Cryptocurrencies: Scams and Preventions

Yishan Wu

Shenzhen Senior High School, China

ABSTRACT

This research paper aims to introduce cryptocurrency, discuss its running process and investment value, as well as analyze fraud cases and prevention measures for cryptocurrency scams. The article's structural framework, represented by Fig. 1, is presented for reference. Along with the rapid development of cryptocurrency, an increasing number of individuals are attracted to its investment value or the great profits that can be obtained in a short time. However, with its special features, such as decentralized management and irreversible exchange, cruel scams arise. Many people do not realize the ingeniousness and seriousness of fraud, and these preventive measures are not widely promoted, so people are easily deceived and become the target group of fraud gangs. Serious scams result in decreasing the reputation and credibility of cryptocurrency because they occur in a variety of situations and use various methods, causing the wealth accumulated for a long time to be wiped out in an instant. Nevertheless, with an overall understanding of the basic knowledge and running process of cryptocurrency and some awareness of common scams, the probability of such fraud incidents can be well reduced. This research paper combines the knowledge to enhance the awareness of cryptocurrency investors to prevent fraud, which is both beneficial to cryptocurrency development and people's investment experience.

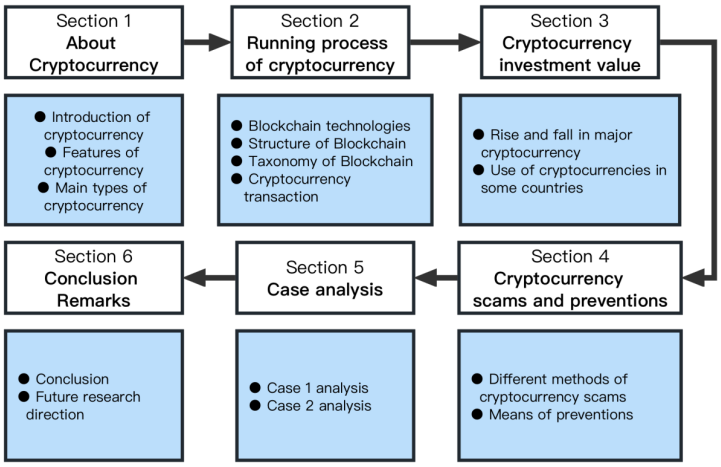


Figure 1.

About Cryptocurrency

Introduction to Cryptocurrency

What is Cryptocurrency

A cryptocurrency is a digital currency designed to be maintained or transacted through a computer network as a medium of exchange and is not dependent on any central authority, such as a government or bank(Milutinović, 2018).

This is a decentralized system for verifying that both parties to a transaction have the money they claim to have, eliminating the need for traditional intermediaries such as banks when money is moved between two entities (Yaffe-bellany, 2022).

History of Cryptocurrency

The idea of cryptocurrencies roughly predates the 2008 Bitcoin white paper by several decades. However, Bitcoin remains by far the most successful cryptocurrency.

In 2008, the renowned Satoshi Nakamoto released a well-known document titled "Bitcoin: A Peer-to-Peer Electronic Cash System," outlining strategies for an internet-based currency that enables direct transactions between individuals(Bitcoin, 2024c). They also use a consensus mechanism called proof-of-work (PoW) to verify that transactions on the Bitcoin network are valid. PoW forces computers to solve algorithmic puzzles to publish new transactions on the "blockchain"(Han et al., 2019). The blockchain contains all transactions on the network and is publicly visible. "Miners" use computing power on the Bitcoin network and are rewarded in BTC for each block they validate.

Features of Cryptocurrency

Anonymity

When talking about anonymity, the main part that must be considered is security.

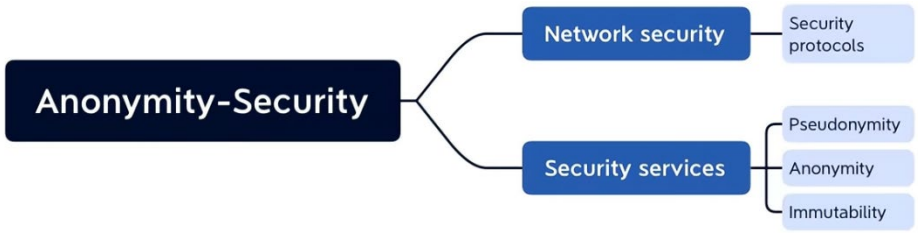


Figure 2.

