HOLISTICA Vol 10, Issue 2, 2019, pp. 167-186 DOI:10.2478/hjbpa-2019-0024

Cryptocurrency: Adoption efforts and security challenges in different countries

Suhag, PANDYA,
Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA
spandya5886@ucumberlands.edu
Murugan, MITTAPALLI,
Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA
mmittapalli7237@ucumberlands.edu
Sri Vallabha Teja, GULLA,
Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA
sgulla1723@ucumberlands.edu
Ori, LANDAU,
Department of Information Technology, University of the Cumberlands, Williamsburg, KY, USA
olandau6200@ucumberlands.edu

Abstract

This research paper is a holistic review done on the rise of Blockchain and cryptocurrency, then elaborate about the great advantages of having a decentralized finance system. The existing scenarios from a sample of countries were reviewed in regards to their effort to adopt cryptocurrency to find some of the challenges like what are the security challenges this new monetary system faces, and limitations faced by different countries. A detailed analysis was done to answer some of the vital questions as such why cryptocurrency is banned in a few countries when other countries see cryptocurrency as a secured mode of payment transaction or what kind of security is provided by cryptocurrency compared to the traditional payments such as pay by cash, credit, or checks. Lastly, this paper also summarizes a high-level overview to propose recommended solutions to overcome the security concerns associated with the adoption of cryptocurrencies and how does the future of cryptocurrency look.

Keywords: cryptocurrency, Blockchain, cybersecurity

1. Introduction

In order to have an understanding of the potential value of cryptocurrency, it is important to first understand the technology behind the cryptocurrency platform, Blockchain. First created by Satoshi Nakamoto in 2008, Blockchain is the base of the non-centralized payment system platform. The initial goal was to create an electronic payment system based on cryptographic proof instead of trust (Waldo, 2019). The great potential of using Blockchain is that option to have to have a discrete, transparent, and even fool proof. The secret lays with the fact that there is no one source of truth.

With implementing Blockchain, many ledger keepers are enabled to keep track of all ongoing transactions (Weber, 2018). By having several sources of truth, the middle man is removed from the transaction, also the information is secured in the sense that the information is shared with too many sources to be lost. For example, in a one ledger platform every transaction needs to go through a middle man. The middle man has to record each transaction, who is the seller, who is the buyer, and the details of the transaction.

There are several key aspects to this type of operation. One is that there is only one source of truth, this can be a risk if a cyberattack may damage it. The second aspect is the current existing need to always have a middle man, no transaction can take place without the help of the ledger keeper (Yuan & Wang, 2018).

Upon examinations, the researchers found out that there are many versions of how to implement a Blockchain platform, but all share these three main features (Waldo, 2019). First, there is the ledger, which is a public piece of information. The ledger is a series of blocks. Each block holds a set of ordered transactions and each block points to the next block as well. The edger, or Blockchain, is shared with many record keepers across the platform, hence allowing the transaction information to never get lost or become outdated. Second, there is the user protocol used.

This is the basis for mutual communication of users in the platform. By having this protocol in place the information that is kept in the ledger is common and unambiguous (Baliga, 2017). Lastly, there is the currency. This is the motivator for the record keeper to continue holding on to and updating the ledger.

The security aspect of the platform is remarkable and yet simple. As described before, the ledger is comprised of sets of blocks. Each block begins with a cryptographic hash found in the previous block, hence creating the chain. The way to Hash values are calculated prevents any number tampering, it is important to understand that the community will be able to spot any changes and breaks in the chain. That type of chain is not unique, it is called a Merkel chain. But here is the key to maintaining the authenticity of the information in Blockchain (Betts, 2016). The Hash key for Blockchain has an added kink. Each Hash number is being created by adding a random set of bits.

Adding this random factor makes it almost impossible to predict the next number (Yuan & Wang, 2018). All of these calculations or Hashing is being done by the record keepers, these are the miners of the coins. By constantly logging the blocks they enable the system to exist, for transactions to take place and maintain the information (Eyal Gün Sirer, 2018).

2. The Role of Cryptocurrency in a Decentralized Platform

Cryptocurrency is the third key component of the Blockchain platform. Once a ledger is created to store the transactions and a protocol is in place to break down the market's rules (Holotescu, 2018). As a currency, Cryptocurrency offers several advantages over government issued and backed currency. The most notable one is that no entity has sovereignty over it, and by being an unregulated currency cryptocurrency provides almost full anonymity (Amanzholova & Teslya, 2018).

The second most known advantage is the decentralization of the system, which provides a close to perfect platform to keep funds in (Holotescu, 2018). Another architectural feature that is appealing is the transparency in the system, there is no back office like modern banks have (Grech & Camilleri, 2017).

