IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024

DOI: 10.17148/IJIREEICE.2024.12902

# E-Commerce Based Secured Payment using Cryptocurrency

**Jeffrin Hannah I[1], Thulasimani K[2]**

P. G. Student, Department of Computer Science and Engineering, GCE, Tirunelveli[1]

Professor, Department of Computer Science and Engineering, GCE, Tirunelveli[2]

**Abstract:** The global e-commerce landscape has witnessed exponential growth, revolutionizing how goods and services are bought and sold. With this surge in online transactions comes the imperative need for robust, secure payment mechanisms. In recent years, cryptocurrencies have emerged as a disruptive force in the realm of digital payments, offering decentralized, secure, and transparent alternatives to traditional fiat currencies. This paper delves into the intricacies of integrating cryptocurrency-based secure payment systems into the e-commerce ecosystem. Cryptocurrencies, powered by blockchain technology, provide a decentralized ledger that records transactions across a distributed network of computers. This distributed nature ensures immutability and transparency, reducing the risk of fraud and unauthorized access to sensitive financial data. Moreover, cryptographic techniques employed in cryptocurrencies offer enhanced security, safeguarding transactions against cyber threats and identity theft. However, the adoption of cryptocurrency payments in e-commerce is not without challenges. One significant hurdle is the inherent volatility of cryptocurrency markets, which can pose risks for both merchants and consumers in pricing goods and services. Scalability issues further complicate the integration process, as the current infrastructure struggles to accommodate the growing demands of a global e-commerce ecosystem

**Keywords:** Bitcoin, Consumer Adoption, Cryptocurrency, Digital Divide, e-Commerce, e- Payment, Payment Gateway-Digital Signature.

## I. INTRODUCTION

In recent years, the landscape of e-commerce has undergone a profound transformation, driven by technological advancements and changing consumer behaviors. With the rise of online transactions, ensuring secure payment mechanisms has become paramount for both businesses and consumers. Amidst this backdrop, cryptocurrencies have emerged as a promising alternative to traditional payment methods, offering a decentralized, secure, and efficient means of conducting financial transactions.

This journal aims to explore the integration of cryptocurrency-based secure payment systems within the realm of e-commerce. Cryptocurrencies, such as Bitcoin, Ethereum, and others, operate on blockchain technology, which provides a transparent and immutable ledger for recording transactions. The decentralized nature of blockchain eliminates the need for intermediaries, thereby reducing transaction costs and minimizing the risk of fraud.

The adoption of cryptocurrency payments in e-commerce holds several potential benefits. Firstly, it expands the reach of businesses by facilitating transactions on a global scale, overcoming the limitations of traditional payment systems that are often bound by geographical borders and currency exchange rates.

However, the widespread adoption of cryptocurrency-based secure payment systems in e-commerce is not without challenges. Concerns regarding price volatility, regulatory uncertainty, and scalability issues need to be addressed to foster trust and confidence among merchants and consumers. Furthermore, integrating cryptocurrency payments into existing e-commerce platforms requires technological infrastructure upgrades and user education initiatives to ensure smooth and seamless transactions.

## II. SIGNIFICANCE OF THE SYSTEM

The study of literature survey is presented in section III, Methodology is explained in section IV, section V covers the experimental results of the study, and section VI discusses the future study and Conclusion.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024

DOI: 10.17148/IJIREEICE.2024.12902

## III. LITERATURE SURVEY

Hash Functions:

Hash functions are essential cryptographic algorithms that take an input (data of any size) and produce a fixed-size output, known as a hash or digest. Cryptocurrencies commonly use hash functions such as SHA- 256 (Secure Hash Algorithm 256-bit) or Keccak-256 (used in Ethereum) for various purposes, including creating digital signatures, securing transactions, and mining blocks.