(1) Network Security: The primary aspect of network security revolves around security protocols. In distributed systems, achieving a flawless consensus protocol remains an elusive goal. Consensus protocols require trade-offs between consistency, availability, and partition fault tolerance (CAP) (Gilbert & Lynch, 2002). Cryptocurrencies have protocols, and any cryptocurrency—Bitcoin, Ethereum, Ripple—has its own unique protocols. In the decentralized world of blockchain, security is provided by protocols that allow data to communicate without powering applications while also providing security.

(2) Security Services:

a. Pseudonym: A pseudonym is a fictitious name that a person or group assumes for a particular purpose, which differs from their original or true name(National Cancer Institute, 2020). Examples of pseudonyms are pen names, nicknames, credit card numbers, student numbers, bank account numbers, etc.

b. Anonymity: Anonymity describes a situation where the identity of the actor is unknown. The big idea here is that a person is unrecognizable, unapproachable, or untraceable (Wallace, 1999). Anonymity is seen as a technology or a way to achieve some other value, such as privacy or freedom.

Immutable: Immutability, or irreversibility, is considered a fundamental property of the blockchain, stemming from the fact that information about a transaction cannot be edited or deleted once it has been successfully verified and recorded into the blockchain (BitDegree, 2023).

Decentralized Finance and No Intermediary

Decentralized finance (DeFi) offers an alternative solution by utilizing a public blockchain network for conducting transactions, thereby removing the reliance on centralized service providers like custodians, central clearinghouses, or escrow agents. Instead, the responsibilities are carried out through what is widely referred to as "intelligent agreements." These agreements consist of computer code instructions stored on the public blockchain and executed in accordance with the system's consensus rules. Revisions to account balances and other status modifications are recorded on the blockchain, ensuring transparency and accessibility for all individuals To Verify (Schär, 2022).

The inherent security and transparency of blockchain eliminate the need for third-party intermediaries, thus requiring trust between users in a decentralized and untrusted environment (Marsh & Dibben, 2005). Blockchain effectively distributes trust from a single center to the entities of millions of users around the world. The highly praised pillar underpinning the secure and transparent nature of the blockchain, and thus guaranteeing its transaction integrity and auditability, is impermanence. The immutability of the blockchain comes from the fact that the transaction data residing in the blockchain are tamper-proof, i.e., they can neither be deleted nor mutated(BitDegree, 2023).

Irreversible Transaction

Once cryptocurrency transactions are verified, they become unchangeable and irreversible. The decentralized structure of blockchains guarantees that no entity has the ability to cancel, alter, or reverse these transactions (Wu et al., 2021). The all-inclusive bitcoin system, which includes blockchain technology, mining activities, proof of work protocols, mechanisms for adjusting difficulty levels, and other essential elements, greatly aids in the creation of an unchangeable record of transactions that is computationally impractical to alter.

Fast Development

Holders can use their cryptocurrencies through rapidly evolving tools and services. It is now possible to convert cryptocurrencies into dollars or euros. These currencies can be funded directly from cryptocurrency wallets through solutions that support conversion and exchange.

Main Types of Cryptocurrency

Bitcoin (BTC)

Bitcoin, the first-ever digital currency, operates as a system that enables the creation of a decentralized ledger known for its remarkable ease of use, transparency, long-lasting nature, and lack of control by any central entity. Its origins can be traced back to a white paper published in 2008. Bitcoin continues to be the most extensively acknowledged form of virtual currency, functioning on its autonomous blockchain network where transactions are authenticated by a decentralized consortium of miners(Bitcoin, 2024a).

Ethereum (ETH)

Ether is a digital currency that operates on the Ethereum blockchain. Just like Bitcoin, Ether has its own dedicated blockchain; however, unlike Bitcoin, there is no upper limit to the amount of Ether that can be created, theoretically allowing for an unlimited number of coins to exist(Ethereum, 2023).

Tether (USDT)

The Ethereum blockchain supports the use of Ether as a digital currency. Similar to Bitcoin, Ether functions within its dedicated blockchain (Tether, 2024); however, unlike Bitcoin, there are no limitations on the total supply of Ether coins and it has the potential for infinite creation.

Binance Coin (BNB)

Binance Coin, which is only accessible on the Binance platform, provides users with lower transaction fees as an incentive. This tactic has successfully encouraged the widespread adoption of Binance Coin and established it as a leading cryptocurrency in circulation(Binance Academy, 2024).