Moreover, the currency itself is not tied to any central bank, which means that the value of a currency can fluctuates greatly. If it was the case that a central bank would have sovereignty over a cryptocurrency, efforts would have been made to stabilize the currency value as central banks usually do with other currencies. This fact makes cryptocurrency a semi-investment tool, for example, 12 months ago the value of Bitcoin, perhaps the most known cryptocurrency, was increased by over 700%.

A cryptocurrency plays several roles. It is the fuel to drive the Blockchain continuous maintenance process forward, allowing a decentralized platform to exist. Also, cryptocurrency can be seen as both a commodity and a currency. There several parties that are willing to deal, exchange or get paid with cryptocurrencies just like any other government-backed currency such as miners, vendors, wallet holders, and exchange (Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker & Savage, 2016). Lastly, cryptocurrency can act as a commodity to hold value stemming from other currencies (Tiwari, 2019).

On the other hand, cryptocurrency can also be seen as a commodity where people can benefit from the increase and decrease in value of the currency (Amanzholova & Teslya, 2018).

3. Market uses for Cryptocurrency

With the rise in popularity of cryptocurrency, many businesses found the new platform desirable for the lack of processing fees, upgraded security, and better performance. Processing fees is another important factor to consider when running a business as each transaction is being charged to the business (Halaburda, 2018). Using the new system would theoretically provide an automated, safe and fast service for exchange goods or services for currency, minus the fees to banks or other types of brokers (Dumitrescu, 2017). It is important to have an understanding of what does fast means in terms of processing a transaction.

A bitcoin transaction may take between 10 to 30 minutes, while a bank backed transaction may take hours or days (Seaman, 2014). This time difference has several effects on a business, for example, the use of cryptocurrency reduces the risk of chargeback fraud. This type of fraud happens when a buyer at an online market places claims that the goods did not arrive and demands a refund.

The platform enforces that refund back to the customer at the expanse of the seller. The most susceptible victims are small and medium enterprises using E-commerce platforms (Guo, Bao, Stuart, Le-Nguyen, 2017). This type of fraud could not take place on a cryptocurrency platform as the seller has to approve the refund from his wallet.

The advantages of Blockchain and cryptocurrency can go far beyond small and medium sellers on e-commerce platforms. Even banks around the world recognize the value in using a better secured and faster currency exchange platform. For large banks, the notion is to substitute certain payments processes that are less secured with Blockchain based methods (Amanzholova & Teslya, 2018). Once the general public is willing to use these kinds of platforms, large banks can consider to incorporate Blockchain as a viable tool.

All the while it is important to understand that the platform benefits works best with a cryptocurrency during 2017, the cook county in Illinois tried to implement a Blockchain based system for recording keep of real estate properties. Because of the fact that there was no incentive to make sure all record holders updated the new block that decentralized system was not kept up-to-date (Halaburda, 2018).

4. Cryptocurrency and Government Oversight

In spite of the favorable circumstances that Bitcoin and different digital forms of money offer in the commercial center, cryptographic forms of money likewise produce new arrangements of snags for worldwide budgetary organizations and state governments managing or observing exchanges. The pseudosymmetry gave to the clients by digital forms of money, combined with the simplicity of exchange, has turned out to be a solid apparatus for non-state and criminal systems seeking after techniques to sidestep charges, legislative guidelines and global authorizations (Milutinović, 2018).

Cryptographic forms of money do not work inside the current monetary framework, and the current financial understandings and laws are ill-equipped to challenge digital currency use. To counter unlawful use, sovereign states must make new laws over the current state and worldwide budgetary foundations to confine cryptographic money exchanges. In any case, in the improvement of new enactment, administrators will be compelled to wrestle between the restrictions of sovereign laws on digital currency and the necessities of household and country security.

Moreover, the administration's quest for new laws will probably be limited by the insurance of freedoms ensured to the residents the secrecy characteristic cryptographic money's Blockchain. In this manner, the importance of this proposition explore questions is to feature the advancing difficulties that sovereign states will experience as digital currencies turn out to be more standard. This proposition likewise breaks down the potential roads of communication and association between the current money related instincts and administrative bodies as they look to restrain, manage, and institutionalize exchanges using digital currencies.

5. Security in Cryptocurrencies

As per Arvind Narayanan (2016), distinguish digital money as a blend of cryptographic and cash, wherein the “utilization of cryptography gives a component to safely encoding the principles of a digital money framework inside the framework itself." Bitcoin's decision of cryptographic capacities is the hash work, a cryptologic capacity that is utilized in Bitcoin to construct a significant number of the more intricate information structures ensuring the security of the convention.

6. Cryptocurrency Ban and other Complications

Decentralized digital forms of money represent another and dynamic test to sovereign states; in this manner, essentially of the cryptographic forms of money curiosity, the worldwide network stays partitioned on what move ought to be made to stand up to digital currencies.

