PalArch's Journal of Archaeology of Egypt / Egyptology

# BLOCKCHAIN: VISUALIZATION OF THE BITCOIN FORMULA

*Fitra Putri Oganda[1], Untung Rahardja[2], Qurotul Aini[3], Marviola Hardini[4], Ankur Singh Bist[5]*

University of Raharja[1,2,3,4], Graphic Era Hill University Bhimtal Campus[5]

E-mail: fitra.putri@raharja.info[1], untung@raharja.info[2], aini@raharja.info[3], marviola@raharja.info[4], ankur1990bist@gmail.com[5]

**Fitra Putri Oganda, Untung Rahardja, Qurotul Aini, Marviola Hardini, Ankur Singh Bist: Blockchain: Visualization Of The Bitcoin Formula-- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(4), 1-14. ISSN 1567-214x**
**Keywords*:* - Bitcoin, SWOT, Blockchain, Cryptocurrency**

## ABSTRACT

Cryptocurrency employments scrambled systems as well as peer-to-peer systems to carefully encourage trade, an innovation created eight a long time prior. Bitcoin, the primary and most well known cryptocurrency and clearing the way as an innovation that disturbs the ancient and constant monetary installment framework that has existed for decades. Whereas cryptocurrency is improbable to supplant conventional fiat monetary standards, they can alter the way internet-connected worldwide markets are associated with each other, clearing boundaries around regulating national monetary standards and trade rates. Innovation progresses at tall speed, and opens the entryway to creating an open and fairly measured computerized economy from a centralized economy. Cryptocurrency can revolutionize computerized exchanging advertise by making a free flowing trading framework value. A SWOT analysis of Bitcoin is presented, which illuminates some of the latest events and movements that can influence whether Bitcoin contributes to the changing economic paradigm in both the financial and non-financial sectors. Then see the challenges ahead and business opportunities in this fundamental technology that are all ready to disrupt this digital world.

## INTRODUCTION

Blockchain may be a principal innovation in which cryptocurrency is the fundamental thing counting Bitcoin [1]. In 2008, an person (or gather) composing beneath the title Satoshi Nakamoto distributed a paper entitled "Bitcoin: The Peer-To-Peer Electronic Cash Framework". This inquire about outlines a peer-to-peer adaptation of electronic cash that has the possibility to create installments online and after that is sent specifically from one party to another without going through budgetary educate. Bitcoin is the primary realization of this concept. Presently "cryptocurrency" may be a name utilized to portray all systems and trades that utilize cryptography [2] to secure all exchanges [3] such as those frameworks where exchanges are channeled through trusted substances [4] centrally. A number of months afterward, an open source program that actualizes an unused convention was discharged, beginning with the Beginning 50 coins piece. Anybody can introduce this open source program and be a portion of the bitcoin peer-to-peer arrange. It has developed in notoriety since at that point with the fast development of data innovation [5] and computers empowering the improvement of computer-based frameworks that encourage the different forms of putting away [6], organizing, and handling different information [7]. The ubiquity of Bitcoin has never ceased expanding since at that point. In expansion, the fundamental Blockchain innovation is presently finding unused applications exterior of fund. As blockchain innovation is encountering quick advancement and investigation of its utilize extends, the joining of other innovations is considered troublesome such as enormous information, the Web of Things, brilliantly colleagues and independent vehicles [8] in making huge openings as well as having potential unintended results social.

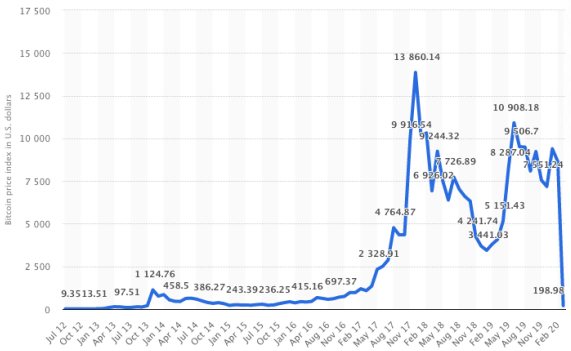


Figure 1. Bitcoin price index from July 2012 to March 2020 Source: Statista [9]

Since the creation of Bitcoin in 2009, the cost of this virtual cash has remained decently steady until January 2013, coming to a greatest esteem of around 20 US dollars. After that month to month cost development was watched until October 2013 when costs come to 198 US dollars. This about ten times increment within the esteem of Bitcoin demonstrated inconsequential compared to the cost rally in November 2013, when the US $ 1,100 limit was broken. After the downtrend period that taken after, the cost of Bitcoin come to 1,349.19 US dollars in April 2017. The number of Bitcoins in circulation has developed month by month and produced to more than 17 million in January 2019. The worldwide esteem of

