Regulation of Bitcoin Currencies: A Review Paper

Roma Khanna, Assistant Professor,

Teerthanker Mahaveer Institute of Management and Technology, Teerthanker Mahaveer University,

Moradabad, Uttar Pradesh, India

Email Id- romakhanna11@gmail.com

ABSTRACT: Prior to Bitcoin, there was no mechanism in existence that enabled any two interested individuals to execute transactions without the involvement of a third party. Third parties were introduced into the process to avoid fraud. As a consequence, engaging the help of a third party resulted in higher transaction costs, which is an issue with the existing online transaction system. Double-spending is an issue with digital currencies due to the ease with which digital tokens may be copied and the incapacity of transaction parties to verify the digital currency's authenticity. Bitcoin has a mechanism in place to prevent double-counting and guarantee the authenticity of each transaction. Bitcoin is a peer-to-peer electronic cash system based on encryption, blockchain, and peer-to-peer transactions. Because there are no restrictions for establishing an account or investing in Bitcoin, the Bitcoin network is quickly growing. It is basically a network available to everyone. The fact that Bitcoin was the first decentralized digital currency adds to its popularity. This currency establishes a brand-new platform for financial transactions.

KEYWORDS: Bitcoin, Cryptocurrency, Blockchain, Cryptography, Anonymity, Timestamp Server, Distributed Ledger.

1. INTRODUCTION

Bitcoin is an uncontrolled digital money that is based on an open source peer-to-peer virtual transaction system that is partly anonymous. We use the term "unregulated" to describe anything that is not controlled by a central authority. Satoshi Nakamoto, a pseudonymous individual, introduced the concept for this crypto currency in 2008. Bitcoin was created by a community of open source developers. It is essentially a private currency supplied by a private business with the express aim of counteracting the government's exclusive monopoly over money production and transmission. Bitcoins are more stable than conventional currencies, which are susceptible to a variety of variables such as recession, inflation, government policies/laws, and political corruption. The value of Bitcoin is not set by legislation. Supply and demand are exactly proportionate to their worth. Bitcoin was created as a response to the issue of double-spending that may occur when utilizing a digital currency system. A single digital token may be used many times, which is a possible vulnerability. A digital file that may be copied or faked makes up this digital token. Bitcoin transactions are final and cannot be reversed. There is a distributed peer-to-peer timestamp server that keeps track of transaction order in a chronological fashion. If Bob wants to transfer $100 to Alice via the Internet, he would have to use a third-party service such as Paytm. Account balances are kept on file by intermediary parties. Paytm deducts $100 from Bob's account and adds it to Alice's account in the aforementioned transaction. Without such middlemen, digital money might be spent twice. Consider the case when there are no ledger intermediates. In this scenario, digital money is nothing more than a computer file. A $100 transaction between Bob and Alice may be accomplished by adding a money file to a message. Sending an attachment to someone, like sending an email, does not erase it from the sender's computer. Bob would keep the duplicate of the money file after she had given it to Alice. Bob may then simply send the same $100 to anybody else she desires. This is known as the "double-spending" issue. Until Bitcoin, the only way to solve problem was to use a trusted third party to maintain track of the ledger. Bitcoin addresses this problem by disseminating the ledger across all system users through a peer-to-peer network.[1], [2]

1.1 What are bitcoins and how do they work?

A. Transactions: A Bitcoin transaction does not need the involvement of any financial institution or government body; rather, individuals complete all transaction stages independently. The transactions are encrypted using the SHA-256 hashing algorithm (Figure 1).