For the research paper, the countries named Bangladesh, Bolivia, Ecuador, Kyrgyzstan, and Nigeria, were analysed to study the complications and challenges in using Cryptocurrencies in their countries. The present scenarios of cryptocurrency in countries like China, Nigeria, etc. were also taken into consideration for comparison and analysis purpose.

As of March of 2018, five nations have received enactment that makes owning or executing with cryptographic forms of money illicit. For instance, in 2017, the nation of Bangladesh has banned Bitcoin and other virtual monetary forms. As per Bangladeshi law, exchanges utilizing Bitcoin or other virtual monetary forms are unlawful, and violators are liable to a sentence of as long as 12 years in jail.

Kyrgyzstan additionally discharged comparable direction in 2014, when the Kyrgyz government banned its natives from utilizing virtual monetary forms. As talked about in the past area, in Ecuador the "issuance, advancement or flow of virtual monetary forms" is illicit.

In like manner, according to the Central Bank of Bolivia's index goals n044/2014, all money or coins not issued or controlled by the legislature, including a rundown of virtual monetary forms are disallowed. The Bolivian government has additionally substantiated itself quick to uphold the arrangement, capturing of its residents in May for utilizing bitcoins and altcoins as speculations.

Nigeria offers a later case of a state starting an official position on digital forms of money. Starting at mid-2017, the Central Bank of Nigeria restricted virtual monetary standards, expressing exchanges in VCs are to a great extent untraceable and mysterious making them vulnerable to maltreatment by culprits, particularly in illegal tax avoidance and financing of psychological warfare.

Example of China

Out of the majority of the countries that have endeavored to boycott cryptographic money, the People's Republic of China (PRC) has taken the most significant activities to confine residential digital money use in what could be depicted as the methodical portion of laws to demoralize digital currency use within Chinese outskirts. Beginning in 2013, the People's Bank of China (PBOC)—the state controlled national bank of China—ordered the nation's initial move toward precluding digital money use when the state banished Chinese based monetary foundations from utilizing bitcoin as a technique for exchange.

By December 4, 2013, the PBOC had exhorted business banks to preclude "settlement or installments identified with bitcoin. It likewise banished trust organizations and reserve the executive's firms from making bitcoin related speculations and exhorted safety net providers not to safeguard bitcoins," China additionally established new necessities to the money related part, requiring all Chinese-based cryptographic money trades and exchanging stages to register with the Ministry of Industry and Information Technology and Telecommunication Bureau. Shortly after the 2013 confinements, China further braced down on household digital currencies use when it requested that all bitcoin exchanging records to close somewhere around April 15, 2014.

7. States' Effect in Banning Cryptocurrencies

Outside of China, sovereign expresses that have restricted cryptographic forms of money seem to have had blended local outcome in their endeavours to keep their residents from getting Bitcoin and different digital currencies. Once more, one such case is in Nigeria where digital forms of money like Bitcoin have been esteemed unlawful. All things being equal, the Nigerian government and national bank both recognize that they are almost weak to implement digital currency laws, conceding in a legislative gathering in 2018 that the National bank cannot control or manage bitcoin.

National Bank cannot control or direct Blockchain. Similar way nobody is going to control or direct the Internet as they do not possess it. For the situation of Nigeria, the state can tell its residents that digital forms of money are illicit, however given the blend of a financial open-door putting resources into bitcoin and the absence of adequate state influence to discover and rebuff violators, it is improbable that the nation will most likely dispense with cryptographic money clients under its way.

A comparable cases were found for countries like Nigeria and Ecuador, where Bitcoin has been unlawful for a long time to date. Shukla & Chaturvedi, writes in mid-2017 regardless of whether the law just permits the stream of electronic supported cash sponsored by the Central Bank, individuals are utilizing and purchasing bitcoin progressively frequently." Likewise, in Venezuela, where the nation has captured Bitcoin excavators previously, the residents keep on gambling indictment by mining and executing bitcoins to get by in the hyperinflated economy (Sayed & Abbas, 2018). This area examines the three reasons why a state would manage digital currencies: customer assurance, the counteractive action of illegal tax avoidance, and monetary arrangement insurance (Oh, 2018).

Purchaser Protection, Sovereign states regularly quote buyer insurance as a principal motivation to control digital forms of money because of the dangers innate in the unregulated cryptographic money showcase. As the BIS states, national banks commonly have an obligation to advance protected and proficient installment frameworks. For example, financial specialists could confront the potential for misfortune because of the instability of significant worth in digital currency markets.

The BIS likewise indicates out that due the relative secrecy in cryptographic money exchanges, there is a substantial danger of extortion in advanced cash markets.

