Bitcoin and the Monetary System Revolution Changes

Leena Alotaibi[1], Azhar Alsalmi[1], Hatim Alsuwat[3] and Emad Alsuwat[1],
Lssthemail@gmail.com, Az.alsalmi@live.com , Hssuwat@uqu.edu.sa, Alsuwat@tu.edu.sa,
[1] Department of Computer Science, College of Computers and Information Technology, Taif University, Saudi Arabia
[2] Department of Computer Science, College of Computer and Information Systems, Umm Al Qura University, Saudi Arabia

Summary
Every day brings a new challenge to the humanities. Life nowadays needs accuracy, privacy, integrity, authenticity, and security to run life systems especially the monetary system. Things now differ from previous centuries. Multiple varieties in digital banking have opened the new and most advanced innovations for human beings. The monetary system is going to developed day by day to facilitate the public. Electronic money has amazed the world and gave a challenge to central banking. For this purpose, there will be a need for strict security, information, and confidence. Blockchain technology has opened new gateways. Bitcoin has become the most famous digital currency, which has created a thunderstorm in digital marketing.
Blockchain, as a new Financial Technology, has satisfied all the security issues and satisfied doing business in secure ways that encourage investors to invest and keep the world business wheel. Assessment of the sustainability of implementing Bitcoin in financial institutions will be discussed. Every new system has its pros and cons in which a clear vision of what we are about to use can be sought. Through this research paper, a demonstration of the monetary system evolution, the new ways of doing business, some evidence in a form of academic cases will be demonstrated through comparison a table, a suggested method to transfer to the new system in safe mode will be proposed, and a conclusion will be concluded.

Key words:
Cryptography; Blockchain; Bitcoin; Security; Monetary System.

1. Introduction

Since the world dived into the electronic era, there was a need to invent crypto currency. The old monetary system started with goods trade and bargain, and then evolved to exchanging metals with other goods and services. After that, the monetary system evolved to what we know now; it became the one we officially use. Governments save the gold in vaults and replace it with paper money and tint coins. Currently, the world is dramatically changing, and the systems are evolving to electronic ones. So, the need for a new monetary system that will fight the sabotage, theft and cons must be invented. In 2017, Bitcoin became a shooting star. Its price multiplied twenty times within twelve months as shown in figure 1. Bitcoin stable the structure day by day and adopt a charming status. In 2018, the well-reputed position astonished the modern world. The dynamics and communication between Bitcoin price and its mining costs have become major interest. Indeed, we have entered a new chapter of Bitcoin mining. We can see that marginal costs and mining effectiveness play a vital role. The price change raised the question of mining bitcoin cost for gaining benefits. Mining is a process for issuing a Bitcoin; this process needs use of software, such as GUIMiner, CG Miner, and BFGminer, and special hardware, such as like ASICMiner, AntMiner, and Avalon [1][2].

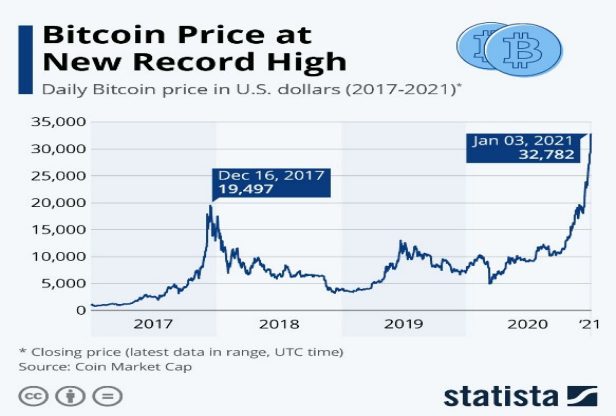

Fig. 1 Bitcoin change through 2017 – 2021

Financial institutes, banks, and monetary companies plan to transfer their systems to peer-to-peer networks with no centralization for trustworthy and sustainable system. Several universal banks have evaluated the role of CBDC, which is the Central Bank Digital Currency, in global payment systems [3].