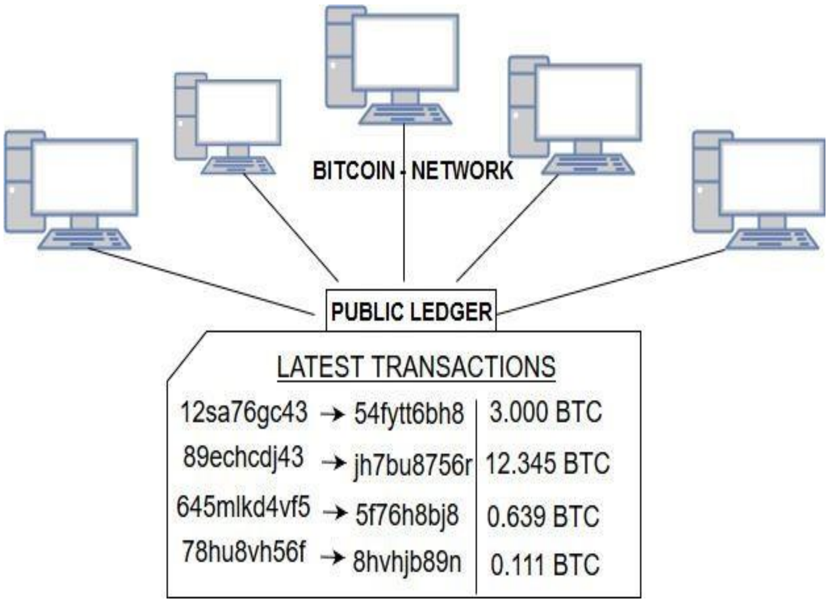

BITCOIN NETWORK
PUBLIC LEDGER
LATEST TRANSACTIONS
12sa76gc43 → 54fytt6bh8 3.000 BTC
89echcdj43 → jh7bu8756r 12.345 BTC
645mlkd4vf5 → 5f76h8bj8 0.639 BTC
78hu8vh56f → 8hvhjb89n 0.111 BTC

Figure 1: The Encrypted Transaction Is Then Recorded In The Decentralized Network's Public Ledger, Which Is Maintained By Thousands Of Computers.

Electronic coin is defined as a sequence of digital signatures. Digital signatures are basically digital tokens. Each individual transfers the coin to the next individual by digitally signing a hash of the previous transaction and the public key of the succeeding individual and adding these to the end of the coin. The recipient can verify the signatures to validate the chain of ownership by this process (Figure 2).

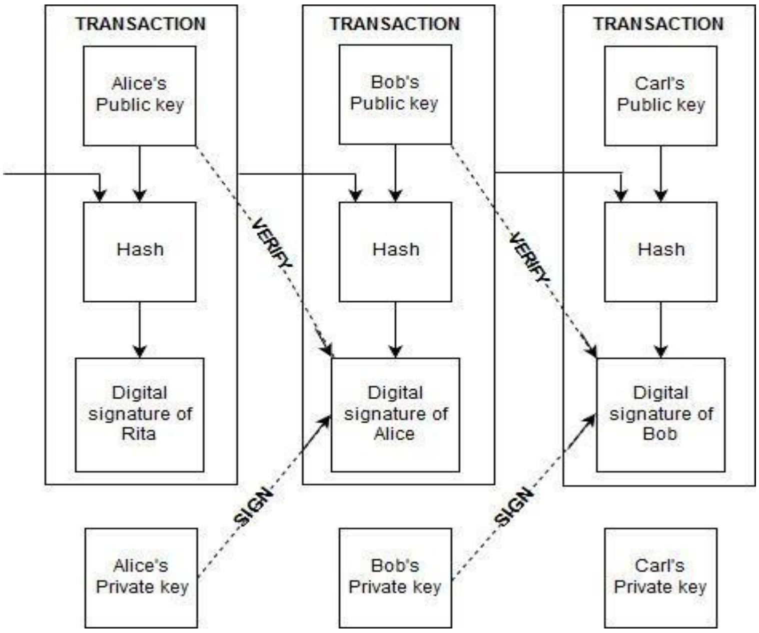


Figure 2: The Encrypted Transaction flow within Recorded in the Decentralized Network's Public Ledger, Which Is Maintained by Thousands of Computers and related private keys of the Dataset.

Because the first transaction is the one that counts, subsequent efforts to double-spend are ignored. The only way to tell whether we didn't miss any transactions is to keep track of everything that happens. Transactions are made public in a ledger, which is a method for parties to agree on the sequence in which transactions should be made. The receiver must show that the majority of nodes agree that the transaction was the first received at the moment of the transaction.[3], [4].

