

Bitcoin and Digital currency: Difficulties, Open Doors and Future Works

Sulthan Taqi Sampoerna Alfian¹, Fathur Ichsanudin²

Management Retail, University of Raharja¹

Social science and political science, University of Muhammadiyah²

Modern, Jl. Jenderal Sudirman No.40, RT.002/RW.006, Cikokol, Kec. Tangerang,
Kota Tangerang, Banten 15117

Jl. Perintis Kemerdekaan I No.33, RT.007/RW.003, Babakan, Cikokol, Kec. Tangerang, Kota
Tangerang, Banten 15118
Indonesia

e-mail: sulthan@raharja.info, ichsanudin.fathur1@gmail.com



Author Notification
07 July 2022
Final Revised
09 July 2022
Published
13 July 2022

Alfian, S. T. S., & Ichsanudin, F. (2022). Bitcoin and Digital Currency: Difficulties, Open Doors and Future Works. Blockchain Frontier Technology, 2(1), 50–57.
DOI: <https://doi.org/10.34306/bfront.v2i1.107>

Abstract

Bitcoin and other conspicuous digital forms of money definitely stand out enough to be noticed since the most recent quite a while. All around the world known as advanced coin and virtual cash, this cryptographic money is acquired and exchanged inside the blockchain framework. The blockchain innovation taken on in utilizing the digital currency has caused a stir inside the financial area, government, partners and individual financial backers. The ascent of the cryptographic money inside this long time starting from the beginning of Bitcoin in 2009 has surprised the market. Cryptographic money is expected as the future cash that would supplant the ongoing paper money around the world. Despite the fact that the interest has grabbed the eye of clients, many don't know about its chances, disadvantages and difficulties for what's to come. Explores on cryptographic forms of money are as yet missing nevertheless at its outset stage. In giving significant aide and view to the scholarly field and clients, this paper will examine the valuable open doors in digital money, for example, the security of its innovation, low exchange cost and high venture return. The inventiveness of this paper is on the conversation inside regulation and guideline, high energy utilization, probability of crash and air pocket, and goes after on network. The future endeavors of cryptographic money and its application will be methodically evaluated in this paper.

Keywords: Blockchain, Digital currency, Future Works, Bitcoin

1. Introduction

: Starting from the commencement of the government issued currency, individuals have been involving it for regular exchange. Exchanging and exchange has been a lot more straightforward. In the year 2009, after the worldwide accident of 2010, the principal type of cryptographic money arose as Bitcoin. It was first presented as a mysterious gathering or person that has presented Bitcoin as the primary advanced money for simpler everyday exchange from one person to another. Bitcoin is worked without go between like banks and financial organizations. It is a type of shared exchange, without the need to uncover one's personality for an exchange to occur. Dissimilar to the ongoing practice, the bank capabilities as the broker or the go-between, knows the character of purchaser and merchant, subsequently causing the issues of individual information insurance. The Bitcoin stage has made the exchanging and exchange of cryptographic money a lot simpler and more free,

without compromising individual data and subtleties. To some, picking this technique for exchange has qualified them to execute uninhibitedly and namelessly.

Bitcoin is the primary computerized coin on the planet to have utilized the blockchain stage. It is made inside an exchange log with PCs taking an interest across an organization. This blockchain has one of the greatest security frameworks by not permitting fraudsters to utilize the money at least a couple of times. The blockchain convention depends on verification of work where it guarantees diggers unite to this construction. The computational activity is known as hashing where the term hashing power alludes to the computational force of mining the monetary forms. The framework in the digital currency market is fairly complicated and very challenging to comprehend, in any event, for the players in the business and specialists concentrating on in this field. There have been numerous specialists uncovering the advantages of Bitcoin, for example, security, low exchange cost, exceptional yield and with respect to elective instruments for a country's bailout system and use for representatives' wages. In spite of that, there are additionally scientists highlighting the gamble and downsides of utilizing this computerized coin, in terms of absence of guideline, high power charge because of energy utilization, absence of safety and different issues like obscurity and exchanging cost.