Bitcoin produced to around 66 billion US dollars at the conclusion of 2018 and much higher than the esteem of other web monetary standards. As of September 2019, there were 5,457 Bitcoin ATMs around the world. In Admirable of that year, the nations with the most elevated number of Bitcoin ATMs were the United States, Canada, the United Kingdom, Austria and Spain. There are still numerous concerns around utilizing Bitcoin for online exchanges and the security of this virtual cash is seen as one of the foremost critical components affecting decisions about buying Bitcoin. The most advantage of a broadly decentralized blockchain is that it can offer assistance construct exchanges [10], coordination [11], and peer-to-peer disintermediary participation in conveyed frameworks without mutual trust and centralized control between each hub and after that based on strategies such as information encryption, timestamps, conveyed agreement calculations, and financial motivating force components. In this way, the blockchain can give a unused arrangement to the long-term issue of tall working costs, has moo effectiveness and security dangers [12] potential information capacity in conventional centralized frameworks. With the fast advancement and popularization of Bitcoin and other cryptocurrency within the final few a long time, the inquire about and application blockchain has moreover been seen to appear an expanding slant of exceptional blasts. Inside the broadly recognized blockchain is in a position to ended up the fifth troublesome advancement of the computing worldview after centralized servers, individual computers, the Web, and versatile or social systems [13]. Blockchain can be considered the another era of cloud computing, and is anticipated to drastically reshape person and organizational behavior models [14], and so realize the move from today's Web of Data to the Web of Future Values [15].

*Bitcoin is the Best Cryptocurrency*

It is imperative to consider Bitcoin all through the system's monetary space. Right presently the Bitcoin portion of the worldwide monetary framework is minutes since there are no budgetary specialists that got to worry about the affect of the Bitcoin money related showcase within the close future. But, as Bernanke said [16], it seems to have an expansive affect on the installment framework [17] within the long run. It is important to consider the Bitcoin framework from a broader perspective. Bitcoin is the foremost well known case that's inherently related to innovation blockchain. It was too the foremost disputable since it made a difference enact billions of dollars of worldwide markets from mysterious exchanges [18] without government control. Since it must bargain with a number of administrative issues including national governments and monetary educate. The foremost critical component of Bitcoin (BTC) is the modernity of the Blockchain, so from that record it isn't conceivable to alter from each BTC exchange that has ever taken put. Since BTC is an open source GitHub extend, each engineer can fork code [19] and make cryptocurrency executions. Diverse perspectives of Bitcoin drop at diverse focuses on the range of centralization or decentralization. Peer-to-peer systems are near to absolutely decentralized since anybody can run the Bitcoin hub and there are decently low obstructions to passage.

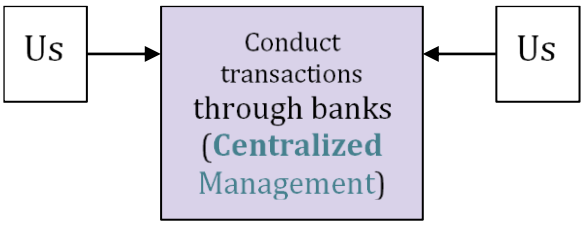


Figure 2. The Model In Payment Uses Traditionally

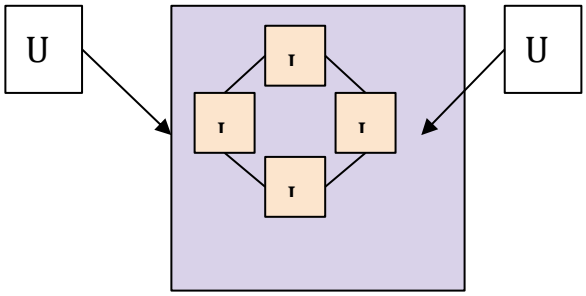


Figure 3. Models In Payment Using Cryptocurrency

In this area, this think about depicts an outline of exchange strategies for conventional cash with a comparison to advanced cash (computerized cash exchange strategies). Figure 2 appears the conventional cash exchange strategy. The method begins when client A exchanges cash to client B. This exchange will go through a framework given by the budgetary supplier which is the managing an account segment. This exchange employments a centralized administration framework [20] controlled by banking institutions. The security of these exchanges is checked and approved by banking institutions. For the most part, a central bank includes a imposing business model right to issue coins and notes (banknotes) for its dissemination range (a nation or a gather of nations); it directs the generation of cash by banks (credit) through financial approach. In this exchange, the esteem of the money is decided utilizing the trade rate. The trade rate is the cost at which two monetary forms can be traded with one another [21]. This can be utilized for exchanging between two money zones. Trade rates can be classified as drifting or settled.