Public-Key Cryptography:

Public-key cryptography, also known as asymmetric cryptography, involves the use of key pairs: a public key and a private key. Public keys are shared openly and used to generate addresses for receiving cryptocurrency payments, while private keys are kept secret and used to sign transactions for spending funds. Algorithms like RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC) are commonly used for generating key pairs and digital signatures in cryptocurrencies.

Digital Signatures:

Digital signature algorithms allow users to authenticate and verify the integrity of transactions in cryptocurrencies. A digital signature is created using a private key and can be verified using the corresponding public key, ensuring that the transaction has not been tampered with and originates from the rightful owner. Common digital signature algorithms used in cryptocurrencies include ECDSA (Elliptic Curve Digital Signature Algorithm) and EdDSA (Edwards-curve Digital Signature Algorithm).

Consensus Mechanisms:

Consensus algorithms are crucial for maintaining the integrity and security of decentralized blockchain networks by ensuring agreement on the validity of transactions and the state of the ledger. The two most prominent consensus mechanisms used in cryptocurrencies are Proof of Work (PoW) and Proof of Stake (PoS), although there are several others like Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and more. PoW requires participants (miners) to solve complex cryptographic puzzles to add blocks to the blockchain, while PoS selects validators based on the amount of cryptocurrency they hold and their stake in the network.

Merkle Trees:

Merkle trees are data structures used to efficiently organize and verify the integrity of transactions in a blockchain. In a Merkle tree, each leaf node represents a transaction, and each non-leaf node is the hash of its children. This hierarchical structure allows for quick verification of the validity of individual transactions and the integrity of entire blocks, enhancing the efficiency and security of the blockchain.

## IV. METHODOLOGY

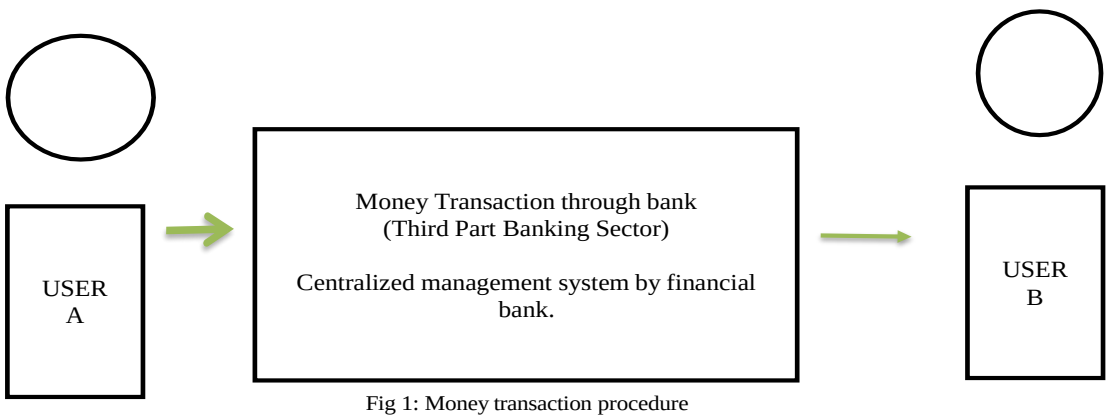



Fig 1: Money transaction procedure

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024

DOI: 10.17148/IJIREEICE.2024.12902

The block diagram illustrates a Money transaction procedure in a bank, the process typically begins with the payer initiating the transfer, providing necessary authentication such as identity verification and account validation, followed by detailing the recipient's information and transaction amount; upon authorization, the bank processes the transfer, which involves clearing and settlement procedures, and upon completion, both parties receive confirmation, and the transaction is recorded for future reference and reconciliation.

