Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.249
Peer Reviewed Journal
https://doi.org/10.69758/GIMRJ/2411IV05V12P0001

e-ISSN No. 2394-8426
Special Issue On CPDE Nov'2024
Issue–III(V), Volume–XII

CRYPTOCURRENCY & BLOCKCHAIN SECURITY STANDARDS

Dr. A. A. Annapurna
Lecturer in Commerce
Government College (Autonomous) Rajahmundry

Abstract

Cryptocurrency is a digital payment system that is facilitated online enabling anyone from anywhere to transact by making payments or sending money. This paper intends to describe the evolution and meaning of cryptocurrency, its functioning, and the security aspects of using cryptocurrency. Digital transformation has already made us experience its presence in all walks of our lives and it is not going to take much time for the emergence of virtual exchange of value. Literacy of these transactions is essential to playing safe in the coming days. Transactions around the world are made in the absence of physical money. Cryptography is used to encrypt and decrypt information, hence the name cryptocurrency. Cryptocurrency works on a public ledger, which is called blockchain. Blockchain technology provides a secure platform. It creates a digital ledger for cryptocurrency transactions. In 2009 the first cryptocurrency was founded by the name Bitcoin and is the best of its kind to date. Still, this system is not immune to cyber-attacks and hackers. Here once money is lost it is lost forever. The backend process is very complex. Transactions are recorded into the blocks and time stamped. Thus, these transactions are secure. Cryptocurrency exchanges, mobile, and web applications are included to set standards for security. An idle cryptocurrency security standard requires an active information system. Cryptocurrency Security Standards (CCSS) provide smart choices and promote decision-making for purchase and investment in the right service. It also helps customers and investors to make better decisions with companies. Usually, standards have ten points to be fulfilled and are put up at 3 levels.

Key words: Cryptocurrency, Bitcoin, Blockchain, Cryptocurrency Security Standard, phishing,

Introduction:

Cryptocurrency has been in hype since the release of Bitcoin. Now Bitcoin and Ethereum are the top two cryptocurrencies that one can invest in. But the questions pondering one's mind,

Is cryptocurrency secure? How best to safeguard digital investments? And what measures exist with respect to cryptocurrency security?

Cryptocurrency: A digital payment system that is facilitated online enabling anyone from anywhere to transact by making payments or sending money is known as cryptocurrency.

Digital wallets are used to store cryptocurrencies and whenever a payment is made or received it is recorded in a public ledger.

All transactions are digitally entered into an online database mentioning the particulars of the transaction. The existence of physical money is totally absent. This implies transactions across the world are made in the absence of physical money.

These are peer-to-peer value exchange systems without banks' interference. For verification of transactions encryption (meaning the transactions are converted into secret codes to hide the true meaning) is used. In other words, cryptography is used to encrypt and decrypt information, hence the name cryptocurrency. Advanced coding is used to store and transmit cryptocurrency data between wallets and to public ledgers. This process ensures security and safety.

In 2009 the first cryptocurrency was founded by the name Bitcoin and is the best of its kind to date. Cryptocurrencies are used to trade for profit wherein prices are made to shoot abnormally high by the speculators.

Functioning of cryptocurrency

It is already stated that cryptocurrency works on a public ledger, which is called blockchain. A blockchain is a record of transactions that are updated and held by currency holders. Through the process of mining, cryptocurrency units are created. Mining involves the usage of computer power to generate coins as an outcome of solving complicated mathematical problems. These coins can be owned by users by buying them from brokers, and cryptographic wallets can be used to store and spend the coins. Owning a cryptocurrency means owning a key that allows us to record payment or receipt transactions among persons without any third-party interference. It is expected in the coming days securities will be traded by integrating technology and the application of blockchain will become the norm.

Evolution of Different Cryptocurrencies:

1. Bitcoin: Evolved in 2009 and most traded till date. It was developed by Satoshi Nakamoto, a pseudonym for an individual or group of people and their identity is unknown.
2. Ethereum: This was developed in 2015. It is a blockchain platform, having its own cryptocurrency known as Ether (ETH) or Ethereum.
3. Litecoin: It is similar to bitcoin and has been successful in developing new innovations including faster payments and processes to promote more transactions.
4. Ripple: It is a distributed ledger system, that was founded in 2012. It helps in tracking different kinds of transactions other than cryptocurrency. The developers of this currency worked with various banks and financial institutions.