The primary thing, every day trade rate developments are determined by the advertise; Within the last mentioned, governments mediate within the advertise to purchase or offer their monetary standards to adjust supply and request at a settled trade rate. In cases where a nation has control over its cash, control is worked out either by the central bank or by the Service of Back. Institutions that have control over financial arrangement are alluded to as money related authorities. Monetary specialists [22] have changing degrees of independence from the government that creates it. Figure 3 appears to be the crypto money exchange method. In the event that client A needs to exchange advanced cash to client B, the exchange must go through the blockchain way. Blockchain within the general record framework that's monitored and approved by clients involved within the common record approval framework employing a computer

framework. Cryptocurrency makes it less demanding to exchange stores between two parties in an exchange, this exchange is encouraged utilizing open and private keys for security purposes. This support exchange is carried out with negligible preparation expenses, permitting clients to avoid the soak expenses charged by most banks and monetary educate for wire exchanges. There's no physical bitcoin; as it were equalizations are kept for common records within the cloud. All Bitcoin exchanges are confirmed by an expansive sum of computing control.

## RELATED WORK

A think about certainly requires investigate strategies in arrange to more effectively get precise data. In this ponder utilizing the inquire about strategy of writing ponder strategy. Writing Think about Strategy could be a valuable strategy for getting researchers' references in getting precise data from past thoughts about and this research method is valuable for storing data that's relevant to the subject or issue that's significant to the subject you need to ponder. There are a few writing ponders that have been carried out in past ponders on Blockchain and Bitcoin and other existing but related thinks about, including:

A logical investigate think about in 2018 conducted by Heribertus Yulianton, Rina Candra Noor Santi, Kristophorus Hadiono and Sri Mulyani afterward on the inquire about conducted was to talk about applying the innovative advancement of the Blockchain, in spite of the fact that there are still numerous things that must be settled, particularly in terms of legitimateness, the innovation utilized can be learned and connected to other things. The innovation that works behind the scenes of crypto monetary forms such as bitcoin and the like is blockchain. In expansion, the blockchain can moreover be utilized on stages to back financial sharing. Inquire about from giving a few modern things that emerge from the execution of the blockchain, one of which is how to get it how the foundation, upkeep, and repair of believe when the setting of the client and supplier is changing [23]. Inquire about conducted by Muhammad Reza Rizky Fauzi in 2017 by talking about each exchange could be a open section on the bitcoin blockchain. As well as being a bookkeeping expansive worldwide exchange investigation on the utilize of exchanges on the Bitcoin blockchain at that point analyzes how the bitcoin blockchain performs the workings of exchanges on its framework. Exchanges are information structures that encode the exchange of values between clients within the bitcoin framework [24].

The ponder was conducted in 2017 by Daniel Augot, Herv´e Chabanne, Thomas Chenevier, William George, and Laurent Lambert where this ponder examines the introduction of plans on personality administration that will be built into the Bitcoin-blockchain, which permits an permanent character just like the blockchain. In expansion, the preferences of Bitcoin which have a decentralized nature to encourage shared control between clients and personality suppliers, permit clients to straightforwardly oversee their claim characters by easily planning the personalities of diverse suppliers indeed as personality suppliers can repudiate personality and uphold control [25].

Scientific research research conducted by Miftah Fajar Asy'ari, Avon Budiyono, Adityas Widjajarto in 2019 discussed the performance test on the processor to be able to run the private ethereum blockchain for coin transfer between ethereum blockchain nodes peer-to-peer as a messaging representation with various parameters. The results obtained are that there are effects of parameters that are changed on processor performance. Especially for nodes that have low specifications, performance up to 100% in some scenarios, in contrast to node specifications that are quite high in performance up to 80% [26]. Investigate conducted by Eric Budish within the year of investigate 2018 that examines the sum of computing control committed to mysterious, decentralized blockchains such as Bitcoin must at the same time fulfill two conditions in adjust counting the conditions without benefit included in competitions looking for lease for prizes related with consequent piece increases to the chain as well as motivation compatibility conditions on framework defenselessness [27].