Running Process of Cryptocurrency

Blockchain Technology

In this age of technology, blockchain technology has experienced significant improvement and acquired tremendous attention from various domains. Many currencies use this technology. Blockchain technology is not as simple as it seems because it includes many complexities. Blockchain involves distributed networks, cryptography, data structures, and other scientific mechanisms, as well as combining with financial concepts like ledgers (Ghosh et al., 2020). Theoretically, due to the use of blockchain technology, cryptocurrencies are immune to counterfeiting and do not require a central authority, as well as can be protected by strong and complex encryption algorithms.

Structure of Blockchain

Block Header

It handles all the blocks and is used to identify a particular block in the entire blockchain. The header of the blockchain consists of six attributes:

(1) Version: The block version includes a set of validation rules that need to be followed (Bitcoin Developer, 2024).

(2) Previous Block Hash: It is a 32-bits bytes field that contains a 256-bits hash of the previous block. This helps create a linear chain of blocks (Bitcoin Developer, 2024).

(3) Merkel Root Hash: A Merkle Tree generates a digital fingerprint of the entire transaction, storing all the transactions in a block. It allows users to verify whether a transaction can be included in a block or not. Therefore, it supports the immutability of delivering as any change in transactions will cause the mismatch of the Merkle root hash. (Bitcoin Developer, 2024; GeeksforGeeks, 2022a)

(4) Timestamp: It is a system that validates the data into the block and assigns the digital document a time or date to be created(Ghosh et al., 2020). It's a digital record of the moment a block was mined.

(5) nBits: An encoded version of the target threshold this block's header hash must be less than or equal to.(Bitcoin, 2024b)

(6) Nonce: It is a field that contains a 32-bit number, which is a central part of the proof of work in the block.(Bitcoin Developer, 2024). Miners alter the nonce until they find the correct block hash.

Cryptographic Principles

Public and Private Keys: The public key is openly accessible and can be obtained by anyone, whereas the private key remains exclusively known to the individual. Other parties can utilize the public key for data encryption and subsequent transmission to you. (Rivest et al., 1978) Subsequently, you can decrypt the data using the corresponding private key to obtain the original information. Conversely, it is also possible to perform the reverse operation by employing the private key for data encryption, which can then be deciphered by others using the public key. When data is encrypted with one's private key, it can only be decrypted using its corresponding public key. This process is commonly employed for data authenticity verification and referred to as digital signing.

Hash Functions: The hash function is a fundamental cryptographic concept utilized in various computer science and information security applications, as well as being extensively employed in cryptocurrencies. It is a mathematical function that takes an input and generates a fixed-size string, typically represented by a hexadecimal number of a specified length.(GeeksforGeeks, 2022b). Typical hash functions are designed to handle variable-length inputs while producing outputs of fixed lengths. These outputs are commonly referred to as "hash values" or "hash codes". Hash functions possess the following properties:

(1) Collision resistance: It is impossible that two different inputs produce the same hash value (NIST, 2023).

(2) Avalanche effect: The result shows a noticeable difference when even a minor adjustment is applied to the input.

(3) Fixed output length: The hash function produces a hash value of fixed length, regardless of the size of the input data (Tutorialspoint, 2024).

(4) Concealed: It is hard to guess the input value from its output value.

Digital Signatures: To ensure data integrity and prevent unauthorized tampering, digital signatures offer a reliable assurance.

The initiator encrypts all data using their private key. Anyone with access to the sender's public key can decrypt the signature and compare it to the original message. Only individuals possessing the private key can generate a signature; therefore, when decrypted and matched against the original message, its integrity is confirmed, in case of any alterations made by an unauthorized party during transmission (Aki, 1983).

Taxonomy of Blockchain

Blockchains can be divided into three categories based on open permissions: Public chain, private chain, and affiliate chain.

The public chain is open to all individuals, enabling global registration and unrestricted trading. Bitcoin and Ethereum are well-known cryptocurrencies that utilize public chains. Conversely, there exists the affiliate chain which employs a restricted access mechanism, limiting usage solely to specific users with designated identities such as Fabric, BCOS, and Changan Chain. Lastly, private chains are utilized exclusively by individuals or companies themselves with an additional access mechanism for specific users only. These types of chains are commonly employed for testing blockchain products like Ethereum and Changan Chain where only one node can be operated while compromising consensus due to the absence of decentralization in their purpose.