Nakamoto, the inventor of Blockchain, hoped that distributed ledger technology (DLT) of Bitcoin will end the role of both commercial banks and central banks in creating and transferring money. In the current monetary system, it is hard to trust banks' reliability in keeping essential utilities. Commercial banks are looking for profit as they are private enterprises and trying to maximize their return on investment (ROI) to preserve their capital providers. Now the Bitcoin system architecture has essential flaws that prevented Bitcoin from performing the three functions of money: initially, it is a store of value; secondly it is a unit of account and finally medium of exchange, otherwise, Bitcoin would have radically reformed the monetary system.

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.21

However, financial institutions recognized the possible benefits from executing DLT and began plans to restructure the Bitcoin construction. One of these projects, the R3 Corda, gave promising results in the clearing of financial mechanisms. The actual application of DLT implies that such technology can be beneficial in retail payments and eventually in monetary reform.

Another way to reform the monetary system is under the consideration of central banks. They are exploring the use of DLT in payment, security, and cross-border settlement of payments with the ultimate goal of improving the efficiency, security, scalability, and resilience of the process [4].

Traditional payment systems controlled by central banks can change forever by using DLT. Private payment systems (such as Facebook's Libra and Pay Pal) with their large social networks could take over the role of central banks and create a new payment system that do not rely on traditional way of deposits. Facebook, for example, has a multi-billion people social network in which digital tokens information can transfer cheaply and rapidly, and can be converted into the most convenient form for the receiver without any intermediates.

Currently, central banks issue cash currency. In the future, the role of issuing digital currency will be shifted to big fintech companies (like Facebook, Alibaba, and Amazon) as they can offer digital alternatives to the bank-built system. Central banks will change their responsibility to issue and maintain stores for value digital currencies. As the stores' keepers and central banks will give access to these stores to licensed institutions and digital currency issuers only to enhance the efficiency and stability of payments. Fintech companies can also apply for licenses to keep reserve balances [5].

2. Literature Review

Satoshi Nakamoto started working on a project in 2009 till the end of 2010 until the launch of the project, while contacting the project team through forums. He worked as a developer; his project transferred to the open-source community by the end of 2010. Nakamoto the mysterious man only knows by his name and wealth that valued about 100 million Bitcoins by todays' values.

The new idea of digital currency helped enhances cryptography, Cybersecurity, and ciphering. Since the use of Bitcoin many attacks registered on multiple occasions. With each attack, a new assessment was evaluated, and enhancements happened. One of the enhancers was Danny Bradbury, he assessed and explained Bitcoin system vulnerabilities and suggested alternatives and changes to conventional monetary system currency [6]. Hacker needs more effort and more professional computers to complete the attack on theft the Bitcoin. Since Bitcoin uses' a decentralized network and depends on Blockchain in its transferring process hackers must make sure to hack more than 51% of the Blockchain connected computers. Hacker needs to change data in no less than 51% of computers to have the new result [7].

Crypto-currency passed through many trials until Bitcoin which consider a successful crypto-currency. Bitcoin-based on the Blockchain technology using distributed database in a form of a general ledger, decentralized peer-to-peer network and the cryptographic key were behind strengths of Bitcoin [8].

Each chain in the Blockchain has Bitcoin transaction, the history keep distributed between blocks. To unlock the block the hacker needs to guess the hash number correctly; the hash number is a complicated and unique number that connect nodes in Blockchain; knowing that there are more than 500,000 nodes in Blockchain will conclude of guessing hash considered impossible and this is only for one node. Each transaction was confirmed by all the Blockchain participants, the consensus of a majority of the members. To change any information more than fifty-one percent 51% of nodes must be successfully hacked to pass collective confirmation, which never happened until now which supports trustworthy transactions [9],[10].

Large business makers and industrial players are joining the use of Bitcoin and implementing the Blockchain framework. Big names like central banks and multinational banks along with computer and technology maker companies also use the Blockchain framework. IBM, Microsoft, Intel, NEC, some countries and institutes like Japan, China banks, Canada central bank, Dubai, India banks either private or governmental, Estonia, West Bengal and Andhra Pradesh among other countries and governmental institutes. This implementation shows trust, provenience, security, and Consensus.