From a number of writing thinks about, it can be concluded that there has been a part of investigate that has been done on Blockchain, particularly on Bitcoin, particularly in terms of its utilization. Where in this consider the center on the Bitcoin framework can be utilized for other contract-based understandings, and works in such a way that there's no single substance that controls exchanges since everybody controls each exchange.

## RESULT AND DISCUSSION

The selection of Cryptocurrency will be an vital subject of consideration within the future, since it can be a truly transformative innovation that's changing the way cash trades around the world. The expanded appropriation of Bitcoin is integrals related to changes within the worldwide advertisement. The worldwide advertisement fueled by the Web is right now exceptionally entrapped. On the off chance that a territorial showcase starts to plummet, it can effectively drag others into it. Bitcoin, just like the Euro, can unreservedly move over numerous national borders, making an environment that in this manner advances worldwide exchange, shared thriving, and indeed peace.

Table 1. SWOT Analysis on Cryptocurrency

| Strength | Weakness |
|---|---|
| Transactions are carried out in a decentralized manner by having a public key encrypted by the hash so secrecy is safe. | The existence of semi-anonymity so that when an act of crime occurs it will be difficult to trace. |
| Opportunity | Threads |

| | |
|---|---|
| Cryptocurrency eliminates the presence of a third person, which affects the industry in trading and international business because it has a fairly high transfer rate in a short amount of time. | There is a high degree of doubt that this will be a big challenge for cryptocurrency to attract public confidence in using cryptocurrency, especially bitcoin.. |

***Strength***

Bitcoin is exceptionally subordinate on two essential innovations of cryptography, the cryptographic open key to be able to carefully sign and the hash work for approving a exchange. The primary cryptographic primitive that we got to get it is the hash work of cryptographic hash capacities may be a numerical work with the taking after three properties:

1. The input can be any string of any estimate.
2. This produces a settled measure yield. For the purposes of dialog in this concrete chapter, we'll expect a 256-bit yield measure. In any case, our discourse applies to anything the size of the yield as long because it is huge sufficient.
3. Can be calculated proficiently. Naturally this implies that for a given input string, you'll hunt for what the yield of the hash work is in a sensible sum of time. More actually, checking n-bit string hashes must have a running time of O (n).

The primary property we require from a cryptographic hash work is that it is affect safe. Collision happens when two distinctive inputs create the same yield. A hash work H (.) Stands up to collisions in the event that no one can discover a collision. Formally:

The hash work H is said to be affect safe in the event that it isn't doable to discover two values, specifically x and y, such that $x \neq y$, but H (x) = H (y)

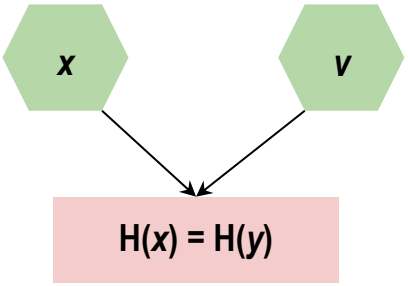


Figure 4. Illustration of Impact on Hash

A Bitcoin exchange could be a advanced signature that signs a exchange that contains 3 primary things: the payer's address, the recipient's address, and the sum (bitcoin) to be exchanged. In these exchanges dispersed to the Bitcoin arrange, for illustration a hub comprising of the center of all users of the program on Bitcoin and after that finally combined once more with other exchanges to be included in one piece. The foremost later square will be joined to the blockchain

through a mining prepare where computer control is utilized to be able to illuminate numerical puzzles, Proof of work (PoW) segments. The square can too store data and other enlightening and this can be where the resource component enters. Basically put, consider the signature with the image μi (with i ∈ N) at that point relate each modifier as a substitute, and state it with μi (T) the result of its application in exchange Q.

$$aai(Q) = Q\{wit(1) \rightarrowtail i\}\{wit(f= 1) \rightarrow\!\!\rangle \perp\}$$
$$ani(Q)= aai(Q\{out \rightarrow\!\!\rangle \perp\})$$
$$asi(Q) = aai(Q\{out(< i) \rightarrowtail (false, 0)\}\{out(> i) \rightarrow\!\!\rangle \perp\})$$
$$sai(Q) = aa1(Q\{in(1) \rightarrowtail Q.in(i)\}\{in(f= 1) \rightarrow\!\!\rangle \perp\}$$
$$\{relLock(1) \rightarrowtail Q.relLock(i)\}\{relLock(f= 1) \rightarrow\!\!\rangle \perp\})$$
$$sni(Q) = sai(ani(Q))$$
$$ssi(Q) = sai(asi(Q))$$