Illegal tax avoidance, the pseudo obscurity natural in cryptographic money has produced various challenges for law implementation offices. As expressed by the 2015 BIS report, the relative obscurity of advanced monetary forms may make them particularly vulnerable to tax evasion and other criminal exercises. Cryptocurrencies can without much of a stretch be exchanged from fiat to digital money, exchanged through various virtual wallets, and afterward traded once more into fiat money by means of a trade or by means of an exchange of cryptographic money to another client's virtual wallet in return for money.

While identifiable through the Blockchain, this procedure confuses the lawful necessities that license law authorization to follow and indict tax criminals. A sovereign state could endeavor to control cryptographic money trades or require its residents to enroll digital money records to expand the perceivability of Transactions.

To protect the monetary policy in the hypothetical occasion that a non-sovereign cryptographic money turns out to be broadly acknowledged and utilized without satisfactory state-controlled guidelines set up, the residents could sidestep the sovereign state and national bank totally. On the off chance that such an occasion was to happen, the outcome could be a debilitating of the sovereign government and national bank to issue and control loan fees and the debilitating of financial arrangement.

The Committee on Payments and Market Infrastructures (CPMI) report clarifies that a far-reaching substitution of banknotes with advanced monetary forms could prompt a decrease in national bank non-enthusiasm paying liabilities. The outcome could be a decrease in national bank profit that establish national bank seigniorage income. Likewise, if digital money winds up across the board, natives would never again require the utilization of banks for the distributed idea of the Blockchain.

The outcome would be an adjustment in the national bank's financial approach.

8. Security Challenges, Advantages and Limitations of Cryptocurrency and Blockchain

Over the last couple of years, people in the retail space have gotten very excited about Bitcoin and digital currencies in general but, institutional markets have not been able to participate for the most part. So, cryptocurrency does not have traditional market participants. It does not have a whole heck of a lot of funds in comparison with regular markets. There is still limbo situation to figure out whether cryptocurrency to give hedge funds asset management companies and traditional finance companies what they need to participate in this. This is where the big money is and the companies will be involved whether to encrypt over mainstream and them getting involved will probably expedite the process or be the spark for crypto going mainstream.

Now they are mainly wanting custodians, the stock and bond market is very different from the crypto market but part of why crypto was designed and this is an advantage that it has over regular Fiat been for safety in order for institutions to participate in digital currencies. Security levels now with regard to security and the Blockchain there have been a few ideas sort of brought forward. Some of them are time lock transactions and fault proposals into the chain and the best way of incorporating crypto safety is to have these mechanisms incorporated into the Blockchain. One downside of this is that transactions would probably take a bit longer to go through.

This might not work for a daily use cryptocurrency that being said there have seen so many security breaches recently. The developers need to invest their time for security at least for the present moment but this is still early days in the crypto Blockchain space. Hopefully, there may be some improvements to this be seen in the near future in cryptocurrency or Blockchain technologies. Security is very important, but users find it as a very tedious job if every day it take somewhere around 20 minutes for a transaction to go through.

There is still a bit of work that needs to be done where our digital currencies are inheriting the problems that the banks could never solve. Banks move digital money and they've been doing so for quite a long time, but security measures are applied by banks in the form of people, account managers and also insurance. Usually the users are paying between three and five percent on the Visa and MasterCard transactions, this covers the users for fraud detections or any anomalies due to the security issues these credit card companies encounter thousands of times per day.

9. Cryptocurrency Security

With all of the hacking going on in the cryptocurrency world right now and a huge influx of newcomers coming to the market. One of the real downfalls of individuals engaged in this space is not really losing their cash from exchanging however from losing their crypto or being hacked. In this way, regardless of whether a user is new or a veteran that has gotten totally self-satisfied as of late, it should begin with passwords. The passwords on most stages and trades will request for a password combinations using a lowercase, a capital letter, and a number character to put in the secret phrase. This is genuinely conventional that can possibly accomplish for a less imperative record like Facebook or Instagram.

Developers may either use something many refer to as a dictionary calculation which in reality simply like a Blockchain hub works through several conditions which take one moment to split into a secret word, if not they'll presumably simply distinguish it from a secret phrase which is a word vigorously connected with the particular individual.

It is better to make passwords around 16 digits in length with a blend of irregular letters meaning literally nothing. Irregular capital letters in the middle of words will still, at the end of the day, throw in some exclamation marks, question marks for good measure. It sounds simple, but this often is forgotten due to laziness and wanting to get set up faster.

A two-factor authentication is the second form of password basically a backup password and secondary measure of security. Once an individual has logged into their platform with the usual username and password one can create a final barrier of entry via two-factor authentication, which is an automatically generated numerical code for the specific platform one is using. This code will be timed depending on how set it up is done, it could last anywhere from several seconds to a minute once the time is up the code refreshes and changes to a new one and entering the old code that's expired will no longer work. This is achievable through the mobile apps available on both iOS and Android, the Google Authenticator app and the Orpheum.

