CRYPTOCURRENCY AS PAYMENT MOD

Ganga D Benal[1], Mayank Sharma [2], Shubham kumar [3] , Vipul Mehta [4], Sohan Chatterjee [5]

[1,2]Assistant Professor Department of Computer Science and Engineering, Cambridge Institute of Technology, Bangalore, India

[2,3,4,5]Students Department of Computer Science and Engineering, Cambridge Institute of Technology, Bangalore, India

***Abstract*—.** Since they function independently of established financial systems, cryptocurrencies have attracted a lot of attention in recent years. One of the most prominent use cases of cryptocurrencies is their role as a payment method. This paper provides a technical perspective on how cryptocurrencies are used as a payment method, including their underlying technology, advantages, challenges, and future prospects..

1. INTRODUCTION

Cryptocurrencies, including Bitcoin, Ethereum, and Ripple, are digital currencies that are decentralized in nature, i.e., they are not governed or controlled by a centralised body like a government or financial institution. Instead, they run on a distributed network of computers called a blockchain that consists of many nodes or computers.

One of the key features of cryptocurrencies is their use of cryptographic techniques to secure transactions and ensure the integrity of the network. When a user initiates a transaction using a cryptocurrency, the transaction details are encrypted using complex mathematical algorithms. These algorithms are virtually impossible to reverse engineer or tamper with, ensuring that the transaction remains secure and cannot be altered once it is recorded on the blockchain.

Another significant difference between cryptocurrencies and traditional payment methods, such as cash, credit cards, or bank transfers, is the absence of intermediaries. In traditional payment methods, transactions typically involve multiple intermediaries, such as banks, payment processors, and clearinghouses, which can result in delays, additional fees, and potential risks of fraud or data breaches. In contrast, cryptocurrencies operate on a peer-to-peer network, allowing users to directly transact with one another without the need for intermediaries. As a result, there is no need for third-party verification, which lowers transaction costs and speeds up transactions.

The decentralized nature of cryptocurrencies also results in increased transparency. Transactions on the blockchain are recorded in a public ledger, which is accessible to all network participants. This transparency provides a high level of accountability and reduces the risk of corruption or fraud, as transactions can be easily audited and traced back to their source.

Furthermore, cryptocurrencies offer the potential for faster, cheaper, and more efficient transactions. Traditional cross-border transactions can take days or even weeks to process, involve multiple intermediaries, and incur high fees. In contrast, cryptocurrency transactions can be processed within minutes or even seconds, with lower transaction fees, making them an attractive option for international transactions.

Overall, cryptocurrencies offer several advantages as a payment method, including security, transparency, speed, and cost-effectiveness. However, it's important to note that cryptocurrencies also face challenges, such as volatility, scalability, regulatory frameworks, and user experience, which need to be addressed for widespread adoption as a mainstream payment method. Nevertheless, cryptocurrencies have the potential to disrupt the traditional payments industry and reshape the way we transact in the future.

.LITERATURE SURVEY

"IEEE Standard for General Process of Cryptocurrency Payment" The general method of bitcoin payment between customers and businesses is defined in the IEEE Standard for General Process of bitcoin Payment. This procedure explains how a customer uses cryptocurrency to pay for goods or services and how the vendor gets compensated with fiat money. It involves a variety of factors, including cryptocurrency payment operators acting as agents, cryptocurrency ownership by users, merchant access to a platform for accepting cryptocurrency payments, banks, and cryptocurrency exchanges.[1]

"IEEE Standard for General Requirements for Cryptocurrency Exchanges " This standard covers the self-control and business ethics of bitcoin exchange platforms, as well as the relationship between them and to cryptocurrency wallets. This standard also covers user authentication programmes, operational methods, and exchange business logic. This standard also covers a small but crucial group of technical criteria, such as terminology, a fundamental architectural framework, key indicators, and end-user interface specifications, in order to accomplish the aforementioned objectives..[2]