Each modifier is spoken to by a combine of images each speaking to the set of marked (gotten) and yield (exchange) (a = all, s = single, n = none), and index i ∈ N. The index this time has meaning which is distinctive depending on the modifier. With respect to the primary image of the modifier, if it may be, at that point the witness list where the signature will be entered, so as to ensure that the signature is tallied since it was included within the witnesses in file i cannot be utilized in witnesses with file j = i. In case the primary image of the modifier is s, as it were the i can input is marked, whereas all other inputs are erased from the exchange.

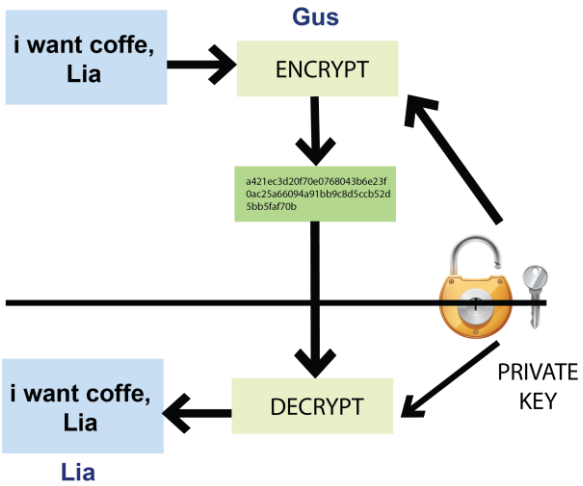


Figure 5. Cryptography of coffee ordering by Lia-Gus

Gus arranged to send a P message containing the words "i want coffee, Lia". The message is at that point scrambled by means of the symmetric cryptographic strategy E with a secret key K. Presently in the event that Lia takes off without unveiling the esteem, at that point Gus can claim the bond at time t. This does not constrain Lia to precise her commitment but she will lose all ties she has put on. So the ensure that he will uncover his mystery esteem depends on the sum of cash he is willing to put into bonds.

```
scriptPubKey:
  OP_IF
    <LiaPubKey> OP_CHECKSIGVERIFY <GusPubKey> OP_CHECKSIG
  OP_ELSE
    <LiaPubKey> OP_CHECKSIGVERIFY OP_HASH <H(x)> OP_EQUAL
  OP_ENDIF
scriptSig for Case 1:
          <GusSignature>  <LiaSignature> 0
scriptSig for Case 2:
          X  <LiaSignature> 1
```

The result could be an irregular message A which is at that point sent by Gus to Lia. At that point Lia who gotten the arbitrary message decrypted utilizing the symmetrical F strategy with the mystery key K. With the encryption method E and decryption F in conjunction with the mystery key K, the irregular message sent from Gus to Lia, indeed in spite of the fact that known by other parties, but the party others were incapable to studied the initial message sent by Gus to Lia. In this way secrecy (privacy) messages from Gus to Lia will be kept up. This strategy is exceptionally valuable particularly since the Web is an uncertain communication medium, since anybody can peer, and tap information bundles sent over the Web arrange. Symmetric cryptography has a few preferences, counting tall execution, where negligible calculations are required within the encryption and unscrambling handle. Lia spent BTC with Gus using the BTC wallet on the smartphone. Lia went through BTC with Gus utilizing the BTC wallet on the smartphone. Lia does this by checking a two-dimensional standardized identification commonly alluded to as a QR code at that point from installment demands gotten from the Gus BTC point-of-sale (POS) framework that contains Gus's goal address, as well as how much Lia must pay and a composed exchange portrayal. So to demonstrate this point in Figure 3, below to be able to imagine.

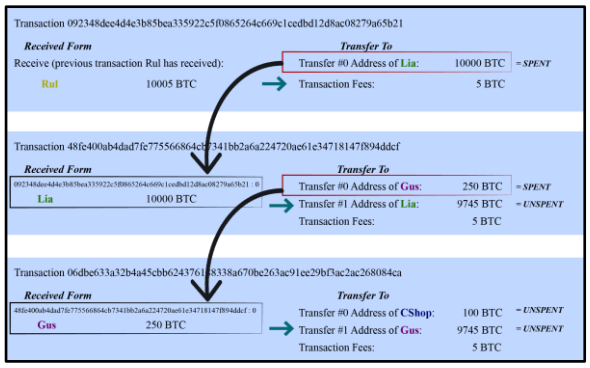


Figure 6. Transaction Model of Bitcoin

Authorization for BTC exchanges employments public key cryptography where client A will get both private and public keys. This affirms that as it were client A can make exchanges on client A; utilize the public key to decide the personality of client A and client A employments the private key to guarantee that certain exchanges have a place to them. In Figure 4, Lia pays Gus for the