Bitcoin came with a promise of sponsorship free; no hold or block payment could happen. It is a promising system that predicts evolution in e-commerce system. No big system regulation or risks can frighten the investors. That is the amount of money invested in Bitcoin has reached 400 billion USD in only 10 years, from 2009 until 2019.
Crypto currency permitted business majors in the market to be applied, to understand the mechanism of workings will be demonstrated. Cryptocurrency, a.k.a. a compromise system, is described as a method that assists inaccuracies. Without face-to-face meetings, blockchain is used along with computer systems to reach an agreement upon data value and finalize agreements. Since publicly open blockchain is globally employed as a decentralized system, the shared information among all users can be utilized to describe the process of adding the next transaction to the blockchain. 'Blocks' , as we stated before, means the transactions each transaction must be confirmed by the majority of users, once the transaction created it cannot be altered or changed and the 'chain' is in what way the data is

connected [11]. Each chain has a unique dependable number called the hash. Hash depends on the information in the block any change will create a new hash, so the alteration affects the number. This hash connects the blocks [6].

Bitcoin Works Explained: if the owner of the Bitcoin wants to buy anything he/she needs to make a transaction that includes transferring the Bitcoin from his ownership to the buyer ownership. A simple way to do so is by writing a cheque digitally by endorsing the prior hash and the key for the possessor; the public key; the payee; adding it at the end of the coin transaction to be transferred. To finalize the barging the seller must sign with his private key that the agreement is complete. There is a time gap between sending the signed check and verify the transfer acceptance. A potential problem that the transaction cannot for sure be registered and the owner still have the Bitcoin for a while. Bitcoin Blockchain considers a solution of broadcasting in public that this transaction is under maintenance creating an internal system for all Blockchain participants to signa confirmation for this transaction. Then a proof of transaction and confirmation that the majority confirms the history of the transaction is required for the payee who considers an evidence of work [5].

Evidence of work, also called proof of work, is a time sensitive process that in most needs 10 minutes. This process maintains transaction integrity. After broadcasting unfinished transactions each node collects the transaction information into a secure Blockchain block. Participants' acceptance for the broadcast and the proposed block considers as a confirmation of the block's correctness. The competence of being active on the system by declaring rewards for active participants consider crucial in the process too, so all will try to have a power computer with fast and stable CPU [5].

Issues with Blockchain Cryptocurrency:

Even though Blockchain cryptocurrency is appealing in its special way, like anything novel, issues and problems arise with its implementation. As Blockchain depends on large amounts of data, and the transferred data between peers. Naturally, this situation is not steady as this would mainly depend on the hardware and bandwidth of both peers, keeping in mind that not all peers are equal, and this could pose a problem regarding data transfer.

Latency Issue: as mentioned in the previous issue, network bandwidth could differ between peers and from this emerged another problem which is the delay in processing a request from the user. Modern transactions and net banking require that requests be processed over the internet almost immediately.

Scalability Issue: to provide trusted security and authenticity, multiple verified logs of the transactions must exist, should an entity lack the devices on which to store these logs, then the blockchain could be compromised. To ensure security, many users are required for the cryptocurrency to be acknowledged as secured and verified. Double Spending Issue: regarding the possibility of late updates of the transaction logs, a person could spend the same cryptocurrency twice where it is spent at two different locations at nearly the same time. This would cause an inconsistency in the transaction data.

Wasted Resources Issue: since the cryptocurrency Bitcoin requires proof of work, it all depends eventually on the work done by the miner, and since multiple people compete to be the first to submit the proof of work, only one person gets his money back while the rest suffer losses in the form of time, manpower, and resources.

Data Malleability Issue: Cryptocurrency is accompanied by an ownership signature. However, what is the guarantee that the owner is responsible for the said transaction? The hacker may be able to alter the transaction and resend it which causes trouble for guaranteeing which transaction is the legitimate one.

3. Case Studies

As mentioned above, changing the money system to the new digital nonphysical Bitcoin will need the implementation of a Blockchain system that needs strong Ethereum protocol hardware. The money transfer process happened without any third party or external authority. Previous transfer obeys banks rule and susceptible to the normal delay. Using this new technique, we can save days and extra transferring charge.