Cryptocurrency Transaction

When the structures and functions above are connected, people can transact cryptocurrency on some platforms, which are called cryptocurrency exchanges. Binance, Coinbase Exchange, and Kraken are currently the top three mainstream exchanges(CoinMarketCap, 2024). During a transaction, when a user intends to transfer virtual currency to another address, they use their private key to sign the transaction as proof of its initiation by the rightful owner. Concurrently, other users can verify the signature using the public key associated with that address to ensure the genuineness of the transaction. This encryption technology employing both public and private keys guarantees the security and dependability of the virtual currency network.

Cryptocurrency Investment Value

Rise and Falls in Major Cryptocurrencies

There are several reasons why the prices of cryptocurrencies always rise and fall. They are influenced by demand and supply, investors' actions, government regulations, as well as media hype (Reiff, 2024).

Demand and Supply

As we all know, demand and supply are the key factors influencing the prices of products or services. The cryptocurrency market is mainly influenced by how much people are able and willing to pay and how many cryptocurrencies are available within a market.

Investors' Actions

Cryptocurrencies' volatility is also driven by investors. If a major player with significant holdings of virtual currency decides to sell a specific quantity, it is highly probable that this action will result in a substantial downturn.

Government Regulation

Government policies have a substantial influence on the volatility of virtual currencies. The regulations announced by the Chinese government and central bank in 2021, declaring all cryptocurrency transactions as illegal, have had a profound impact on Bitcoin mining(People's Bank of China, 2021; Reiff, 2024). Consequently, the price of Bitcoin experienced a significant decline to approximately $29,700 in August 2021(Reiff, 2024).

Media Hype

Media organizations provide a plethora of cryptocurrency information to investors; however, the veracity of these insights and forecasts remains inadequately verified. When a media organization extensively promotes the exponential growth potential of a specific cryptocurrency, it incites an influx of investments from numerous individuals, consequently driving up its value.

Use of Cryptocurrency in Some Countries

In the dynamic landscape of cryptocurrency advancements, some nations embrace and endorse the proliferation and exchange of digital currencies, while others have enacted measures to curtail their growth. Here is an image about the legality of cryptocurrency by country or territory (Wikipedia, 2024).

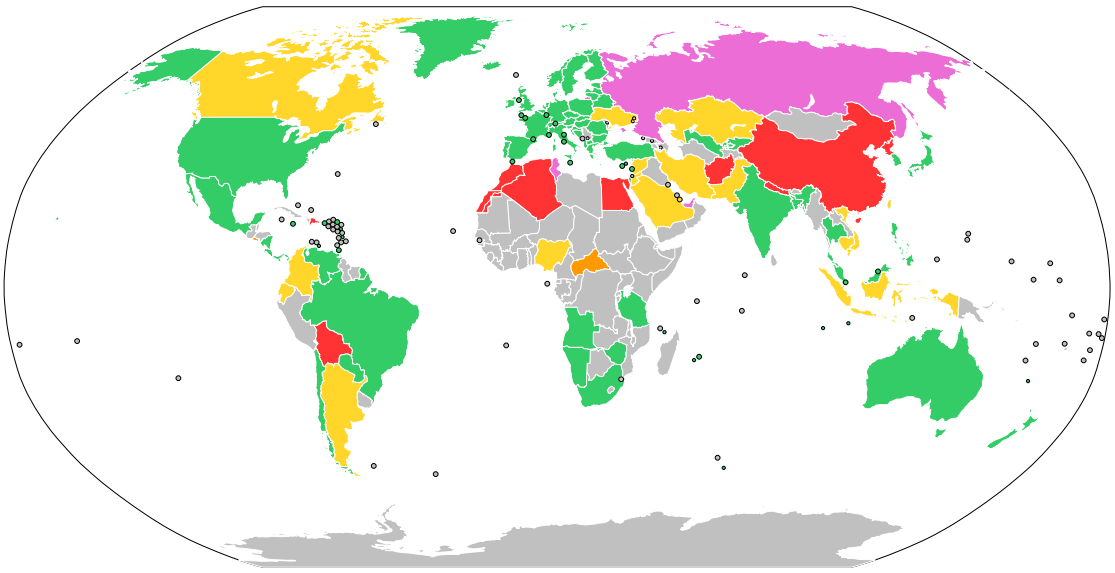
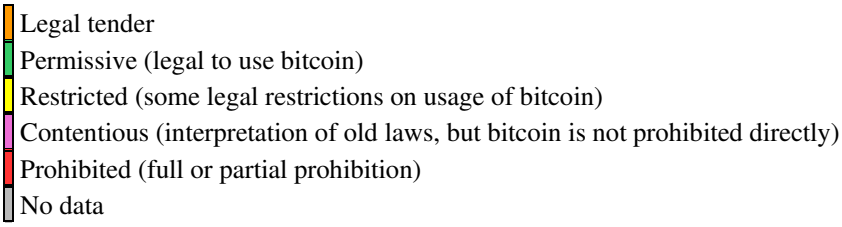