Every cryptocurrency platform should offer the option of two-factor security. Once the app is downloaded, simply scan the QR code for the relevant platform and it will generate an ongoing numerical password for every individual login. This is especially crucial in cryptocurrency to where somebody can easily have users' passwords and usernames. However, the two-factor would stop them dead in their tracks as they would need their phone or device running the app to then breach it and gain full access.

Finally, private keys, when any user is holding cryptocurrencies in a wallet, an auto-generated private key is the make or break between the user's wallet being compromised or not. This is the single most important piece of information that one needs to keep as secret at all costs. Once this is in the hands of potential threats then it's already too late.

The usual method people choose is to simply write stories in their phones notes folder or on their computer. This is almost insane as any person would just increase the likelihood of being hacked. If anything, it would actually be much wiser to store this information on a piece of paper as an example this way one can copy and paste their key into a Microsoft Word document and print out several copies to store it in a safe location where it fits best.

The Blockchain is the increasing list of records called as blocks that are getting linked and would be secured using Cryptography. It allows peer-to-peer transactions with no involvement of any third party and also makes manipulation of data very difficult.

Every technology has advantages but at the same time possess some limitations that need to be considered while using that technology. The limitations of Blockchain technology are:

- *Each of technical knowledge.* Despite Blockchain's increasing quality, still several investors are not awake to all the technical terms and additionally, there's no correct documentation that helps users to urge careful information. Due to that, investors are not able to raise queries directly or get their doubts resolved.

- *Fewer people are available with proper certification.* As compared to the demand for Blockchain today, the consultants at this technology are quite a few. There are people who can provide knowledge about the Blockchain but, they are not fully well versed with the technicality involved within.
- *Scalability.* This is the major limitation in the Blockchain world where are the transactions made in the network should be verified by each and every node. By this, the speed of the transaction will be limited. To overcome these scalability issues, they are working on distributed ledger technology that is based on the Hyperledger Fabric.
- *Less Privacy.* Since it is a distributed ledger, even though the identities are unknown but still with the transaction patterns it is possible to link the user identity for that address and information about the user can be obtained.
- *Security Concerns.* The Blockchain is the network of people. If half of the people get dishonest and get into the habit of manipulation of data. Then it becomes the reason for the failure of a complete network. So, they need to observe closely to avoid misusing the data and ensure security.
- *Complexity.* Blockchain technology cannot be easily understood by people as it involves a lot of mathematical calculations. With its complexity, it can be understood overnight.
- *Manual Errors.* Manual errors can bring out the outdated log information and can also create mismatching data while entering into the database. In order to have valid data, the data needs to be verified. Due to which these 2 phrases “garbage in”, “garbage out” is used in the context of the Blockchain.

10. Key Advantages of Cryptocurrencies

The total variety of bitcoins is fastened, and Bitcoin would not depreciate because of inflation, not like national currency. Stealing cryptocurrency could be a terribly troublesome task that offers a bonus in developing countries wherever theft could be a major drawback. Many citizens of developing countries head to work abroad or in alternative cities.

They transfer cash to their families each month by Western Union or bank transfer (if the family includes a bank account) however face terribly high bank charges and conversion fees (up to 20%). Cryptocurrency transfer has no fees, thus solving this problem. Many citizens of developing countries do not have a checking account or Mastercard. However, more folks have smartphones with a mobile cash account which will be enclosed within the cryptocurrency system. It only takes a few minutes to open a crypto wallet; furthermore, doing so is completely free.

11. Recommended Problem Solution(s) Approach:

Based on the discussions and findings on the key challenging areas related to security concerns in adopting cryptocurrency, below are some of the solutions approaches to overcome those challenges and make use of cryptocurrencies worldwide in a more efficient and secured way:

Technical knowledge and Resource creation

The nation governments need to realize the fact that cryptocurrencies and Blockchain technologies are future trends and anticipate the demand to fulfill these requirements. Therefore, the government should encourage the companies in these businesses to create enormous amount of knowledge creation as well as produce technical experts to handle the operations as well as support.

There has to set up a trusted certification authority to measure the expertise and knowledge in this area. International councils of countries should be formed to regulate and protect the benefits of their users and tradeoffs.

Scalability

As scalability can be seen as an issue with cryptocurrency and even more with Blockchain technology since they cannot carry too many small transactions due to their small block sizes. The transmission gets delayed due to its limited block size. Making more efficient and serialized transactions can help in solving the issue. Mini-Blockchain can be developed and synced with the network and small proof protects the loss of security and all the nonempty addresses can be stored in a separate database to solve the coin ownership data loss. Some of these enhancements can potentially offer quicker network synchronization, faster transactions, more spaces for the blocks and increase anonymization.