Currencies other than bitcoins are called Non-Bitcoin cryptocurrencies or altcoins to differentiate them from the original.

Steps to Purchase a Cryptocurrency

Step 1: Identify a platform: This process involves deciding or choosing a traditional broker or cryptocurrency exchange.

A traditional broker is one who offers services to buy and sell cryptocurrency, and other financial assets. The trading cost is low and deals in a few cryptocurrencies.

Cryptocurrency exchanges offer different cryptocurrencies, wallet storage, interest-bearing account options, etc. Asset-based fee is collected by these exchanges.

Factors affecting the choice of platform:

a. Type of cryptocurrencies offered
b. Fees charged
c. Security Features offered by the platform
d. Storage and withdrawal options and
e. Educational resources

Step 2: Funding:

After choosing the platform, the account has to be provided with funds. This enables us to commence trading. Crypto exchanges allow users to purchase crypto using fiat. Fiats are government-issued currencies like the US dollar, the British pound, or the Euro using debit or credit cards. This option varies among different platforms. Cryptocurrencies are highly volatile and it is not advisable to purchase them with credit cards. Also, the fees charged varies according to the payment method used. Due diligence is suggested.

Step 3: Placing Order:

An order can be placed using brokers' or exchange's Web or mobile platform.

There are other ways to invest in crypto like PayPal, a cash app, Venmo, Bitcoin trusts, bitcoin mutual funds, and Blockchain stocks or ETFs. The best choice among the above depends on the investment goal and risk aptitude of the investor.

Literature Review

1. Alexakis, C., Anselmi, G., & Petrella, G. (2024). Flight to cryptos: Evidence on the use of cryptocurrencies in times of geopolitical tensions. *International Review of Economics and Finance*, *89*. https://doi.org/10.1016/j.iref.2023.07.054, This paper investigates cryptocurrency trading during geopolitical crises, focusing on Bitcoin, Ether, Ripple, Dash, and Tether. It finds increased cryptocurrency trading during periods of geopolitical tensions, possibly driven by reasons such as protecting savings, making payments, and avoiding sanctions. The study also notes a decrease in crypto trading when crypto-related services are explicitly included in financial sanctions. Additionally, it observes a significant increase in the outflow from Ukrainian Hryvnia into cryptocurrencies since the conflict began, suggesting a shift from domestic currency to cryptocurrencies among Ukrainians.
2. Liang, H., & Chen, J. (2024). Non-interactive SM2 threshold signature scheme with identifiable abort. *Frontiers of Computer Science*, *18*(1). https://doi.org/10.1007/s11704-022-2288-x, " A threshold signature is a special digital signature in which the N-signer share the private key x and can construct a valid signature for any subset of the included t-signer, but less than t-signer cannot obtain any information. Considering the breakthrough achievements of threshold ECDSA signature and threshold Schnorr signature, the existing threshold SM2 signature is still limited to two parties or based on the honest majority setting, there is no more effective solution for the multiparty case. To make the SM2 signature have more flexible application scenarios, promote the application of the SM2 signature scheme in the blockchain system and secure

cryptocurrency wallets. This paper designs a non-interactive threshold SM2 signature scheme based on partially homomorphic encryption and zero-knowledge proof. Only the last round requires the message input, so make our scheme non-interactive, and the pre-signing process takes 2 rounds of communication to complete after the key generation. We allow arbitrary threshold t ⩽ n and design a key update strategy. It can achieve security with identifiable abort under the malicious majority, which means that if the signature process fails, we can find the failed party. Performance analysis shows that the computation and communication costs of the pre-signing process grows linearly with the parties, and it is only 1/3 of the Canetti's threshold ECDSA (CCS'20).