"Daojing He, Shihao Li, Cong Li, Sencun Zhu, Sammy Chan, Weidong Min, and Nadra Guizani" Security incidents involving digital currency wallets are rising along with their popularity. They result in the exposure of users' personal data and security risks to users' possessions. The most widely used mobile operating system, Android, is examined in this article along with the security threats associated with digital wallets. The threat model and security objectives are first established, after which the attack surface and attack vectors from the perspective of wallet apps and the Android operating system are analysed. Two real-world digital currency wallet apps are used in experiments, and the findings demonstrate the necessity and significance of designing safe cryptocurrency wallets by exposing various significant security issues in these apps.[3]

The term "blockchain" refers to a growing collection of data known as blocks that are connected through encryption. A cryptocurrency wallet stores blockchain private and public keys but not the actual value of the currencies. Customers can use wallets to engage with blockchains to send and receive virtual currency and tokens as well as adjust their balance. The three subcategories of various currencies wallets are software, hardware, and paper. There are desktop, mobile, and web software wallets. One must have a thorough understanding of wallets given the growing use

of blockchain in numerous businesses. There are numerous wallet types to choose from. This article examines the features of multi-currency wallets, including supported fiat currencies, anonymity, cost, platform support, key management, and wallet recovery techniques.[4]

"Yi Liu, Ruilin Li, Xingtong Liu , Jian Wang , Lei Zhang , Chaojing Tang and Hongyan Kang," With the widespread use of Bitcoin, a lot of malicious software aiming to steal bitcoins through the network has surfaced. Bitcoin heavily relies on the elliptic curve digital signature method to ensure the security of transactions. Each user can have a large number of addresses that have been hashed using his public keys to receive money. To authorise spending those coins, the user needs the private keys linked to these addresses. A Bitcoin wallet can help its user maintain and protect all of their private keys. Complete private key storage on local storage, however, presents a significant issue in the event of theft. We provide a practical way to improve Bitcoin wallet security in order to protect users' private keys remember to produce private keys as necessary. Instead of storing whole private keys on local storage, only a list of random seeds is required. Without the passphrase, no one could generate all of the private keys by using random seeds. [5]

"Yi Liu, Xingtong Liu, Lei Zhang, Chaojing Tang and Hongyan Kang" Bitcoin is a decentralized cryptocurrency that has recently gained popularity on a global scale. To keep track of all transactions in the Bitcoin system, Blockchain functions as a public ledger. An exchange of bitcoins involves a number of inputs and outputs, each having a distinct hash value. The owners of the transferred bitcoins, however, are only able to sign the transaction to verify the content's integrity but not the script's output. The capacity of an attacker to intercept, change, and rebroadcast a transaction into the Bitcoin network is known as transaction malleability in the Bitcoin system. Through this approach, the transaction issuer is persuaded to believe that the first transaction was unsuccessful in being added to the blockchain.. Attackers took advantage of the flaw, which resulted in the bankruptcy of the biggest Bitcoin exchange in existence at the time. In this work, we describe a method to safeguard the user wallet in order to prevent this scenario from occurring again. Our system verifies a transaction's success by using both the address balance it spends and the transaction's distinct hash value. [6]

"Arunmozhi Manimuthu, Raja Sreedharan V , Rejikumar G and Drishti Marwaha", Bitcoin is an open-source cryptocurrency-based technology that functions as a private payment system on a peer-to-peer grid. In a peer-to-peer network, Bitcoin relies on complex cryptography that is supported by the local community. This study examines academic works to determine how bitcoin is discussed there. A thorough research of the literature is used to report on the characteristics of bitcoin in the study. The paper is supported by primary data from published works and secondary data from publicly available case studies that are pertinent to the topic.Bitcoin first appeared to represent optimism for a brighter future, but it is difficult to forecast how bitcoin will develop. Both practitioners and academics have access to a completely new universe thanks to bitcoin. The report also discusses the "potential" of bitcoin and highlights the requirements, requirements, implications, and difficulties that bitcoin encounters when processing commercial transactions. [7]

"Fangdong Zhu, Wen Chen, Yunpeng Wang, Ping Lin , Tao Li, Xiaochun Cao and Long Yuan", Centrally located in a storage space is the private key. However, consumers run the risk of losing their Bitcoins if the storage facility is destroyed or compromised. This inspired us to provide HA-eWallet, a novel online wallet architecture, in this paper. Instead of using just one private key to sign a Bitcoin transaction, HA-eWallet uses numerous private keys, and the private keys are kept in distinct locations.In order to build the Active-Active architecture and cycle the capability and workload, we also establish a second service unit. Additionally, we incorporate a disaster recovery method into our suggested architecture in the event of a catastrophe.[8]