Privacy Issues/Anticipate Primitive Breakage

The user privacy leaks and primitive breakage are the major security concerns and they can even occur after the transaction has happened and businesses also do not want that their transaction histories for any tradeoffs have been made public. The use of more secured public key/private key combinations can strengthen the security challenges. According to the research work done by Gao, Yu-Long and others (February 2018), they proposed a signature scheme based on lattice problem as an enhanced security feature. They also proposed a lattice basis delegation algorithm to generate private keys to select a random value and sign message.

The adoption of Post-Quantum Blockchain includes Hash-based cryptography, Lattice-basis cryptography, Code-basis cryptography, Multivariate cryptography and other post-quantum cryptography algorithms. Post-Quantum Blockchain (POB) is a combination of post-quantum cryptography as well as Blockchain as that doubles the ability to resist the traditional attack methods.

The companies should provide an algorithm where they should be able to hide users' information and when they use a particular address, it does not reveal that address details. Rather to avoid primitive breakage, users should get restricted in reusing the same address as it also protects their privacy. By doing so, if one scheme is broken, the other scheme is still protected by hash values.

Key Management/User Anonymity

Private Key Management has been one of the major security concerns to trust cryptocurrency and even for Blockchain as they directly deal with identity authentication and information encryption. Therefore, appropriate use of mathematical algorithm and computer technology must be done to ensure it allows users with their privacy and data security. Some of the recommended approaches are:

- To provide a minimum number of transactions block wise to make it difficult for the attacker to perform pre-image attack against the mining header target such as Proof of Work with the use of coin-based transaction.
- Introducing new address types with a stronger hashing and signature schemes can help alleviate the issues arising due to a weakened hash or signature scheme while migrating from old addresses
- Try to avoid nested hashes for Main Hash and implement a redesigned headers and transactions without use of any old primitives.

Mixing Services

Increased use of mixing services can reduce the risk of users' anonymity being compromised. There are several methods being used as part of mixing services to protect users' identity. For an example, a decentralized and online peer-to-peer mixing cryptocurrencies such as Bitcoin allows online payments to be sent without any intermediation. Peer-to-peer mixing protocols allows to eliminate the mixing fee and without any intermediation, makes each individual participants as anonymous and a series of transactions privately permutes the ownership. It should allow the user to deny signing their transaction if they found that the desired output address is not included.

Mixing overlay protocols can hide the flow of funds among the participants and process advanced cryptographic techniques to provide a strong user privacy through it mixing design where no participant can link any input to output addresses. In a decentralized mixing, each party encrypts the recipient addresses in layers under the keys of all parties to the user's right and sends it to all the other user addresses to the next party. This next party then eliminates the outermost layer and then the final party can compile all the cryptocurrency transaction and post them on the Blockchain.

Once everybody sees their recipient address, they sign the transactions. Similarly, Bitcoin Mixing methods, centralized mixing methods are also used to protect users' privacy, security, and anonymity.

Double Spending

Double Spending is one of the challenges of cryptocurrency. It refers to a transaction failure where the coins are spent in more than one transaction. This creates a problem with real-time transfers. Use of Proof-of-work based Blockchain can ensure that all the transactions and the order of their executions are available to all the nodes and they can be verified by the entities. Timelocking protocol is another approach to ensure fair payments. Timelocking protocol allows a payer to reclaim the payment within a specific time window if that payment has yet not been spent. Many Blockchain-based applications like Bitcoin and others have the feature of Timelocking.

12. Future Research Direction

This section outlays and discusses about the future need of research direction for cryptocurrency to overcome some of the crucial open issues. There have been researches going around worldwide and cryptocurrency companies are working hard to strengthen their cryptocurrency transactions more efficient, easy, and secured by removing complexities and enhancing better security features. However, they still need to consider future research work to provide the unique aspects and grow the business as well as use of cryptocurrency.

Looking at the way cryptocurrency technology is shaping up, the focus of the business companies as well as researchers will be more on two main concepts; distributed ledger technology (DLT) and Blockchain.

Distributed Ledger Technology (DLT)

Distributed Ledger Technology looks very promising, but it is still in its very early stage of developments. The companies have to find user-centric solutions that benefit their users without having many risks or concerns. With further development of DLT, there will be a combination of artificial intelligence, robotics, cloud computing, digital payments and machine learning with DLT can be seen in the future.

In a short-term future from now, the third-party intermediaries will be cut with the use of distributed ledger technology. This will further reduce the overall costs, eliminate the abuse of power and readjust commercial benefits to both businesses as well as users.

Blockchain

Blockchain is essentially a part of Distributed Ledger Technology (DLT) which is already in use. It has already made significant impact and providing efficient digital solution as a means of commercial transactions and payments. Blockchain has been established and accepted widely by both the technology industry as well as finance industry; for an example Bitcoin. However, the researchers and even cryptocurrency companies are still working hard to get the best solutions to overcome some of the security, privacy, authenticity, confidentiality, as well as integrity issues remain around Blockchain.