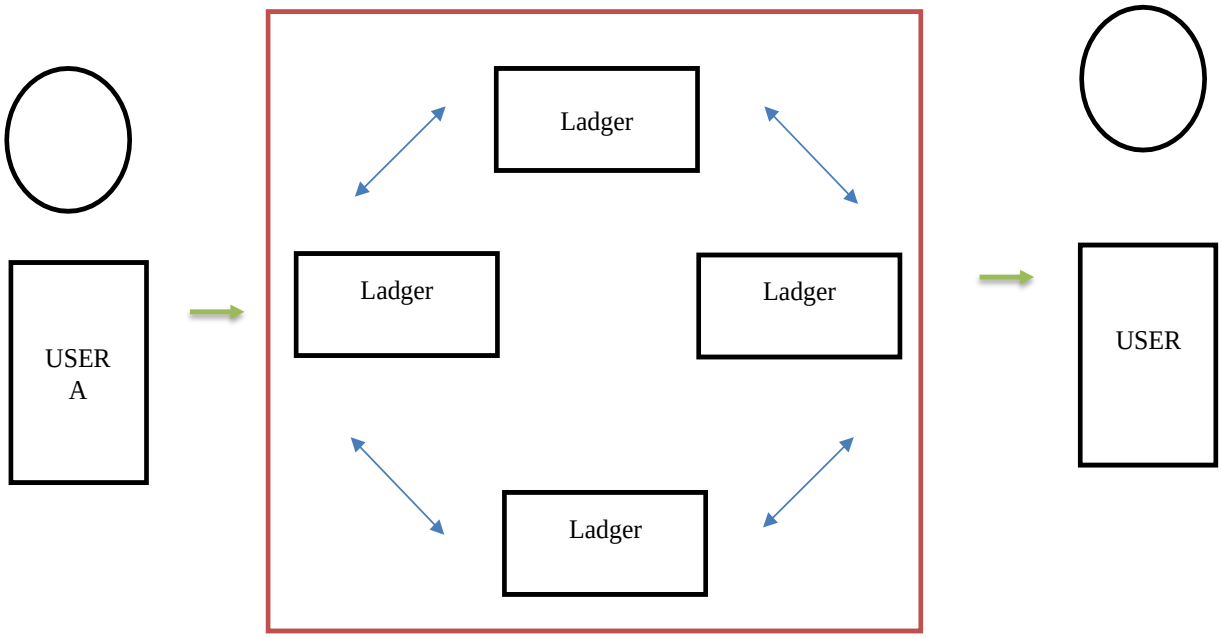



Fig 2: Cryptocurrency Transaction

The block diagram shows a cryptocurrency transaction, the sender initiates the transfer by generating a transaction with the recipient's wallet address and the amount to be sent, which is then signed with the sender's private key; this transaction is broadcasted to the cryptocurrency network where it undergoes verification and validation by network nodes before being included in a new block by miners, subsequently receiving confirmations as additional blocks are added to the blockchain; once confirmed, the cryptocurrency is credited to the recipient's wallet, and both parties can monitor the transaction's status through a blockchain explorer, ensuring transparent and secure peer-to-peer transfer of digital assets.

Hash Functions Algorithm:

The SHA-256 (Secure Hash Algorithm 256-bit) algorithm is widely used in various applications, including blockchain technology, digital signatures, password hashing, and data integrity verification. Here are some common use cases of the SHA-256 algorithm.

Blockchain Technology:

In blockchain protocols like Bitcoin and Ethereum, SHA-256 is used extensively to create cryptographic hash functions. Each block in the blockchain contains a hash of its header, which includes metadata such as the previous block's hash, transaction data, and a nonce. Miners compete to find a nonce that, when combined with the block's data, produces a hash value below a target threshold, thus solving the Proof of Work puzzle and adding a new block to the blockchain.