Figure 3. (Legality of Cryptocurrency by Country or Territory - Wikipedia, 2023)(Wikipedia, 2024). Legal status of bitcoin (Wikipedia, 2024)



Amsterdam Airport Allows Travelers to Convert Euros into Cryptocurrencies

The Amsterdam-based Schiphol airport has introduced an automated teller machine (ATM) that enables departing passengers to conveniently convert their remaining euros into either bitcoin or Ethereum. This move allows for a more convenient and accessible way for individuals to exchange currencies, particularly those interested in investing in cryptocurrency. The airport will install a machine in the departures terminal for travelers to exchange euros for two popular cryptocurrencies before leaving the country. The Consumer Products & Services Director at Schiphol Airport predicts that this bitcoin ATM will offer a hassle-free solution for travelers who cannot use euros in their home countries, allowing them to easily exchange their money into cryptocurrencies like Bitcoin and Ethereum. The pursuit of this initiative is driven by the increasing recognition of cryptocurrency as a valuable additional service for travelers in different international airports worldwide(Zhao, 2021).

Cryptocurrency Scams and Preventions

The increasing adoption of cryptocurrencies has garnered significant attention from legitimate investors as well as fraudulent individuals seeking to exploit this expanding market. Here are some prevalent scams and effective countermeasures against them.

Phishing and Deceptive Platforms

Fake Cryptocurrency Exchange

Description: Scammers create fake platforms for trading cryptocurrencies with the intention of luring investors through attractive incentives.

Risk: Investors may unknowingly transfer their funds, only to realize later that the exchange is fraudulent, leading to financial losses.

Preventive measures: Adhere to reputable and well-established cryptocurrency exchanges. Conduct comprehensive investigations on newly introduced exchanges and exercise caution when dealing with unfamiliar platforms.

ICO and Fake Cryptos

Description: Deceptive Initial Coin Offerings (ICOs) entice potential investors with enticing prospects for early investments. However, once the funds are gathered, the ICO fails to materialize, resulting in financial detriment.

Risk: Investors face monetary losses without any returns on their investments.

Preventive measures: To minimize the similarity score, it is advisable to conduct extensive research on initial coin offerings (ICOs) prior to making any investments. It is recommended to make use of available resources provided by regulatory authorities like the U.S. Securities and Exchange Commission (SEC) for conducting thorough due diligence.

Rug Pull Scams

Description: Crypto projects that generate excessive hype often prove to be non-existent, resulting in the disappearance of creators along with investors' funds.

Risk: Investors face potential loss of funds when the project abruptly disappears.

Preventive measures: Take precautions against excessively exaggerated projects. Prioritize confirming the authenticity of cryptocurrency ventures prior to making any investments.

Investment and Trading Scams

Ponzi Schemes

Description: Ponzi schemes entail utilizing funds from fresh investors to provide returns to previous investors.

Risk: Investors experience financial losses when the scheme eventually collapses.

Preventive measures: Exercise caution when considering investment opportunities that guarantee substantial returns without any associated risks.

Pump-and-Dump Bitcoin Scams

Description: Traders manipulate the value of an asset, such as Bitcoin, by artificially increasing it and subsequently selling it off quickly, resulting in a substantial decline in price.

Risk: Investors who purchase during this inflated period may experience financial losses.

Preventive measures: It is advisable to engage in comprehensive research prior to finalizing investment choices.

Information Interception and Identity Theft

Social Engineering Scams

Description: Fraudsters use phishing, hacking, and social media scams to trick investors into sharing personal information.

Risk: Fraudsters can access investors' portfolios if they have unauthorized login credentials.

Preventive measures: Exercise caution when asked to alter passwords or reveal information. Verify the origins of communication and utilize secure channels for transmission.

Middleman Scams

Description: Fraudsters illicitly obtain confidential data exchanged between investors and exchanges, thereby acquiring passwords or wallet keys.