A. Concept of Cryptography

Bitcoin is based on a "cryptographic proof" method that enables a person to trade directly with another party without the requirement for a third party to approve the transaction. Certain cryptography principles must be understood in order to comprehend the Bitcoin notion. Cryptography is a phenomena that ensures the confidentiality and security of communications by ensuring their authenticity, integrity, and non-repudiation. The following goals are maintained by cryptography:[5], [6]

B. Authentication

A message's recipient should be able to verify the data's provenance. A method for authenticating the sender of data, such as utilizing a public key, should be in place.

C. Integrity

Data integrity refers to the sanctity of data. The recipient of a message should be able to verify that it was not tampered with during transmission; an intruder should not be able to substitute a genuine one with a fake one. Intentional and inadvertent tampering are both possible. Unintentional tampering occurs when message packets encounter random bit errors or noise while traveling from one node to the next.

D. Non-repudiation-

A sender should not be able to claim that an impostor sent the communication instead of him. It implies that the message sender is unable to dispute the message's validity.

E. Confidentiality

It refers to the process of restricting access to a piece of information to a group of people by encrypting the data and distributing the secret key with the group. Now we'll go through some of the reasons why cryptography is essential in Bitcoin: If two individuals wish to exchange private communications, they may use encryption to conceal their real message (plaintext) using an encryption method and encryption key. In turn, the encryption process converts the original communication to cipher text, rendering it indecipherable to an intruder or anybody else.

This encrypted communication will be unreadable and can only be seen if you have the decryption key to convert it back to the original message. Decryption is the opposite of encryption, in which the encrypted text is unscrambled and returned to its original form. Nowadays, just the encryption/decryption keys are kept secret, whereas the encryption and decryption methods are known or may be known in most situations. In today's world, there are two types of encryption algorithms: symmetric and asymmetric encryption algorithms. Both parties use the same key for encryption and decryption in a symmetric encryption method, whereas both parties use separate keys in an asymmetric encryption technique. Symmetric-key encryption is effective for encrypting data on your computer/server, but it is inefficient for transmission since the same key is used for both encryption and decryption. The disadvantage of this method is that people who want to communicate with each other need to agree on a key, which should ideally be done face to face since you already know why you're encrypting your conversations in the first place: you believe your communication route is unsafe. You can't simply transmit an encryption key in an email, text message, or phone conversation since it may be intercepted by anybody, either deliberately or accidentally. Overall, securely sharing the shared key between two individuals may be challenging. Their real owners are transferring them. Digital signature and verification are handled differently by ECDSAThe signature algorithm uses the private key, whereas the verification process uses the public key. The private key is an unpredictably or randomly generated integer between 1 and the order. The public key is generated by multiplying the base point by the private key's value, which is expressed as follows in the form of an equation:

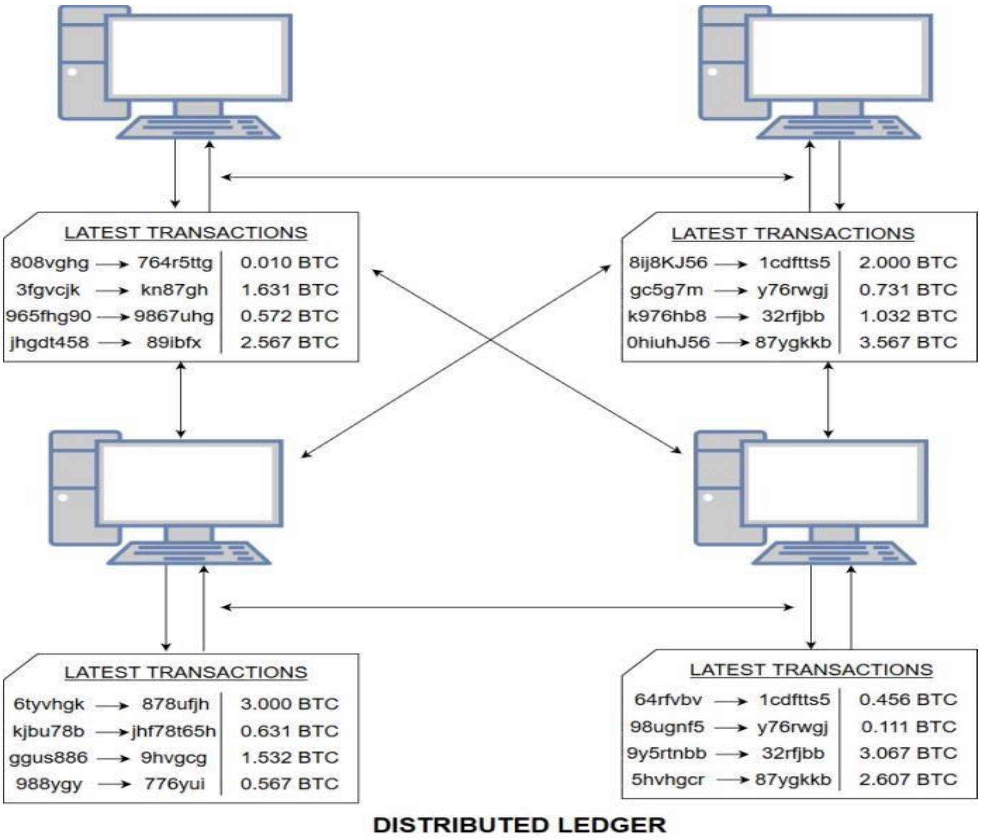
$$\boxed{\text{Public key} = \text{Private key} * \text{Base point}}$$

This indicates the maximum number of private keys that may be generated, which is equal to the order. ECDSA digitally signs transaction data using an elliptic curve and a finite field in such a manner that third parties may verify the signature's validity while the signer maintains full control over the signature's creation.[7], [8]

Public-key cryptography: this kind of cryptography combines encryption, decryption, and digital signatures. To encrypt and decode communications, this cryptographic method requires the establishment of a key pair consisting of two distinct keys: the public key and the private key. When it comes to communication and transactions, public key cryptography is regarded much superior than symmetric key encryption. Each Bitcoin transaction employs public-key encryption to protect the anonymity of all parties involved. Two mathematically related keys are generated as a result of this encryption procedure. The payee keeps one key, similar to a private key such as a password or pin. A private key is a single unsigned 256 bit integer (32 bytes) that is created at random and used to access the Bitcoins held in the payer's account. The other key is made public, such as the name of a bank or an account location where the money are held, and is referred to as the payee's public key. The public key is used by the payee to find the payer's account. The other individual can only access the payer's account and take money if he has access to the related private key. The payer then authorizes and enables the withdrawal of Bitcoins from their account using their own private key. All transactions using a public key are then broadcast to the whole Bitcoin community and recorded in a public ledger that is open to the world. Because of the complexity of public key encryption, counterfeiting a Bitcoin transaction would need more processing power and more computationally difficult than the whole Bitcoin network. As a result, public encryption effectively guarantees the security of Bitcoin transactions.

2. DISCUSSION

Distributed ledgers offer a continuously updated, shareable, and transparent record of every transaction that occurs in their order. A distributed ledger is also used to track the transfer of Bitcoin ownership. This effect simplifies the intrinsically complicated commercial operations. The use of mutual distributed ledgers will play a major role in lowering office expenses and reducing market risks. Rather of entrusting the ledger to a single authority, the ledger is maintained by a community of peers who share responsibility for its upkeep. Establishing agreement among peers who share ledger maintenance ensures the ledger's identity and integrity (Figure 3).