3. Houy, S., Schmid, P., & Bartel, A. (2024). Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review. *ACM Computing Surveys*, *56*(1). https://doi.org/10.1145/3596906, Cryptocurrencies are increasingly popular, leading to a growing use of cryptocurrency wallet applications. These wallets are vulnerable to various attacks, and there is a gap between potential defenses and their implementation. Our research covers different attack vectors and suggests areas for future research to address this gap.
4. Yu, Q., Liao, S., Wang, L., Yu, Y., Zhang, L., & Zhao, Y. (2024). A regulated anonymous cryptocurrency with batch linkability. *Computer Standards and Interfaces*, *87*. https://doi.org/10.1016/j.csi.2023.103770,Cryptocurrencies like Bitcoin use blockchain for peer-to-peer transactions, but the public nature of on-chain data can compromise user privacy. To address this, we propose a new regulated anonymous cryptocurrency protocol to protect honest users' privacy while enabling authorities to trace suspicious transactions and identify malicious actors if needed. We demonstrate the protocol's security properties through detailed analysis and validate its feasibility with a prototype system.
5. Fuadi, F., Afrizal, A., Shabri Abd. Majid, M., Marliyah, M., & Handayani, R. (2022). A STUDY OF LITERATURE: CRYPTOCURRENCY OF SYARIAH PERSPECTIVE. *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, *2*(1). https://doi.org/10.54443/ijebas.v2i1.135, "Cryptocurrency is a digital or virtual currency that can only be used through devices connected to the internet. It offers advantages such as transaction security and global usability, but also has weaknesses, including the lack of supervisory authority and legal disagreements in many countries. There is a dynamic debate among experts, including scholars studying it from an Islamic perspective. Research aims to examine its use from the perspective of usul al-fiqh, allowing it under certain conditions, including the removal of prohibited elements mentioned in Quran surah An-Nisa verse 29. These elements are gharar and mayshir, and cryptocurrency must also have clear legality for security in its use.
6. Buja, A. G., Katan, M., Nasrijal, N. M. H., Alwi, S. F. S., & Siang, T. G. (2022). Into the Look: Security Issues, Crypto-Hygiene, and Future Direction of Blockchain and

Cryptocurrency for Beginners in Malaysia. *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2021*. https://doi.org/10.1109/ICRAIE52900.2021.9703957, The text you provided is a brief overview of blockchain and cryptocurrency for beginners in Malaysia. It discusses the vulnerabilities to cyber-attacks, as well as potential criminal activities such as money laundering and online gambling related to cryptocurrency. It also proposes improved crypto-hygiene as a guideline to mitigate cyber-attack risks for beginners interested in cryptocurrency and blockchain applications.

7. Sung, S. (2021). A new key protocol design for cryptocurrency wallet. *ICT Express*, *7*(3). https://doi.org/10.1016/j.icte.2021.08.002, This study proposes a secure key protocol using session keys and the Federated Byzantine Agreement (FBA) to address cryptocurrency wallet key theft. The model enhances security, reduces computation costs, and improves user privacy without relying on decentralized exchanges.
8. Bhushan, B., Sinha, P., Sagayam, K. M., & J, A. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers and Electrical Engineering*, *90*. https://doi.org/10.1016/j.compeleceng.2020.106897 "Blockchain is a decentralized public ledger that provides secure data storage and sharing. This paper surveys blockchain technology, analyzes security threats, emphasizes privacy needs, outlines challenges, proposes solutions, and highlights future research challenges."
9. França, A. S. L., Amato Neto, J., Gonçalves, R. F., & Almeida, C. M. V. B. (2020). Proposing the use of blockchain to improve the solid waste management in small municipalities. In *Journal of Cleaner Production* (Vol. 244). https://doi.org/10.1016/j.jclepro.2019.118529, A small municipality in São Paulo, Brazil is decisively replacing its paper-based waste management system with a blockchain-based system using Ethereum. This innovative approach will utilize social crypto-coins instead of printed cards to significantly enhance security, efficiency, and contribute to the Sustainable Development Goals.
10. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. In *Digital Communications and Networks* (Vol. 6, Issue 2). https://doi.org/10.1016/j.dcan.2019.01.005, "Since the release of Satoshi Nakamoto's Bitcoin white paper in 2008, blockchain has slowly become a frequently discussed method for securing data through decentralized, peer-to-peer systems. This research identifies literature that uses blockchain for cybersecurity and highlights its potential applications in IoT, networks, cryptography, web applications, certification schemes, and secure storage of Personally Identifiable Information (PII). The review also points to future research areas, such as blockchain security in IoT and for AI data."

Summary of Literature Review: The emerging literature review revolves around different models of cryptocurrencies among the World Economies. It is proven that digital currencies are evolving as a highly preferred source of investment with due diligence to its safety and security provided by the respective state authorities. A prudent integration of Technology is a researched area in most emerging economies. Under these circumstances, there is a felt need to understand A2Z of Digital currency.