Risk: The pilferage of assets is possible due to the interception of sensitive information.

Preventive measures: Refrain from using insecure networks and exercise vigilance against potential risks of interception.

Cryptocurrency Personal Fraud Case Analysis

In recent years, the impact of cryptocurrency scams have become a critical concern. More and more people are using decentralized cryptocurrency, which means that the risk of cryptocurrency exchanges is also increasing. Here are some examples of cryptocurrency scams.

Phony Exchange

This form of fraud has seen a rise in occurrence over the past few years, as it involves the combination of counterfeit exchanges and deceptive tactics to exploit individuals who may lack knowledge about cryptocurrency trading or its associated risks.

In this specific instance, Trader A became a victim of the scam when she received a text message purportedly from Binance, one of the world's largest cryptocurrency exchanges. The message informed her about regulatory modifications and urged her to transfer her held currency within a specified timeframe due to these changes. Additionally, the message contained a hyperlink that appeared to lead to Binance's official website. Trusting the authenticity of this communication as being genuinely from Binance, Trader A clicked on the provided link and was redirected to a browser interface that closely resembled Binance's legitimate website. This tactic is frequently employed by scammers who create counterfeit websites resembling genuine ones with the intention of deceiving users into disclosing their login credentials.

Recklessly unaware of any malicious intentions concealed within this seemingly authentic webpage, Trader A proceeded to input her account password as instructed. However, little did she know at that moment, this action led to an unauthorized swift transfer of her Bitcoin and Ethereum holdings out of her account. The total value of these pilfered cryptocurrencies equated to around $50,000 – a substantial financial and emotional setback for Trader A. Regrettably, instances such as these underscore the increasing sophistication employed by scammers in their tactics while continuously discovering means to exploit vulnerabilities within digital platforms.

It is crucial for individuals involved in cryptocurrency trading or any online financial transactions to remember the importance of being cautious while receiving unsolicited messages or clicking on unfamiliar links. To avoid falling prey to scams like these, it is advisable to verify the legitimacy of such communications through independent channels.

FTX Scam

Cryptocurrency fraud is far more than individual fraud. There are larger teams to create more difficult to detect fraud. At the beginning of November 11, the world's third-largest exchange collapsed due to the $8 billion hole caused by customer withdrawals. This case is quite complex and involved a huge loss of investment capital. FTX scam is also a classic case of a Ponzi scheme.

FTX Trading Ltd., commonly referred to as FTX (abbreviated from "Futures Exchange"), is a defunct company that previously operated a cryptocurrency exchange and crypto hedge fund plagued by fraudulent activities(Zuckerman & Osipovich, 2020). Founded in 2019 by Sam Bankman-Fried and Gary Wang, the exchange experienced its peak in July 2021 with more than one million users, ranking as the third-largest cryptocurrency exchange based on trading volume (The Associated Press of NPR, 2022).

Alameda and FTX, as two sister companies founded by SBF, cooperate with each other. FTX is responsible for issuing the token FTT, while Alameda is responsible for boosting the token price. In the early stages, FTX can secretly sell more low-priced FTT to Alameda, allowing the latter to earn higher profits in the secondary market. In a chaotic cryptocurrency market, these practices are openly conducted without disguise(Bloomberg, 2023; Osipovich, 2021).

On November 2nd, reports from industry media such as CoinDesk revealed detailed information about Alameda's balance sheet, raising concerns in the market. It was discovered that Alameda had purchased a large amount of FTT tokens at lower prices and drove up their market price, but instead of selling them for profit, they used these high-priced FTT tokens as collateral to apply for loans on the FTX platform. However, these loans were funded by misappropriated customer funds from the FTX platform. Specifically, out of the 16 billion yuan in customer funds held on the FTX platform, over 10 billion yuan was used by Alameda to execute its aggressive strategy, resulting in a massive shortfall of 8 billion yuan on the FTX platform when user redemption demands increased. With a huge capital shortfall,

FTX filed for bankruptcy within a week, and the value of its shares went straight to zero. At the point of the cryptocurrency firm's declaration of insolvency, FTX and FTX US were facing a combined deficit of approximately $8.7 billion. It is the second-highest financial fraud case in U.S. history, behind Bernie Madoff's spectacular 2008 fraud (Torpey, 2023).