Digital Signatures:

SHA-256 is used in conjunction with public-key cryptography algorithms like RSA or ECC to generate and verify digital signatures. When signing a message or document, the SHA-256 algorithm is applied to the data to produce a hash, which is then encrypted using the signer's private key to create the digital signature. Recipients can verify the signature by decrypting it with the signer's public key and verifying that the computed hash matches the original data.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024

DOI: 10.17148/IJIREEICE.2024.12902

Password Hashing:

In cybersecurity, SHA-256 is commonly used for password hashing to securely store user passwords in databases. Instead of storing plaintext passwords, the SHA-256 algorithm is applied to the passwords to generate irreversible hash values, which are stored in the database. When a user attempts to log in, their input password is hashed using SHA-256, and the resulting hash is compared with the stored hash for authentication.

Cryptocurrency payment

User clicks on the "Login with MetaMask" button. MetaMask popup prompts the user to sign in or connect their wallet. Upon successful authentication, the user's Ethereum address is obtained and used for subsequent actions. Authenticated user session with MetaMask.

Payment Processing Algorithm:

User selects the product to purchase and initiates the payment process. The system generates a payment request containing the product details and the buyer's Ethereum address. MetaMask verifies the transaction details and prompts the user to confirm the payment. Upon confirmation, the transaction is signed with the user's private key and broadcasted to the Ethereum network. Moralis monitors the blockchain for the transaction confirmation and updates the payment status accordingly.

Transaction Verification Algorithm:

Moralis retrieves the transaction details from the Ethereum network using the transaction hash.
The system verifies the transaction status and confirms its validity. If the transaction is confirmed, the payment status is updated accordingly. Verified transaction status.

Order Fulfillment Algorithm:

The system validates the payment confirmation and the availability of the ordered products. Upon successful validation, the order fulfillment process is initiated. The seller is notified of the confirmed order and requested to fulfill it by shipping the products to the buyer. Once the products are shipped, the order status is updated, and the buyer is notified. Fulfilled order status.

Security Enhancement Algorithm:

The system conducts regular security audits to identify potential vulnerabilities. Vulnerabilities are prioritized based on their severity and impact on system security. Security patches and updates are implemented to address identified vulnerabilities. Continuous monitoring and threat detection mechanisms are deployed to mitigate security risks. Enhanced system security and reduced risk of security breaches.

Database Integration

The database underpinning this system is robust and secure, encompassing various modules to handle different types of data efficiently. For an e-commerce platform based on secured payment using cryptocurrency with React, Moralis, and MetaMask, the Moralis database would typically store various types of information related to users, products, transactions, and system settings. Here's an overview of the types of information that the Moralis database may contain:

User Information:

Including username, email address, Ethereum address (linked with MetaMask), and authentication tokens. Such as language, currency preference, and notification settings. Including product name, description, price in cryptocurrency (e.g., ETH), quantity available, and images. For organizing and filtering products. Details of completed transactions, including transaction IDs, buyer and seller Ethereum addresses, payment amounts, and timestamps. Information about orders, such as order IDs, purchased products, quantities, and total amounts. Records of system activities, such as user logins, product updates, and transaction processing. Aggregated data for tracking key performance indicators (KPIs), user engagement metrics.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024

DOI: 10.17148/IJIREEICE.2024.12902

## V. EXPERIMENTAL RESULTS

META MASK INTEGRATION:

$T=(P\times C)+( 100V \times P\times C)+(F\times C)+B$

Where:
T = Total cost in cryptocurrency.
P = Price of the product in fiat currency.
C = Conversion rate from fiat to cryptocurrency.
V = Variable transaction fee percentage.
F = Fixed transaction fee in fiat currency.
B = Blockchain network fee in cryptocurrency.

Input Parameters:

P: The price of the product is in fiat currency.
C: Conversion rate from fiat to cryptocurrency.
F: Fixed transaction fee in fiat currency.
V: Variable transaction fee as a percentage.
B: Blockchain network fee in cryptocurrency.