Researchers, Eyal and Sirer believe that Blockchain is a decentralized system but the miners are centralized, hence selfish miners may get a value more than its fair amount since Bitcon is not incentive-compatible option. Hence, the companies need to work on a direction to make the miner system more decentralized as an act of balancing. Future work may be seen with improving the testing scenario with Blockchain technology. Since each cryptocurrency developed using Blockchain till date have their own way of performances.

Blockchain testing mechanism should be considering as a priority requirement as it is possible that developers may avoid the performance related challenges to attract investors. Further, there is a possibility of seeing a combination of data analytics and Blockchain since Blockchain technology is more distributed, secure, and immutable, it can be used to store data and information which is difficult to alter by anyone. Since Blockchain technology offers a secured design to store the data as well as the information stays in the same format till the network exists, there will be an entrant of Blockchain technology with an increased use in various industries like retail, healthcare, public administration.

It will be more helpful in preventing hacking attacks and data loss. Even down the line, a combination of Blockchain and big data analytics can be utilized to identify the patterns in consumer spending and quick identification of risky behaviors or transactions that reduces the real-time transaction costs. Also, it is expected that Smart Contracts can replace traditional hardcopy contract in near future; however, it will require transparency and trust between both the contractual parties for digital assets.

Internet of Things (IoT)

Besides financial transaction, future engagement can be seen with Blockchain based Internet of Things (IoT) to handle security and privacy challenges as Blockchain technology uses participating nodes resources and decreases delay by removing many-to-one traffic problems. This may further benefit the user with their real identity is not being disclosed and they are interacting with a generated user address.

Regulatory and Legal Compliances

Some of the rules and regulations will be disregarded and will leverage new ways of using the technology with future enhancement. Furthermore, the banks, financial institutions, as well as governments will have to revise their regulatory laws and terms. Government regulations will have revised and stricter regulatory controls to prevent criminal activities over the cryptocurrency networks. It is expected that a paradigm shift will be seen in the financial system towards fairer and more transparent for the general public with the use of cryptocurrency.

13. Conclusion

The main focus of the researchers of this paper was to understand and analyse the current scenario of cryptocurrency in the global market, how it has been perceived in some parts of the world, complications, and challenges faced by them in the adoption of cryptocurrencies. Also, it was evident that cryptocurrency despite having some core advantages is not yet accepted globally. Some of the countries have even banned the use of cryptocurrencies looking at the complexities and security aspects associated with it. Though, the researchers were also able to research and analyse the cryptocurrency built using Blockchain technology and the potential of Blockchain technology. However, cryptocurrency is indeed very vulnerable in today's date, even though it has gone through many improvements over the years.

While security, privacy, and criminal activities remain as primary concerns to adopt cryptocurrency, Blockchain technology provides more secured structure and algorithm for cryptocurrency. However, the future of cryptocurrency is still uncertain, and it is vulnerable from security aspects with a threat of innovative attacks to come out.

The researchers also offer some initial recommendation solutions guidelines to make the cryptocurrency easier and more secured. The researchers of this paper believe that future research work should involve the cryptocurrency developers and user communities to lay out a join plan to enhance more secured and user-friendly version of cryptocurrencies with the use of growing technologies like Blockchain as well as Distributed Ledger Technology.

References

[1] Amanzholova, B., & Teslya, P. (2018). *Threats and Opportunities of Cryptocurrency Technologies*. 14th International Scientific-Technical Conference APEIE.

[2] Baliga, A. (2017). *Understanding Blockchain Consensus Models*. Retrieved from: https://pdfs.semanticscholar.org/da8a/37b10bc1521a4d3de925d7ebc44bb606d740.pdf

[3] Betts, B. (2016), *Blockchain: the missing link in cloud security*. Retrieved from: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=3&sid=5f3dfc33-69e7-4d7f-8e3b-6d8d992455c5%40sdc-v-sessmgr06

[4] Bruce, J. (2014). *The mini blockchain scheme.*

[5] Decker, & Wattenhofer, R. (2014). *Bitcoin Transaction Malleability and MtGox*. European Symposium on Research in Computer Security (ESORICS).

[6] Dumitrescu, G.C. (2017). *Bitcoin – A Brief Analysis of the Advantages and Disadvantages.* Global Economic Observer; Bucharest Vol. 5, Iss. 2.

[7] Eyal, I., & Gün, S.E. (2018). *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*. Communication of the ACM.

[8] Gao, Y.-L., Chen, X.-B., Chen, Y.-L., Sun, Y., Niu, X.-X., & Yang, Y.-X. (2018). *A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain.*

[9] Giechaskiel, I., Cremers, C., & Rasmussen, K. (2018). *When the "Crypto" in Cryptocurrencies Breaks: Bitcoin Security under Broken Primitives.* Copublished by the IEEE Computer and Reliability Societies.