Security Aspects:

Blockchain technology provides a secure platform. It creates a digital ledger for cryptocurrency transactions. The digital ledger makes it highly complicated for hackers to hack information. This phenomenon of the blockchain makes it most preferred worldwide. Yet this system is not immune to cyber-attacks and hackers.

Here once money is lost it is lost forever. The backend process is very complex. Transactions are recorded into the blocks and time stamped. Thus, these transactions are secure. It is proposed to make them further secure by measures like,

1. Two-stage authentication process. In the first stage, a username and then a verification code that is texted to a smartphone or sent to email is a good example of two-way security.
2. Every investor should make sure to invest by opening their own cryptocurrency.
3. Investors in cryptocurrency should be aware of the related security standards.

Cryptocurrency and blockchain security standards

Cryptocurrency exchanges, mobile, and web applications are included to set standards for security. An idle cryptocurrency security standard requires an active information system.

A well-designed information system helps to manage and standardize the techniques and performance methods to ensure security. Cryptocurrency Security Standards (CCSS) provide for smart choice and promote decision-making for purchase and investment in the right service. It also helps customers and investors to make better decisions with companies. Usually, standards have ten points to be fulfilled and are put up at 3 levels.

The ten points for setting standards are as follows:

- Key/seed generation
- Wallet Creation
- Key Storage
- Key Usage
- Key Compromise policy
- Keyholder Grant/ Revoke Policy and Procedures
- Third-party audits
- Data Sanitization Policy
- Proof of Reserve
- Log Audits

Risk in investing cryptocurrency and means to mitigate:

Investment in Cryptocurrency is not that secure because of the absence of third-party check. Though security standards adopted by different platforms minimize the risk, yet the personal faults at the individual level require attention. These risks include:

1. Cryptocurrency on a single exchange makes it prone to hackers.
2. Local Cryptocurrency often leads to data loss or stealing.
3. Email phishing attacks.
4. Personal attacks like SIM Swap assaults for clearing the 2-way authentication are used.
5. Cryptocurrency can be lost due to a natural disaster or by any accident.
6. Loss of generation of wealth which leads to damage of digital assets. This is caused by non-distribution of digital assets.

Protection of digital assets: The following points are of significance to protect Digital Assets.

1. Make a thorough study on Cryptocurrency Exchanges.
2. Cryptocurrency must be stored with due safety.
3. investors should plan a hybrid strategy to make investments.
4. Strong password
5. Use trustworthy wallets.
6. Do not share the digital currency key.

Prevention of Cyber Attacks:

1. Avoid storing cryptocurrency on digital storage.
2. Invest in buying a cryptocurrency hardware wallet.
3. Do not use public wifi while making transactions.
4. Use a private and secured internet connection.
5. Keep the security level high and do not install any unsecured apps.
6. Use 2-stage authentication and verification for better secure transactions.
7. Make sure to stay away from the bitcoin gambling sites.
8. Hold cryptocurrency privately.
9. Use a unique and robust password.
10. Do not share your passwords, key, and wallet details with anyone.

Following the above suggestions, investors can avoid loss arising from cyberattacks.

Security Measures for Cryptocurrency:

Some of the ways by which you can secure your crypto investments are as follows:

- Cold Wallet is a better option as it is not connected to the internet.
- Use a secured Internet Network
- Maintain multiple wallets
- Ignore phishing Mails
- Keep changing passwords.
- Update the device with the latest software
- Have antivirus software to protect the device from viruses and malfunctions.
- Keep keys separate and with high security.
- Invest in multiple cryptocurrencies rather than single currency.

Conclusion:

Future transactions are most likely to happen digitally without the physical existence of currencies. This will facilitate quick and safe transfers and minimize the factor fluctuations that are found in current money markets. Thus, understanding the concept of safely trading in cryptocurrency is very important to gain profit from investment.

References

https://www.blockchain-council.org/cryptocurrency/complete-guide-on-cryptocurrency-security/
https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency
https://www.ibm.com/topics/blockchain-security
https://www.simplilearn.com/what-is-blockchain-security-and-its-examples-article
https://www.geeksforgeeks.org/what-is-blockchain-security/