Output Parameters:
Total Cost in Cryptocurrency (T):
Total amount the customer has to pay in cryptocurrency.
Convert Price to Cryptocurrency:
Price in Cryptocurrency=$P\times C$

Calculate Variable Transaction Fee:
Variable Fee= $100\ V \times P$
Convert Fixed Transaction Fee to Cryptocurrency:
Fixed Fee in Cryptocurrency=$F\times C$

Calculate Total Fees:
Total Fees in Cryptocurrency = Fixed Fee in Cryptocurrency+(Variable Fee$\times C$)

Calculate Total Cost in Cryptocurrency:

T=**Price in Cryptocurrency+Total Fees in Cryptocurrency+B_rate P (price_fiat) = 100 USD**

C= **(conversion_rate) = 0.000034 BTC/USD**

F =**(fixed_fee_fiat) = 2 USD**

V= **(variable_fee_percent) = 1.5%**

B =**(blockchain_fee_crypto) = 0.0001 BTC**

The proposed system aims to develop a robust e-commerce platform that ensures secure and efficient cryptocurrency transactions. Leveraging technologies such as React for the front end, Moralis for blockchain interactions, and MetaMask for wallet authentication and transactions, the system provides a seamless and user-friendly experience for buyers and sellers engaging in cryptocurrency payments.

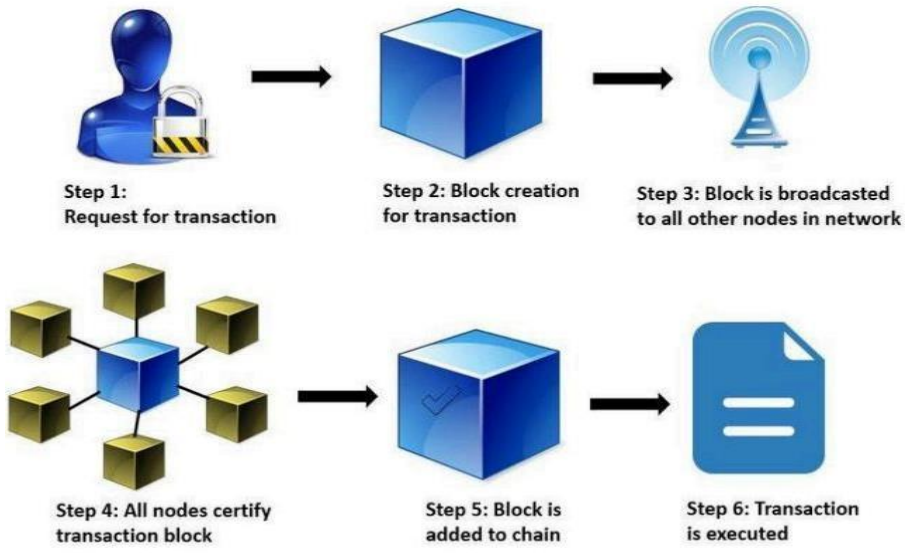
The technology of blockchain may also be adapted and implemented in other activities, such as healthcare, insurance, supply chain, IOT, and so on. Although it was designed to operate as a distributed ledger (on decentralized systems), it may also be deployed on centralized systems as a way to assure data integrity or to reduce operational costs.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