II. UNDERLYING TECHNOLOGY

Cryptocurrencies utilize various technical components to function as a payment method. The most fundamental component is the blockchain, It is a distributed ledger that immutably and chronologically records all transactions. Transactions on the blockchain are secured using cryptographic techniques, such as public-key cryptography, which assures that the cash can only be accessed by the intended recipient.
In addition to the blockchain, cryptocurrencies also use consensus algorithms to validate transactions and maintain the integrity of the network. For example, Bitcoin uses Proof of Work (PoW), where transactions are validated and added to the blockchain by miners who solve challenging mathematical puzzles. On the other side, Ethereum, is transitioning from PoW to Proof of Stake (PoS), where validators stake cryptocurrency as collateral to validate transactions.

III. METHODOLOGY

To explore the topic of cryptocurrencies as a payment method, a comprehensive literature review and analysis of existing research, articles, reports, and publications were conducted. The methodology used in this technical paper is as follows:

1. Literature Review: A thorough review of academic and industry literature was conducted to gather relevant information on cryptocurrencies as a payment method. Various databases, such as Google Scholar, IEEE Xplore, and research articles from reputable journals and conferences, were utilized to collect relevant literature.
2. Analysis of Existing Research: The collected literature was carefully analysed to identify key concepts, trends, and findings related to cryptocurrencies as a payment method. The analysis included examining the advantages, disadvantages, and challenges associated with cryptocurrencies in payment transactions.
3. Comparison with Traditional Payment Methods: The methodology also involved a comparison of cryptocurrencies with traditional payment methods, such as cash, credit cards, and bank transfers. The comparison was based on factors such as security, transparency, transaction speed, and cost-effectiveness.
4. Case Studies: Case studies of real-world examples of cryptocurrencies being used as a payment method were analysed to understand their practical application and challenges faced in different contexts. Case studies included examples from various industries, such as e-commerce, remittances, and cross-border transactions.
5. Synthesis of Findings: The findings from the literature review, analysis of existing research, comparison with traditional payment methods, and case studies were synthesized to provide a comprehensive overview of cryptocurrencies as a payment method. This synthesis helped in identifying the key opportunities,

challenges, and potential future developments in this field.

6. Limitations: The limitations of cryptocurrencies as a payment method, such as volatility, scalability, regulatory challenges, and user experience, were discussed based on the literature review and analysis.
7. Conclusion: Finally, the paper concluded with a summary of the key findings and recommendations for further research and potential future developments in the field of cryptocurrencies as a payment method.

In conclusion, this technical paper utilized a systematic methodology of literature review, analysis of existing research, comparison with traditional payment methods, case studies, synthesis of findings, and discussion of limitations to provide a comprehensive overview of cryptocurrencies as a payment method. The findings from this research can help in understanding the current state, opportunities, challenges, and potential future developments in this field, and contribute to the ongoing discourse on the role of cryptocurrencies in the payments industry.

IV. ADVANTAGES

Cryptocurrencies offer several advantages as a payment method:

1. Security: Cryptocurrencies use cryptographic techniques to secure transactions, making them highly secure and resistant to fraud and unauthorized access.
2. Transparency: Transactions on the blockchain are transparent and traceable, providing a high level of accountability and reducing the risk of corruption and fraud.
3. Speed and Efficiency: Cryptocurrency transactions are typically processed faster than traditional payment methods, especially for cross-border transactions, which can take days or even weeks with traditional systems.
4. Cheaper Transaction Fees: When compared to more conventional payment options, cryptocurrency transactions frequently have cheaper transaction fees. which can be cost-effective, especially for large transactions.
5. Accessibility: Cryptocurrencies are borderless and can be used for transactions globally without the need for intermediaries, making them accessible to anyone with an internet connection.

