulation of initial coin offerings in China: Problems. Prognoses and Prospects, 19(3), 465-502.

DeVries, P.D. (2016), An analysis of cryptocurrency, bitcoin, and the future. International Journal of Business Management and Commerce, 1(2), 1-9.

Evans, C.W. (2015). Bitcoin in Islamic banking and finance. Journal of Islamic Banking and Finance, 3(1), 1-11.

Grinberg, R.J. (2012), Bitcoin: An innovative alternative digital currency. Hastings Science and Technology Law Journal, 4, 159.

Grobys, K., Sapkota, N. (2019), Cryptocurrencies and momentum. Economics Letters, 180, 6-10.

Hendrickson, J.R., Luther, W.J. (2017), Banning bitcoin. Journal of Economic Behavior and Organization, 141, 188-195.

Huckle, S., Bhattacharya, R., White, M., Beloff, N. (2016), Internet of things, blockchain and shared economy applications. Procedia Computer Science, 98, 461-466.

Islam, M.R., Nor, R.M., Al-Shaikhli, I.F., Mohammad, K.S. (2018), Cryptocurrency vs. Fiat Currency: Architecture, Algorithm, Cashflow and Ledger Technology on Emerging Economy: The Influential Facts of Cryptocurrency and Fiat Currency. Kuala Lumpur, Malaysia: Paper presented at the 2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M).

Liu, J., Li, W., Karame, G.O., Asokan, N. (2018), Toward fairness of cryptocurrency payments. IEEE Security and Privacy, 16(3), 81-89.

Minoli, D., Occhiogrosso, B. (2018), Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.

Moore, W., Stephen, J. (2015), Should Cryptocurrencies Be Included in the Portfolio of International Reserves Held by the Central Bank of Barbados? Bridgetown, Barbados: Central Bank of Barbados WP/15/16.

Paquet-Clouston, M., Haslhofer, B., Dupont, B. (2019), Ransomware payments in the bitcoin ecosystem. Journal of Cyber Security, 5(1), 3.

Peck, M. (2016), A blockchain currency that beat s bitcoin on privacy [news]. IEEE Spectrum, 53(12), 11-13.

Peck, M. (2017), Blockchains: How they work and why they'll change the world. IEEE Spectrum, 54(10), 26-35.

Phillip, A., Chan, J.S., Peiris, S. (2018), A new look at cryptocurrencies. Economics Letters, 163, 6-9.

Poon, J., Dryja, T. (2016), The Bitcoin Lightning Network: Scalable off-chain Instant Payments.

Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M. (2018), On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173-190.

ur Rehman, H., Khan, U.A., Nazir, M., Mustafa, K. (2018), Strengthening the bitcoin safety: A graded span based key partitioning mechanism. International Journal of Information Technology, 2018, 1-7.