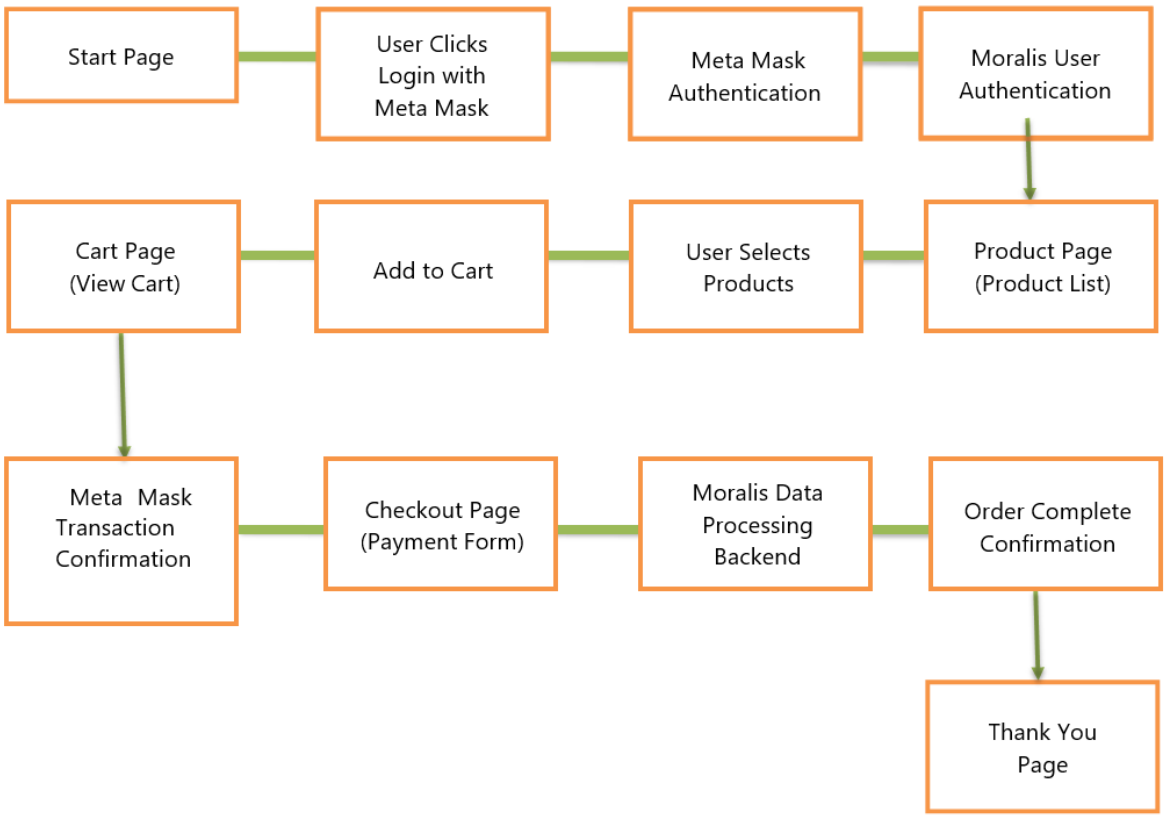
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024

DOI: 10.17148/IJIREEICE.2024.12902




*Blockchain technology*

The e-commerce transactions by leveraging cutting-edge technologies such as React, Moralis, and MetaMask to ensure secure and efficient payment processing using cryptocurrencies. With React powering the front end, the system offers a dynamic and user-friendly interface, allowing seamless navigation through product listings, cart management, and checkout processes.




Moralis, integrated into the backend, manages blockchain interactions, user authentication, and transaction monitoring, ensuring transparency and reliability throughout the payment process. Meanwhile, MetaMask provides secure wallet authentication and transaction processing, enabling users to seamlessly authorize cryptocurrency payments. Together, these components form a robust and innovative methodology for e-commerce-based secured payment, offering users a secure, transparent, and hassle-free experience in conducting transactions with cryptocurrencies

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2024
DOI: 10.17148/IJIREEICE.2024.12902