[10] Giechaskiel, I., Cremers, C., & Rasmussen, K.B. (2016). *On Bitcoin Security in the Presence of Broken Cryptographic Primitives*. European Symposium on Research in Computer Security (ESORICS).

[11] Grech, A., & Camilleri, A. F. (2017). *Blockchain in Education.* Inamorato dos Santos, A. (ed.). Joint Research Centre.

[12] Guo, Y., Bao, Y., Stuart, B., & Le-Nguyen, K. (2017). *To sell or not to sell: Exploring sellers' trust and Risk of Chargeback Fraud in cross-border electronic commerce.*

[13] Halaburda, H. (2018). *Economic and Business Dimensions Blockchain Revolution without the Blockchain?.* Communication of the ACM

[14] Highwater, T. (2018). *Eight reasons to use cryptocurrency payments in 2019.* Retrieved from: https://news.bitcoin.com/eight-reasons-to-use-cryptocurrency-payments-in-2019/

[15] Holotescu, C. (2018). *Understanding Blockchain Opportunities and Challenges*. The 14th International Scientific Conference, eLearning and Software for Education Bucharest.

[16] Li, H., Liu, D., Dai, Y., Luan, T. H., & Yu, S. (Jan/Mar 2018). *Personalized search over encrypted data with efficient and secure updates in mobile clouds*. IEEE Trans. Emerg. Topics Comput., vol. 6, no. 1, pp. 97-109.

[17] Liu, J., Li, W., Karame, G., & Asokan, N. (2018). *Toward Fairness of Cryptocurrency Payments.* Copublished by the IEEE Computer and Reliability Societies.

[18] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. & Savage, S. (2016). *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*. Communication of the ACM

[19] Mike, O. (2018). *How secure is blockchain really?*. Retrieved from: https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

[20] Milutinović, M. (2018). *Cryptocurrency*. Ekonomika, 64(1), 105-122. Retrieved from http://scindeks.ceon.rs/article.aspx?artid=0350-137X1801105M

[21] Mukhamedov, K.S., & Ritter, E. (2005). *Analysis of a Multi-party Fair Exchange Protocol and Formal*. Proceedings of the 9th International Conference on Financial Cryptography and Data Security (FC 05), pp. 255–269.

[22] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

[23] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press. Retrieved from: https://books.google.co.in/books?hl=en&lr=&id=LchFDAAAQBAJ&oi=fnd&pg=PP1dq=cryptocurrency+by+narayanan&ots=ArpG9V0HkK&sig=GQoJZ4Ae9Tsn_n3w7MGEtsDA_Y#v=onepage&q=cryptocurrency%20by%20narayanan&f=false

[24] Oh, J. H., (2018). *The Foreign Exchange Market with the Cryptocurrency and Kimchi Premium*. Retrieved from https://www.econstor.eu/handle/10419/190386

[25] Rahouti, Mohamed, Xiong, Kaiqi, & Ghani, Nasir. (Sept 2018). *Bitcoin Concepts, Threats, and Machine-Learning Security Solutions.*

[26] Sarthak, M. (2018). *How Blockchain can Disrupt the Card Payments Industry – And Why It Hasn't Already.* Retrieved from: https://hackernoon.com/blockchain-for-disrupting-card-payments-dff87840313c

[27] Sayed, M. N., & Abbas, N. A. (2018). *Impact of crypto-currency on emerging market focus on gulf countries*. Life Science Journal, 15(1). Retrieved from: http://www.lifesciencesite.com/lsj/life150118/16_33506lsj150118_92_97.pdf

[28] Seaman D. (2014). *The Bitcoin Primer: Risks, Opportunities, And Possibilities.* Amazon Digital Services LLC.

[29] Shukla, V., & Chaturvedi, A. (2018). *CRYPTOCURRENCY: CHARACTERSTICS AND FUTURE PERSPECTIVES. EVERYMAN S, 77*. Retrieved from: http://www.sciencecongress.nic.in/pdf/e-book/june-july-18.pdf#page=14

[30] Tiwari, N. (2019). *The commodification of cryptocurrency.*

[31] Vallois, V., & Guenane, F. A. (2017). *Bitcoin transaction: From the creation to validation, a protocol overview,* in Proc. Cyber Secur. Netw. Conf. (CSNet), pp. 1-7.

[32] Waldo, J. (2019). *A Hitchhiker's Guide to the Blockchain Universe*, Communication of the ACM

[33] Weber, M. (2018). *An Advisor's Introduction to Blockchain*. Society of Financial Service Professionals.

[34] Yuan, Y. & Wang, F. (2018). *Blockchain and Cryptocurrencies: Model, Techniques, and Applications.* IEEE Transactions on system, man, and cybernetics: system, Vol. 48, No. 9.