V. CHALLENGES

Despite the advantages, there are also challenges associated with using cryptocurrencies as a payment method:

1. Volatility: Cryptocurrencies are highly volatile, with prices that can fluctuate significantly within a short period of time. This makes them less stable and less reliable for transactions, as the value of the cryptocurrency can change before the transaction is confirmed.
2. Scalability: Some cryptocurrencies, such as Bitcoin, have limitations in terms of scalability, with slow transaction times and high transaction fees during peak periods. This can affect the user experience and hinder widespread adoption as a payment method.
3. Regulatory Framework: Cryptocurrencies are subject to various regulatory frameworks in different jurisdictions, which can create legal uncertainties and compliance challenges for businesses and users.
4. User Experience: Cryptocurrency transactions can be complex and require technical knowledge, which can be a barrier to entry for mainstream adoption. Additionally, the irreversible nature of cryptocurrency transactions can also be a disadvantage in case of mistakes or fraud.

`

V. CONCLUSION

In conclusion, cryptocurrencies, such as Bitcoin, Ethereum, and Ripple, have emerged as a decentralized digital currency that holds the potential to disrupt the traditional payment landscape. Through a systematic review of literature and analysis of existing research, it is evident that cryptocurrencies offer several advantages as a payment method, including faster, cheaper, and more transparent transactions. The utilization of cryptographic techniques for securing transactions and controlling the creation of new units adds an additional layer of security to the payment process.

However, cryptocurrencies also face challenges as a payment method, such as volatility, scalability, regulatory frameworks, and user experience. The lack of widespread acceptance and regulatory clarity, coupled with the fluctuating value of cryptocurrencies, presents risks and uncertainties for both consumers and merchants.

Furthermore, cryptocurrencies are often compared with traditional payment methods, such as cash, credit cards, and bank transfers, in terms of their security, transparency, transaction speed, and cost-effectiveness. While cryptocurrencies offer unique advantages, they also have limitations that need to be addressed for broader adoption in the payments industry.

Despite the challenges, cryptocurrencies have been increasingly used as a payment method in various industries, including e-commerce, remittances, and cross-border transactions. Real-world case studies have provided insights into the practical application of cryptocurrencies for payments, highlighting both the opportunities and challenges associated with their use.

Looking ahead, future developments, trends, and potential use cases of cryptocurrencies as a payment method are still evolving. As regulatory frameworks continue to evolve, technological advancements are made, and user adoption increases, cryptocurrencies may play a more significant role in the payments landscape in the future.

In conclusion, cryptocurrencies have the potential to revolutionize the way payments are made by offering advantages such as decentralization, security, transparency, and efficiency. However, challenges related to volatility, scalability, regulations, and user experience need to be addressed for wider adoption. Further research, innovation, and collaboration between stakeholders are required to unlock the full potential of cryptocurrencies as a payment method in the future.

I. REFERENCES

[1] “Daozhuang Lin,Wei Tang,Hui Ding,”IEEE Standard for General Process of Cryptocurrency Payment”,

[2]“Daozhuang Lin,Wei Tang,Hui Ding,“IEEE Standard for General Requirements for Cryptocurrency Exchanges”,

[3] “Daojing He, Shihao Li, Cong Li, Sencun Zhu, Sammy Chan , Min, and Nadra Guizani, “Security Analysis of Cryptocurrency Wallets in Android-based Applications”,

[4] Saurabh Suratkar, Mahesh Shirol,Sunil Bhirud “Cryptocurrency Wallet: A Review”,

[5] Yi Liu, Ruilin Li, Xingtong Liu , Jian Wang , Lei Zhang , Chaojing Tang and Hongyan Kang, “An Efficient Method to Enhance Bitcoin Wallet Security, IEEE 2017”.

[6] Yi Liu, Xingtong Liu, Lei Zhang, Chaojing Tang and

Hongyan Kang, An Efficient Strategy to Eliminate Malleability of Bitcoin Transaction, IEEE 2017,

[7] Arunmozhi Manimuthu, Raja Sreedharan V , Rejikumar G and Drishti Marwaha, A literature review on Bitcoin: Transformation of crypto currency into a global phenomenon, IEEE 2018.

[8] Fangdong Zhu, Wen Chen, Yunpeng Wang, Ping Lin , Tao Li, Xiaochun Cao and Long Yuan, Trust Your Wallet: A New Online Wallet Architec-ture for Bitcoin, IEEE 2017.