2. Research Method

In this beginning stage, the promotion was trifled with just from the PC fans all over the planet. In 2010, Mt Gox, a Japanese organization, made a stage involving Bitcoin as an exchanging system with 20 coins changing hands at 4.951 pennies. The absolute volume was around one U.S dollar. As the utilization of Bitcoin had expanded, the cost had heightened immensely, and at the time this paper was composed, the cost had flooded definitely to the U.S dollar of 6,777. As indicated, the premise of the bitcoin esteem depends on shortage. It fills in as the establishment to put a worth to any type of cash. In the ongoing act of utilizing the government issued money, the financial power or the national bank holds and saves the cash. National bank of a nation has the influence in changing the course of cash and its outright amount. The bank can deliver just a restricted measure of this paper cash for controlling the monetary economy of a nation, hence making shortage. This shortage will be kept in the bank accounting and will be protected by the lawful guidelines. The unavoidable issue that emerged as Bitcoin was presented, are these digital currencies considered as genuine cash?, history has illustrated that cash should have the accompanying models: (1) A store of significant worth. It is a buying power that clients can control to purchase products in the ongoing opportunity to see what's in store. (2) A mechanism of trade. The capacity to make installments and (3) A unit of record. The worth that can be estimated of any products available to be purchased. Cash hypothetically should meet this multitude of rules yet it isn't generally the situation. Examining Bitcoin and other cryptographic money in their ongoing structure, every one of the three models are easy to refute. One can propose that it has a store esteem because of the capacity for buying power, however because of vulnerability, one can't gauge whether Bitcoin can be utilized in the future as it is being utilized at this point. For mode of trade, some can legitimize that digital currency can be utilized for a vehicle of trade, yet to others the merchandise that can be traded are restricted. Assuming this large number of three models are set to be the pre-necessity for any ware to be given the height of cash, hence it ought to be acknowledged inside the setting of its utilization and application. detailed that cigarettes met this multitude of standards during the difficult season of The Second Great War where detainees in war camps exchanged it for exchange. Further back in time, cooking salt can be viewed as having esteem in the hour of the Roman domain where the soldiers' compensation were paid in salt. With respect to digital currency, it very well may be viewed as cash to individuals who are PC and web empowered. The issue lies in the way that a little part of individuals overall approaches web gadgets. Hence, inside this unique circumstance, like the detainees in the conflict camp and the Roman soldiers, digital money just is restricted to

those approaching the web. revealed that around 20,000 Bitcoin holders in the Unified Realm with just 300 exchanges every day.

This number would be much more modest in arising and non-industrial nations because of the absence of web access. proposed that digital money, especially Bitcoin, is all the more a stage for installment as opposed to cash because of its continuous convertible to a traditional money in fixed esteem. This digital money is not the same as different resources concerning its portfolio examination, risk the board and opinion investigation. Contrasted with different resources, for example, gold, property, stocks and value, cryptographic money has a comparable portfolio as far as having specific worth. Digital currency notwithstanding, looks like individuals' feeling as when the worth lifts with an ever increasing number of individuals ready to acknowledge them as installment. These distinctions set out different open doors in the market where financial backers and partners can profit from it. Accordingly, to recognize digital currency as the substitution for the government issued currency in the present financial matters is as yet untimely and requires further grasping in application, hypothetically and basically.

3. Results and Discussing

How was digital currency at first acquired or got? As to government issued currency, it is given by the national bank, while digital money is made by mining through the blockchain utilizing cryptography innovation. This is the strategy for giving new cryptographic money. The blockchain framework comprises clients, designers, diggers, hub maintainers and the communications that guarantee the usefulness of the circulated records. Such a mining process expects excavators to have capital costs in buying the product and equipment. The product incorporates GUIMiner, BFGminer and CGminer are the models utilized in Bitcoin mining. While the equipment's are AntMiner, Avalon and ASICMiner. Mining of different monetary forms that utilizes various calculations requires the utilization of very good quality and high velocity realistic cards. For another excavator, one requirement is to enroll a wallet and scrambled banking on the web that can store and acknowledge the digital currency. At the point when an excavator can settle the riddle in the blockchain framework, the computerized coins will be compensated and moved to the wallet that has been foreordained before. As per large numbers of the digital money conventions, how mining works is by approving exchange by connecting to the block that was acknowledged before. The blockchain innovation will keep each exchange in its unit. An interesting ID is relegated to each block and the block going before it. This is known as the evidence of work convention. Evidence of work is a convention of checking an exchange and illuminating others about it. Clients or excavators need to take care of business in approving or sealing that they are the genuine characters. These works rotate around calculation and astound that can be addressed by PCs numerical interaction. Evidence of work adjusted in digital currency working standard is to supplant the unified installment framework forced by the financial framework. The primary premise of this framework is to charge the client for example the help requester in taking care of an issue that is viewed as difficult to tackle contrasted with checking it. By this, verification of work standard would have the option to restrict the admittance to some random assistance in mining and exchanging the digital money. Excavators would need to tackle the riddle implanted in the block, which contains the hash of the past block, the ongoing block exchange hash and address that will be compensated after the riddle is settled. This is the fundamental of the mining system. This thus made a block chain, a hint of the exchange that occurred. This blockchain innovation will forestall any fraudsters to twofold spend of digital money by altering the exchanges in the record.