LATEST TRANSACTIONS

808vghg → 764r5ttg	0.010 BTC
3fgvcjk → kn87gh	1.631 BTC
965fhg90 → 9867uhg	0.572 BTC
jhgdt458 → 89ibfx	2.567 BTC

LATEST TRANSACTIONS

8ij8KJ56 → 1cdftts5	2.000 BTC
gc5g7m → y76rwgj	0.731 BTC
k976hb8 → 32rfjbb	1.032 BTC
0hiuhJ56 → 87ygkkb	3.567 BTC

LATEST TRANSACTIONS

6tyvhgk → 878ufjh	3.000 BTC
kjbu78b → jhf78t65h	0.631 BTC
ggus886 → 9hvgcg	1.532 BTC
988ygy → 776yui	0.567 BTC

LATEST TRANSACTIONS

64rfvbv → 1cdftts5	0.456 BTC
98ugnf5 → y76rwgj	0.111 BTC
9y5rtnbb → 32rfjbb	3.067 BTC
5hvhgcr → 87ygkkb	2.607 BTC

Figure 3: Distributed Ledger of the System Prescribed in the Hierarchical Manner of Data Flow in Database.

The value of Bitcoins is determined in large part by ledgers. Because Bitcoin users have confidence in the ledger underpinning Bitcoin to keep an accurate record of activities and ownership, the decentralized digital currency has been able to flourish all over the globe. Because all ledgers are equal, anybody may get a copy of the ledger for inspection, although verifying the ledger's integrity is more common. There are a number of factors that contribute to consumers' confidence in Bitcoin. For starters, since Bitcoin is a true measure of value, we can simply convert it to other currencies or the value inherent in products and services. Second, the demand for Bitcoins is not going away anytime soon, making it an important aspect to consider when utilizing them as a method of exchanging value. Finally, the currency's value stays constant, allowing us to utilize it as a store of wealth.[9], [10]

3. CONCLUSION

We now have a remedy to the faults in the current digital transaction system, thanks to the invention of Bitcoin technology. Cryptography improves security by validating transactions with the same cutting-edge encryption technology used in military and defense applications to preserve anonymity. Blockchain allows P2P (peer to peer) value transactions without the need for a middleman and also aids in the maintenance of a public ledger to record all transactions taking place across the globe, removing the need for any intermediary. It also includes a transparent public ledger that records all transactions once they have been verified, as well as the order in which they occur. Bitcoin's usage as a means of trade has been restricted in recent years, with the exception of criminal activity. An rise of Bitcoin investors has been linked to an increase in Bitcoin exchange volume in the past. It's been utilized to do business outside of conventional, regulated channels and, presumably, as a speculative investment possibility. People invest in Bitcoin because they think it will one day become a full-fledged global currency. Bitcoin is generally acknowledged across the globe and is unaffected by government interference. It is conceivable that the future repercussions will be a spectacular conceptual and technological accomplishment, which might be utilized by governments or existing financial institutions to issue their own Bitcoins.

REFERENCES:

[1] K. V. Tu and M. W. Meredith, “Rethinking virtual currency regulation in the bitcoin age,” *Washingt. Law Rev.*, 2015.

[2] A. Seetharaman, A. S. Saravanan, N. Patwa, and J. Mehta, “Impact of Bitcoin as a World Currency,” *Account. Financ. Res.*, 2017.

[3] A. Gump and C. Leonard, “Blockchain: regulating the future of finance,” *Int. Financ. Law Rev.*, 2016.

[4] M. Ponsford, “A Comparative Analysis of Bitcoin and Other Decentralized Virtual Currencies: Legal Regulation in the People’s Republic of China, Canada, and the United States,” *SSRN Electron. J.*, 2015.

[5] L. J. Trautman, “Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace,” *SSRN Electron. J.*, 2018.

[6] Y. Kurihara and A. Fukushima, “How Does Price of Bitcoin Volatility Change?,” *Int. Res. Econ. Financ.*, 2018.

[7] N. M. Kaplanov, “Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation,” *SSRN Electron. J.*, 2012.

[8] S. Kethineni and Y. Cao, “The Rise in Popularity of Cryptocurrency and Associated Criminal Activity,” *Int. Crim. Justice Rev.*, 2020.

[9] R. Bollen, “The Legal Status of Online Currencies Are Bitcoins the Future?,” *SSRN Electron. J.*, 2016.

[10] S. Robberson and M. McCoy, “A Bit Like Cash: Understanding Cash-For-Bitcoin Transactions Through Individual Vendors,” *J. Digit. Forensics, Secur. Law*, 2018.