coffee arrange by making a modern exchange from the past exchange input with Rul, which employments Lia's open key as the goal address for the BTC included. When Lia utilized portion of the stores to pay Gus on his coffee arrange, Lia given her individual key to open it. This guarantees that the exchanges are read-only for each other client on the BTC organize since it is for all intents and purposes outlandish for anybody to adjust them without knowing Lia's private key. After the organize is associated, Lia has sufficient BTC to be able to cover the exchange required for exchanges with Gus, at that point BTC is required to be exchanged utilizing Gus's public key. This states that to spend the sum exchanged, Gus must create his individual key. In other words it speaks to a secure exchange of values between Lia and Gus. The security of this exchange is carried out by the timestamping and hashing capacities of the validator on the BTC arrange, which is able shape the ultimate exchange chain. This guarantees that Lia with her individual key moreover cannot alter the exchange that has been affirmed by her, since it is in fact not attainable, so Lia must alter all squares within the chain to alter one block.

### *Weakness*

Bitcoin has a few inner shortcomings that are portion of its plan and cannot be effectively altered. The common record community, or chain square, implies that each client can see each exchange. There's semi-anonymity, in that the bitcoin wallet proprietor cannot be specifically identified, but it may be a bit tense for a few potential adopters. The open piece chain is shared with all clients, which suggests it is defenseless to assaults since of simple get to. Bitcoin contains a flawed notoriety through occasions that delineate negative pictures of digital monetary standards in common, not fair Bitcoin. But an internet commercial center that permits thousands of medicate merchants and about one million clients to form illicit sedate exchanges. Bitcoin is their fundamental exchange vehicle, due to need of government following and semi-anonymity. This movement ran from 2011 to 2013, and earned deals of nearly one billion USD. It is alluring for the online showcase to act against the equity it restricts, so that the semi-anonymity property of bitcoin appears negative for law-abiding citizens. Without positive promoting towards the esteem of semi-anonymity for ordinary clients, the common client base will think that cryptocurrency is as it were utilized by hoodlums.

### *Opportunities*

Cryptocurrency is in a one of a kind position as a pioneer in transformative innovation which will final the budgetary framework long. By its nature, it can fill holes in current monetary innovation and can offer assistance illuminate conventional keeping money issues by getting to be a peer-to-peer framework. Transformative innovation is begun by understanding particular issues in an industry.

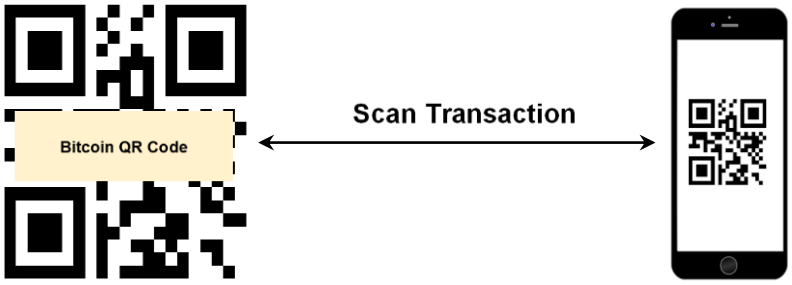


Figure 7. Transaction using QR Code Encryption

For illustration within the outlines in Figure 2 and Figure 3, cryptocurrency is prepared to assist cure issues related to customers who don't have a bank account. It has an ad-hoc bitcoin organize capability, two clients can exchange bitcoin with each other by filtering the QR code shown on their portable phone printed by the application. Typically a really special arrangement to a issue that has existed for a long time for a few individuals. This will continuously increment as the client base develops, so request for cryptocurrency systems and way better applications will develop at the cutting edge. There's a colossal showcase for potential designers to form these applications, as this innovation can influence any industry that depends on trusted third-party clearing frameworks. Bitcoin advancement into transformative innovation is driven by its capacity to unravel ancient issues, combined with a steady and developing community of engineers and clients. Businesses are beginning to see the esteem of using cryptocurrency for universal exchanges, particularly when exchanges ought to happen rapidly in reaction to crises. Cryptocurrency is as it were situated to fathom this issue much obliged to the speed and ease of exchanges in a peer-to-peer system. Cash can be exchanged universally, but ordinarily arrives days after being sent and not for the complete sum. Exchanges can be struck with a number of costs that cannot be clarified since they cross the line, making it troublesome to send the right sum to other businesses. A great illustration of this type of crisis need is a web company that's enduring from a refusal of benefit assault and needs prompt security from the company's arrange security. In this situation, exchange speed is most critical for every miniature the company's site is down and benefits are misplaced. Cryptocurrency contains a major advantage over conventional monetary forms much obliged to its dexterity in conducting quick peer-to-peer exchanges, particularly within the situation of universal businesses.