Many cases show business companies try to implement the Bitcoin system although use the virtual space can be affected by many things as mentioned before like secure IP address, protected proxy and the cyber-criminals or frauds Bitcoin-related offenses. China, Bangladesh, Bolivia, Ecuador, and Japan forbid their banks and financial institutions to trade Bitcoins on large scale but allow an individual to do so.

Case 1

Indian Banks:

Private sector banks and governmental banks along with financial services industry companies all individual or cooperate started since 2017 till now implementing Blockchain to earn a stable marketplace. Billions of dollars were invested in such a method to change the infrastructure using the Ethereum protocol. Knowing your customer help in this investment even though the banks of India establish IDRBT; The Institute of Development and Research in Banking Technology. India considers a major country who drive toward the benefits of Blockchain and Bitcoin this drive through showed proof of success [12][13][14].

Case 2

Silk Road:

Silk Road is a famous Dark net created in 2011 by Ross William Ulbricht. This malicious web considers Bitcoin as the acceptable currency to make its illegal trades selling drugs and stolen goods. In two years, this site earns 1.2 billion dollars. In 2013 The FBI accidentally found the email of the owner used carelessly in an online forum. Silk Road was a system that besides the Blockchain used the technique and tumbler technique. This technique secures the IP address reduces traffic, eliminates traffic analysis. As a system Bitcoin used efficiently in buying, selling, and transferring so regardless of the wrong use the system valid [2][15].

Case 3

Coin.Mx:

Coin.Mx is a case created in November 2013 by Yuri Lebedev. Russian-based payment to buy legal and illegal and also to wash money used Coin.Mx as an exchange service system using Bitcoin to pay for the exchanging data. The system implemented in many countries using the tumbler technique and showed success in the market as an exchanging system [16][17].

Table1: Comparison between case studies

Source	***Aim***	Method
Case Study 1	Earn a marketplace Dominate and precede others	Ethereum
Case Study 2	Run illegal business on darknet without being caught	Tor and tumbler
Case Study3	Sell data and pay for exchanging service	Tumbler & Blockchain

4. Discussion

Through the paper, the pros and cons have been explained along with the main reason that drives investors to change the system. Upper explained cases also support the idea of the true benefit behind the scenes. The main reason is to gain more money and to earn a stable marketplace, alleviate the money transferring process. Bitcoin has shown enormous growth in the market. Digital currencies have developed new setups, bitcoin popularity confused the old banking systems and compelled them to be advanced. The only main concern is cybercrimes. As well as the digital world has presented advanced technologies in the finance sector, there is a strict need to develop a security system to prevent cybercrimes and hackers.

From the beginnings of 2007 to 2021 journey of bitcoin faces many difficulties and problems. Bitcoin adopted many conditions, earlier, it was considered as an illegal method, and gradually bitcoin changes many positions, but as well time passed, bitcoin got success in 2017/2018 broke all the previous records and become a shining star in 2021.

The first case used Bitcoin for the good illegal cause. While the second and the third cases used Bitcoin as a hidden secure method to do either money laundry, spy business, or drug business. Implementation in the real world showed reliability and stability. The paper's contribution is to alleviate the burden of searching through many references and research papers. That the paper summaries pros and cons along with the implementation of the new currency and the use of this currency, paper also shows the benefits that the world can gain if implementing this method. Research shows, how the digital market developed in the world. Introduction and the success of cryptocurrencies and blockchain systems astonished the world. Blockchain technology has opened new gateways. Bitcoin has become the most famous digital currency, which has created an advanced vision in finance marketing.

5. Conclusion

The paper predicts that the future supports the use of the digital coin Bitcoin. Multiple varieties in digital banking have opened the new and most advanced innovations for human beings. The new era needs new blood and new technologies. The world has become smart, the overall structure has been changed and she has adopted the modern shape of a global village. Digital cryptocurrencies like bitcoin have been changed the total scenario of the financial market. It was 2009 when bitcoin starts mining and the world was thinking that Mr. Satoshi Nakamoto is dreaming but as well time passed, bitcoin got success in 2017/2018 and broke all the previous records. In April 2021 bitcoin cross the highest limits and its price reaches $62000. It was the super success of bitcoin and the digital world.