- Critics of Cryptocurrency

There have been significant pundits of cryptographic money, one of them is whether it is a type of a resource cash. In its ongoing structure, being able to perform financial exchange, bitcoin and digital forms of money are a lot nearer and meet the meaning of cash. Despite the fact that cryptographic forms of money really do have total measures of the three fundamental

attributes of cash which are store esteem, unit of record and strategy for exchange, it has a greater part of the components.

- Opportunities and Advantages

Being a somewhat new product, the chances of cryptographic money looks encouraging. Regardless of having raised as far as its cost and worth, the leafy foods' future open doors are as yet being pursued. The accompanying article examines the sensible chances of cryptographic money for the clients, financial backers and including the public authority.

- Secure Technology

The blockchain is considered to be perhaps of the best stage and most modern innovation since the revelation of the web. It gives proficiency to online exchange, in terms of its security and classification. For their situation concentrate on inferring that, aside from empowering the utilization of cryptographic money, the blockchain can safeguard private data and furthermore kill the intermediation from any establishments. Despite the fact that there were reports expressing that Bitcoin was found to uncover 40% of the client's personality. This report was guaranteed after the clients had followed the proposal set by Bitcoin. This issue of personality security is significant in view of the highlights of the cryptographic money that safeguard the client's profile by decentralizing framework. Two blemishes in this study is that it doesn't utilize real blockchain framework however recreation, and the reenactment was just finished in one staff just consisting of understudies. Other than this, no different examinations up to writer's perusing that have uncovered the blemishes of utilizing Bitcoin and cryptographic money that uncovered the gamble of uncovering client's very own data. One of the dangers in claiming computerized coins is twofold exchange, and that implies someone can give two exchanges lined up by conceding similar coin to two unique beneficiaries. On account of unified and online exchange, the bank functional framework can identify such dubious movements. Blockchain innovation is exceptionally good. Fraudsters can not perpetrate such wrongdoing since one can't change nor approve a few records simultaneously. As indicated, security of the digital money can be broken on the off chance that fraudsters can handle a colossal sum stake in the confirmation of work hash influence. Hash power is the figuring power controlling ability.) expressed that hash power is the power required by the digital money organization to ceaselessly work. The hash power is included in a normal of 10 minutes that power is consumed. By controlling most of the stake in the confirmation of work, fraudsters can twofold spend on a similar block by covertly setting up the blockchain branch ahead of time earlier communicating it to the chain organization. Hypothetically, misrepresentation should be possible in an enormous scope given that fraudsters can handle at specific levels of the hash power. From Bitcoin's calculation of binomial irregular walk, fraudsters can twofold in the event that they control 51% of the registering power. In the evidence of work convention, the check regardless of whether there is twofold exchange depends exclusively on the hash power, rather the chance of numerous phony characters. This has guaranteed that the issue of fraudsters having the option to control a larger part of the hash power is subverted by the check of other techniques instead of depending entirely on the hash power. The supposition that will be that it is considerably more troublesome in controlling greater part of the framework hash power than controlling the characters of the larger part. Cryptographic money calculation is more efficient and is superior to utilizing Visas. Despite the fact that it is as yet understudied, digital currency has a lot of lower handling charges with the solid exchange it gives. made sense that utilizing digital money is safer while doing exchange. The component of moving digital money is by verification by the purchasers and merchants. The verification between the two players will forestall fraudsters in fashioning any new exchange or postponing any discount exchange. Contrasted with Mastercard, these products have occurred and will keep on continuing because of its system. The innovation behind Mastercard exchange is working inside the cardholder, vendor, dealer bank, Visa organization, giving bank and specialist co-op. For any single exchange, the cycle is more going on under the surface. It needs to go through to this large number of elements before an exchange can be settled. Fraudsters and a chance for committing extortion can exist in any of these stages. Despite the fact that particular measures have been assumed in lessening praise card extortion, the framework is more defenseless when contrasted with blockchain. The framework applied by the Mastercard

innovation is as yet not secure as the cryptography innovation has by the digital currency. expressed that in spite of being algorithmically muddled, the blockchain framework isn't perplexing. The intricacy just exists in the hub and numerical riddle that will be addressed by the mining system. Other than that, the blockchain innovation gives helpful capabilities to all clients. It is probably not going to go before a turbulent framework in light of the strength and irreversibility. The records of advanced reports on the web and recognizable proof are all around safeguarded inside the blockchain framework until further notice and the not so distant future.