### *Threats*

Bitcoin has a few impediments to expel so that client acknowledgment is far reaching. The esteem of the variance is an episode of cryptocurrency putting questions on clients, as well as speculators. Within the conclusion the restricting figure in cryptocurrency is common acknowledgment. Vacillations in esteem decrease the certainty that customer esteem will be kept up on a day-to-day basis, restricting certainty within the esteem of the money as a entirety. The need of possession of the cryptocurrency center implies that any endeavor to cure this showcasing issue using advertising can hypothetically offer assistance to

speculation competition companies. This can be not an perfect circumstance for a showcasing arrange. Cryptocurrency has too seen extortion and burglary, for the most part due to inaccurate framework settings by the trade company. These hacks for the most part make the news, and can effortlessly persuade conventional individuals that they are an hazardous area to put their cash. There's too a big crevice within the law that incorporates the utilize of cryptocurrency. As long as cryptocurrency remains in an range that's not for the most part covered by law, client acknowledgment will be constrained. The client ought to accept that each exchange that employments cryptocurrency is legal and official. The advertise and the government are moderate to respond to unused innovation. Within the conclusion, all of these components restrain buyer certainty in bitcoin and cryptocurrency.

## CONCLUSION AND FUTURE WORK

In this paper, the objective is to be able to make, oversee and persuade Bitcoin administration policies that abuse blockchain innovation. The most advantage of this approach is that the approach can be realized within the world of blockchain, so that it can be caught on by all circles at that point that get to rights can be exchanged from one client to another as it were through blockchain exchanges. The approach has been approved through the execution of references based on Bitcoin. As a crucial innovation with transformative potential, blockchain and cryptocurrency have found a wide range of application plans in different sorts of businesses, extending from strategies that base information capacity, encryption, and confirmation to the mid-level budgetary and resource administration as well as different high-level trade models. In this paper, we present the technical details of Bitcoin and other formulas, how bitcoin can run and carry out transactions according to its users and discuss some of the potentials in the Bitcoin research scheme. So the great hope of this paper is to be able to stimulate more detailed investigations and innovative research in this new direction.

## ACKNOWLEDGMENT

We would like to thank all members of the UR Blockchain who have provided their support so that they can make a significant contribution and analysis in visualizing bitcoin as cryptocurrency.

## REFERENCE

“Mastering Bitcoin: Unlocking Digital Cryptocurrencies - Andreas M. Antonopoulos - Google Books.” [Online]. Available: https://books.google.co.id/books?hl=en&lr=&id=IXmrBQAAQBAJ&oi=fnd&pg=PR4&dq=Unlocking+Digital+Cryptocurrencies&ots=9BfUoyKpR-&sig=mdXezMFQvlcuR7zlsZSkRT0wyWQ&redir_esc=y#v=onepage&q=Unlocking Digital Cryptocurrencies&f=false. [Accessed: 24-Feb-2020].

O. Goldreich, Providing sound foundations for cryptography : on the work of Shafi Goldwasser and Silvio Micali. .

U. Rahardja, T. Hariguna, and W. M. Baihaqi, "Opinion mining on e-commerce data using sentiment analysis and k-medoid clustering," in Proceedings - 2019 12th International Conference on Ubi-Media Computing, Ubi-Media 2019, 2019, pp. 168–170.

P. Isenberg, C. Kinkeldey, and J.-D. Fekete, "Exploring Entity Behavior on the Bitcoin Blockchain," pp. 1–2, Oct. 2017.

Q. Aini, U. Rahardja, A. Moeins, D. M. Apriani, and D. M. Apriani, "Penerapan Gamifikasi pada Sistem Informasi Penilaian Ujian Mahasiswa Untuk Meningkatkan Kinerja Dosen," J. Inform. Upgris, vol. 4, no. 1, Jul. 2018.