Digital banking and digital currencies have developed new setups, bitcoin popularity confused the old banking systems and compelled them to be advanced. The summary of the article revolves around the digital currencies, blockchain, and the brightened success stories of bitcoin. Mr. Satoshi Nakamoto's thinking establishes new and most modern alidades in digital currency. The use of Bitcoin will be fast and easy, it is supposed to eliminate the time required to transfer money using the traditional bank methods. Although some concerns are mentioned above and some cases of wrong use, but the overall conclusion support the idea of using the Blockchain infrastructure and the Bitcoin digital currency.

References

[1] Kristoufek, L. : Bitcoin and its mining on the equilibrium path. In: Energy Economics, vol. 85, (2020)
[2] Kethineni, S., Cao, Y., & Dodge, C. Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. In: American Journal of Criminal Justice, 43(2), 141-157. (2018)
[3] Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., Arami, M. : How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. In: Technological Forecasting and Social Change, vol. 158, (2020)
[4] Opare, E.A., Kim, K. :A compendium of practices for central bank digital currencies for Multinational financial infrastructures. In: IEEE Access, vol. 8, pp. 110810–110847(2020)
[5] Huibers, F. Distributed Ledger Technology and the Future of Money and Banking. In: Accounting, Economics, and Law: A Convivium, (2021)
[6] Efanov, D., Roschin, P. The all-pervasiveness of the blockchain technology. In: Procedia Computer Science, (2018)
[7] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. Where is current research on blockchain technology?—a systematic review. In: PloS one, vol. 11, (2016)
[8] https://coinmarketcap.com/ accessed March 26, (2021)
[9] Khadka, R. The impact of blockchain technology in banking: How can blockchain revolutionize the banking industry?. (2020)
[10] Konstantinidis, L., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., Decker, S., Blockchain for business applications: A systematic literature review. In: Springer, Cham, pp. 384-399, (2018)
[11] Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. An overview of smart contract: architecture, applications, and future trends. In: 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 108-113).IEEE. (2018)
[12] Gupta, S. N. Gyan Vahini-Creation of an Open Access National Digital Infrastructure Grid through Functional Separation Using Smart Contracts and Blockchain. In: AKGEC INTERNATIONAL JOURNAL OF TECHNOLOGY, Vol. 10, (2018)
[13] Manda, V. K., Polisetty, A. Status check on blockchain implementations in India. In: SSRN 3265654, (2018)
[14] Sachan, K., Aadhaar & Blockchain: opportunities and challenges for India. In: Doctoral dissertation, Massachusetts Institute of Technology, (2018)
[15] Bouri, E., Roubaud, D., & Shahzad, S. J. H. Do Bitcoin and other cryptocurrencies jump together?. In: The Quarterly Review of Economics and Finance, 76, 396-409. (2020)
[16] Blockchain. (2017, April 13). Bitcoins in circulation.Retrieved April 15, 2017, from https://blockchain.info/charts/total-bitcoins.
[17] Bartoletti, M., Lande, S., & Zunino, R. Bitcoin covenants unchained. In: Springer, pp. 25-42 Cham. (2020)

Leena Alotaibi received her bachelor's degree in information systems from Al-Imam Mohammad Ibn Saud Islamic University, Saudi Arabia, in 2017. Currently, she is a graduate student at Taif University. She is doing her master's degree in cybersecurity studies. Leena's research interest includes cybersecurity and Bitcoin.

Azhar Alsalmi received her bachelor's degree in computer science from Taif University, Saudi Arabia, in 2009. Azhar is a teacher at the Ministry of Education in Saudi Arabia. Currently, she is a graduate student at Taif University. She is doing her master's degree in cybersecurity studies. Azhar's research interest includes cybersecurity and Bitcoin.

Hatim Alsuwat is an assistant professor of Computer Science in the College of Computers and Information Systems at Umm Al-Qura University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Information Security, Cryptography, Model Drift, and Secure Database Systems.

Emad Alsuwat is an assistant professor of computer science in the College of Computers and Information Technology at Taif University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Probabilistic Graphical Models (esp. Bayesian Networks), Artificial Intelligence, Information Security, and Secure Database Systems.