- Cost of Transaction

Since the beginning of time, individuals have been involving a financial structure for everyday exchange of some sort. As soon as an exchanging framework, the bargain framework had got the business rolling, where individuals traded or dealt their merchandise, with the understanding from the two sides. As the time changed, the government issued currency intended for individuals to exchange easily, without carrying enormous items to exchange. As the world enters the 21st hundred years, digital money has overwhelmed the market. There have been enormous global organizations involving Bitcoin as their type of cash, and in any event, utilizing it to pay the representatives month to month compensation. As the ongoing expense of exchange, digital money and Bitcoin exchange charges are lower contrasted with other ordinary monetary standards. With the noticeable highlights of digital currency, decentralized and liberated, accounted for its minimal expense of exchange. There have been extensive issues in the ongoing installment framework that is being polished by credit and finance cards. The interest being charged for clients who default on their installments is too high and that can endanger a client into monetary sadness. This has not been the situation for digital currency, where exchanging happens when start to finish clients concurred and really at that time will settlement of cash be made. Furthermore, digital currency can be worked for 24 hours per day, 7 days seven days consistently. The information value is accessible quickly by which anybody on the planet can exchange with next to no cost as long as the web is available. As the world is besieged with late improvement of the web of things (IoT) and dependence on large information, being able to exchange without time constraint is a simplicity for clients. This strategy for installment would work with the more youthful age who are supposed to become entrepreneurs and working inside their own time span, without joining with traditional working hours. This approach to exchanging is likewise appropriate for the web clever without forking out extra expense that accompanies utilizing other installment frameworks.

The pundits encompassing digital money have been raised starting from the primary day of its beginning. The criminal behavior allegation of digital money was acknowledged when the Silk Street outrage halted its activity by the FBI. Silk Street was a well known market where clients exchange Bitcoin. Silk Street was charged as a stage for business including drug and other criminal operations. In any case, the closure of Silk Street was not the shortcoming of Blockchain nor digital currency. All things considered, it was the hoodlums and fraudsters who had taken advantage of this innovation for their own desire for benefits, very much like other stages that can help them. The second such case was Mt Gox where it lost cash totaling 350 million bucks . One would have envisioned, before a framework is completely evolved and turns into a dependable and vigorous innovation, time factor is an immense thought. Digital currency calls for more than adequate investment before it very well may be utilized and applied by the mass individuals all through the world. Indeed, even Paypal, the electronic installment framework that was presented in the year 1999 had a few times been the objective for fraudsters. It had really been gone after something like multiple times subsequent to being completely strong and had laid out as a productive and dependable electronic installment framework on the planet. As the historical backdrop of the Bitcoin is concerned, the air pockets are impacted by the hypothesis and cost drop was impacted by the intercession by the public authority and focal money related organizations. Subsequently, for the premium of general society in expecting the advantages of digital money, the government ought to create a legitimate strategy and guideline that can shield the public premium as well as principal players in the financial market. A settled market would guarantee that the monetary strategy of a nation can be adjusted without curbing the collaboration from the national bank. This really

relies on how the public authority follows up on the ongoing digital money market, either leaning toward or decreasing its presence for the last time.