I. Handayani, U. Rahardja, E. Febriyanto, H. Yulius, and Q. Aini, "Longer Time Frame Concept for Foreign Exchange Trading Indicator using Matrix Correlation Technique," in Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019, 2019.

S. Davidson, P. De Filippi, and J. Potts, "Economics of Blockchain," SSRN Electron. J., Mar. 2016.

A. Fajri and M. Yamin, "Digital Currency like Bitcoin within the International Monetary System Field," Verit. J. Ilm. Hub. Int. (International Relations Journal), vol. 10, no. 20, pp. 57–68, Mar. 2019.

"• Bitcoin price index monthly 2012-2020 | Statista." [Online]. Available: https://www.statista.com/statistics/326707/bitcoin-price-index/. [Accessed: 04-May-2020].

I. U. Rahardja and S. Raharja, "Artificial informatics," 2009 4th IEEE Conf. Ind. Electron. Appl. ICIEA 2009, pp. 3064–3067, 2009.

E. Portmann, "Rezension „Blockchain: Blueprint for a New Economy"," HMD Prax. der Wirtschaftsinformatik, vol. 55, no. 6, pp. 1362–1364, Dec. 2018.

Y. Yuan and F. Y. Wang, "Blockchain: The state of the art and future trends," Zidonghua Xuebao/Acta Autom. Sin., vol. 42, no. 4, pp. 481–494, Apr. 2016.

"Eris Industries." [Online]. Available: https://erisindustries.com/. [Accessed: 24-Feb-2020].

F. Agustin, F. P. Oganda, N. Lutfiani, and E. P. Harahap, "Manajemen Pembelajaran Daring Menggunakan Education Smart Courses," Technomedia J., vol. 5, no. 1, pp. 40–53, Apr. 2020.

Sudaryono, U. Rahardja, and N. Lutfiani, "The Strategy of Improving Project Management Using Indicator Measurement Factor Analysis (IMF) Method," in Journal of Physics: Conference Series, 2020, vol. 1477, no. 3.

"Ben Bernanke's letter to Congress: Bitcoin and other virtual currencies 'may hold long-term promise' — Quartz." [Online]. Available:

https://qz.com/148399/ben-bernanke-bitcoin-may-hold-long-term-promise/. [Accessed: 04-May-2020].

P. A. Sunarya, U. Rahardja, and D. I. Desrianti, "Development assessment module portfolio e-IMEi students with learning to improve the quality of concentration case study mavib," Int. J. Econ. Res., vol. 13, no. 8, pp. 3597–3606, 2016.

X. Yi and K. Y. Lam, "A new blind ECDSA scheme for bitcoin transaction anonymity," in AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 2019, pp. 613–620.

J. Jiang, D. Lo, J. He, X. Xia, P. S. Kochhar, and L. Zhang, "Why and how developers fork what from whom in GitHub," Empir. Softw. Eng., vol. 22, no. 1, pp. 547–578, Feb. 2017.

C. Lukita, M. Hatta, E. P. Harahap, and U. Rahardja, "Crowd funding management platform based on block chain technology using smart contracts," J. Adv. Res. Dyn. Control Syst., vol. 12, no. 2, pp. 1928–1933, 2020.

X. Li and C. A. Wang, "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," Decis. Support Syst., vol. 95, pp. 49–60, Mar. 2017.

U. W. Chohan, "Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions," SSRN Electron. J., Oct. 2017.

H. Yulianton, R. Candra, N. Santi, K. Hadiono, and S. Mulyani, IMPLEMENTASI SEDERHANA BLOCKCHAIN. 2018.

M. R. R. FAUZI, "IMPLEMENTASI DAN ANALISA PENGGUNAAN CARA KERJA TRANSAKSI PADA BLOCKCHAIN BITCOIN." Universitas Telkom, 2017.

D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lambert, "A user-centric system for verified identities on the bitcoin blockchain," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, vol. 10436 LNCS, pp. 390–407.

M. F. ASY`ARI, "ANALISA PARAMETER ETHEREUM PADA JARINGAN PEER TO PEER BLOCKCHAIN DI APLIKASI TRANSFER KOIN TERHADAP ASPEK PROCESSOR." Universitas Telkom, S1 Sistem Informasi, 2019.

E. Budish, "The Economic Limits of Bitcoin and the Blockchain Bitcoin and the Blockchain : A Critique in 3 Equations," NBER Work. Pap. No. 24717, 2018.