## VI. CONCLUSION AND FUTURE WORK

Cryptocurrencies are a hot topic in the global financial system. There is great volatility of cryptocurrencies exchange rates. With this, there is a high risk of trading these cryptocurrencies. Their growth has been able to gain the attention of many speculators. They are easily portable. It is only after the required trust in the cryptocurrencies after which they will be used on a wider scale. If the cryptocurrencies fail to gain that trust, then their boom might decline. They are still in their infancy, and itis not sure as to when they will be maturely traded in the markets globally. Many different cryptocurrencies have gained the required attention. Some nations have started to issue national cryptocurrencies. It is quite possible that shortly, the bitcoins might have a way for cryptocurrencies to flourish. Despite the flaws, bitcoins are still considered tour-de-force in the digital currency. It has provided an alternative currency for the less developed countries and has opened the doors of economic transformation. In this way, it gives the individuals more choices to manage their finances. Without regard to bitcoins accomplishing the lofty transformations, the cryptocurrencies are seen to Thirteenth International Conferencebe entering the financial stage and changing the global financial landscape forever. In many places, Crypto is not accepted as a legal tender. Since crypto transactions are hidden and there is no governing body, it is impossible to trace the case of fraud. It also does not save your transaction details therefore, the transaction is irreversible that is only one-way. Although, crypto is only for those who have the proper knowledge associated with it.

## REFERENCES

[1]. Adam Mukharil and Rani Nur Hanifah 2019 IOP Conf. Ser.: Mater. Sci. Eng. 662 032037 Bitcoin influence on E-commerce.
[2]. Bamert T, Decker C, Elsen L, Wattenhofer R, Welten S (2013) Have a snack, pay with Bitcoins in peer-to-peer computing (P2P). IEEE thirteenth international conference on IEEE 2013, pp 1-5
[3]. Buterin V (2014) Ethereum white paper: a next-generation smart contract and decentralized application platform. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf. Accessed 28 Feb 2019
[4]. Cheong C, Fong S, Lei P, Chatwin C, Young R (2012) Designing an efficient and secure credit card-based payment system with web services based on the ANSI X9.59-2006. J Inf Process Syst 8(3):495–520
[5]. Eskandari S, Clark J, Hamou-Lhadj A (2016) Buy your coffee with Bitcoin: real-world deployment of a Bitcoin points of sale terminal. 2016 Intl IEEE conferences on ubiquitous intelligence and computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people, and smart world congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), IEEE, pp 382–389. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016. 0073
[6]. Greenspan G (2015) MultiChain private blockchain—white paper. https://www.multichain.com/download/MultiChain-White-Paper.pdf. Accessed 28 Feb 2019
[7]. Hassan A, Eltayieb N, Elhabob R, Li F (2018) An efficient certificateless user authentication and key exchange protocol for client-server environment. J Ambient Intell Hum Comput 9:1713–1727
[8]. International standard ISO/IEC 18004, Information technology—automatic identification and data capture techniques—QR Code 2005 bar code symbology specification. ISO/IEC 18004:2006(E), Second edition
[9]. Isaaca J, Zeadally S (2012) Anonymous secure payment protocol in a payment gateway centric model. Procedia Comput Sci 10:758–765
[10]. Kim J, Kim Y (2011) A secure credit card transaction method based on Kerberos. J Comput Sci Eng 5(1):51–70
[11]. Malik J, Girdhar D, Dahiya R, Sainarayanan G (2014) Multifactor authentication using a QR code and a one-time password. J Inf Process Syst 10(3):483–490
[12]. Staiger, R. W., & Sykes, A. O. (2010). “Currency manipulation” and world trade. World Trade Review, 9(4), 583–627. doi:10.1017/S1474745610000340
[13]. Straub, D., Boudreau, M.-C., Gefen, D., & Straub, D., Boudreau, M.-C., Straub, D., … Gefen, D. (2004). Validation Guidelines for IS Positivist Research. Communications of the Association for Information Systems, 13(1), 380–427. doi:10.17705/1CAIS.01324
[14]. Teoh, W. M. Y., Chong, S. C., Lin, B., & Chua, J. W. (2013). Factors affecting consumers’ perception of electronic payment: An empirical analysis. Internet Research, 23(4), 465–485. doi:10.1108/IntR- 09-2012-0199
[15]. Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science, 46(2), 186–204. doi:10.1287/mnsc.46.2.186.11926
[16]. Vissor, L. (2016). Where to Spend Bitcoin in South Africa. Retrieved from https://www.luno.com/blog/en/post/south-africa-pay-with-bitcoin.