- Improvement and Future Work on Cryptocurrencies

It is evident that the rise of digital money will assume a huge part on the planet's financial texture. It is the way that each market analyst, specialist, and financial backer needs to act and take significant measures to fortify their insight on blockchain innovation overall. As digital money has not yet arrived at development in terms of time period, further examinations on its innovation, potential and hazard ought to be contemplated to guarantee that the open doors are not only a simple accident. Likewise, the forthcoming difficulties don't alleviate partners into the dejection of monetary disappointments. Future examination on diminishing the 51% assault on the blockchain mining organization ought to be additionally improved. The security convention ought to be better, in the event that it is not the equivalent than the traditional concentrated financial framework in safeguarding the client's money related resources. Security part of clients warrants the earth shattering tribute from the players in this new industry so the certainty and trust of the blockchain innovation would permit it to be the standard for clients in doing their day to day exchange through the web. In lessening the expense of mining the cash, a proof of stake would give lesser energy utilization in mining these computerized coins. In confirmation of stake philosophy, an individual needs to approve the coins that they own and the sum. The individual requirements to make an exchange of their coins that they ship off their record as a prize with the data of predefined rate. The confirmation of stake looks like a wager-like plan that gives a similar opportunity to all excavators. Besides, a half breed technique that comprises both verification of work and evidence of stake had been proposed, by compensating part of the confirmation of work to all hubs that are dynamic and simultaneously the stake decides the ticket acquired to all pools. proposed Verification of Movement (PoA) that joins the evidence of work and confirmation of stake. In PoA, the movement term alludes to dynamic clients that keep up with the full web-based hub and the one that ought to be compensated. Conflictingly, in confirmation of stake, disconnected clients can in any case amass the coins over the long run and this can prompt twofold expenditure of a similar block. PoA gives much better security in confronting future danger on digital money. It has a greater extra room and the organization correspondence allows low punishment. Additionally, PoA likewise has low exchange charges, consuming less energy and the geography of the organization can be made do. Consequently, PoA electives act as a superior stage for digital money because of its capacity to battle twofold spending and in particular the expense in securing the cryptographic money contrasted with confirmation of work. The market has been plunged with numerous new digital forms of money that had previously made it into the market and there are many actually ready to be delivered. There have been many arising monetary standards that are testing and contending Bitcoin in terms of its cost and market capitalization. Despite the fact that at the hour of composing, just Ethereum and Wave had arrived at three figure costs. Bornholdt proposed a model called Moran process on new arising cryptographic money. The model does recreation available where the monetary standards are exchanged. The model can reenact the steady pace of new mined coins, exchanging exercises of the specialists and the correspondence among clients exchanging on the business sectors. Every one of the monetary standards are tradable among themselves, with the affirmation of the record holders. It was likewise found that Bitcoin can be exchanged with different coins and the future could see that the exceptionally justified Bitcoin be supplanted by other entrancing coins that might have better elements. In this way, concentrating on these elements, for example, security, profit from venture and low mining cost can figure out which of the new and rising advanced coins can supplant Bitcoin in the near future. Future work on utilizing the verification of work has been examined. One of them is to boost the result of the confirmation of work by reusing it. Reusing this result as in the asset in settling any numerical riddle by a generally granted client can reuse it by remunerating other clients from the figured out tackled issue. Another idea is to utilize the energy created by the mining system from electrical energy to warm energy. This can be acknowledged in cool environment nations, where the impressively high intensity energy set free from the calculation of addressing the numerical riddle can be utilized to warm private houses and other family tasks requiring heat energy. has observed that Bitcoin can support

the monetary financial exchange and the US dollars. It was placed that like gold that doesn't rely upon the focal power, Bitcoin can lessen any gamble on the lookout. For the time being, Bitcoin's dynamic exchanging recurrence among clients empowers it by showing the supporting capacities. This shows that Bitcoin has an unmistakable and potential in the portfolio examination of the world securities exchange, as well as its generally safe administration. further recommends that Bitcoin and gold are proficient instruments in decreasing the gamble in speculation. Although this assertion is still somewhat untimely in esteeming Bitcoin as a similar standard as gold, the potential is there and opens the conduit to the opportunities for future exploration. It is understood that having significant information in the blockchain innovation would be fundamental in controlling the adverse consequence of involving digital money in everyday exercises. Consequently, skill in this field ought to team up with strategy creators and the public authority offices in making guidelines and arrangements relating to a nation's substitute utilizing cryptographic money. Information the board among industry players and specialists ought to be upgraded to cause individuals to grasp the potential and hazard in utilizing digital currency. Indeed, even specialists from the foundation of higher learning ought to be locked in with the general population as they have the information asset of working with the local area in having better information on specific issues.

4. Conclusion

Digital currencies are setting down deep roots. The eventual fate of exchanging lies well with new arising advances that can help humankind. Obviously, clients and industry players can assess whether digital currency can benefit or mislead them, as per their goals and viewpoints in claiming it. This paper has surveyed the amazing open doors in cryptographic money in terms of the security of its innovation, low exchange cost and high venture return. For the difficulties, the conversation spun around regulation and guideline, high energy utilization, plausibility of crash and air pocket, and goes after on network. The improvement and future work on cryptographic money incorporate further developing the security convention, chipping away at verification of movement, utilizing the result of evidence of work and applying the information to the executives framework. Taking a gander at the uplifting perspective of blockchain innovation and the possibility of government in managing digital money, more top to bottom examinations on a few parts of digital money ought to be finished. Accepting the open doors from part of the pie in the cryptographic money and blockchain innovation can be gainful for specialists. From that point, application in involving cryptographic money in the best of its capacity would be quite possibly of the most conspicuous disclosure in the 21st hundred years

References