The downfall of FTX underscores the potential hazards linked to cryptocurrency investments and raises concerns regarding safeguarding investors in this rapidly evolving market. It serves as a reminder that individuals should exercise caution and thoroughly investigate before engaging in any investment activities. Investors should remain vigilant, educate themselves about possible risks, and seek guidance from reliable experts when navigating the cryptocurrency market. By doing so, they can make well-informed decisions while minimizing their exposure to fraudulent schemes (Yaffe-Bellany et al., 2023).

Furthermore, it is crucial for global authorities to cooperate on regulatory frameworks that safeguard investors while also encouraging innovation. Given the increasing worldwide acceptance of cryptocurrencies, it becomes imperative to establish unambiguous directives in order to cultivate a secure and open atmosphere for individuals involved in this emerging category of assets.

Conclusion Remarks

Discussion

Social

Looking at it from a societal perspective, the future advancement of cryptocurrencies holds the potential to drive both economic growth and heightened vulnerabilities in terms of security. The integration of blockchain technology can foster efficiency and transparency, thereby contributing to economic progression. However, the emergence of digital assets may also give rise to challenges pertaining to cybercrime and fraudulent activities, necessitating robust security measures and law enforcement capabilities.

Financial

In the realm of finance, continuous advancements in technology and innovations in currency, such as the introduction of central bank digital currencies (CBDCs), have the potential to reshape the traditional financial landscape. It is essential to strike a balance between fostering innovation and safeguarding against any disruptions that may arise. Regulatory frameworks must adapt accordingly to ensure a secure and equitable financial environment.

Political & Legal

Politically and legally, the direction of cryptocurrency development will heavily rely on effective governance and regulation. Governments should establish policies that steer the responsible growth of this emerging sector. Regulatory authorities must tackle potential risks and vulnerabilities to uphold market stability while encouraging innovation.

Personal

From a personal standpoint, the future of cryptocurrency offers both possibilities and hazards. Individuals who possess expertise and abilities in this domain may discover fresh career opportunities, but they must also navigate potential drawbacks such as investment uncertainties and concerns regarding privacy. It will be crucial for individuals engaging with cryptocurrencies to enhance their financial knowledge and consciousness.

Essentially, the fate of digital currencies relies on finding a careful equilibrium between fostering creativity and mitigating potential hazards. The path ahead is shaped by societal, economic, political, and individual elements that call for a comprehensive and flexible strategy to guarantee responsible expansion in this constantly evolving virtual domain.

Conclusion

In summary, this study thoroughly explores digital currency, covering operational processes, investment appeal, and the complex landscape of fraudulent activities. Figure 1 provides a comprehensive visual guide.

As discussed, individuals' lack of fraud prevention knowledge makes them vulnerable to deceptive tactics used by fraudulent groups. These schemes, occurring in various scenarios, not only deplete personal wealth but also damage trust within the cryptocurrency community. However, a solid understanding of cryptocurrency fundamentals and awareness of scams significantly reduces the risk of falling victim to fraud.

In the evolving digital asset landscape, striking a balance between promoting technological advancements and implementing prudent regulations is crucial. Proper oversight mitigates risks associated with fraudulent activities, establishing a strong foundation. Collective awareness of potential scams is essential for cautious navigation. Embracing cryptocurrencies' transformative power in a secure and regulated framework inspires confidence in their enduring potential.

Reference

Aki. (1983). Digital signatures: A tutorial survey. *Computer*, *16*(2), 15-24. https://doi.org/10.1109/mc.1983.1654294

Binance Academy. (2024). *BNB*. Binance Academy. Retrieved Feb 8, 2024 from https://academy.binance.com/en/glossary/bnb

Bitcoin. (2024a). *Bitcoin for Individuals - Bitcoin*. Bitcoin for Individuals. Retrieved Feb 8, 2024 from https://bitcoin.org/en/bitcoin-for-individuals

Bitcoin. (2024b, Feb 8, 2024). *nBits, Target Threshold*. Bitcoin. https://btcinformation.org/en/glossary/nbits

Bitcoin. (2024c). *A Peer-to-Peer Electronic Cash System*. Bitcoin. Retrieved Feb 8, 2024 from https://bitcoin.org/en/bitcoin-paper

Bitcoin Developer. (2024). *Block Chain*. Bitcoin Developer. Retrieved Feb 8, 2024 from https://developer.bitcoin.org/reference/block_chain.html

BitDegree. (2023). *What is Immutable?* BitDegree web Learning Hub. Retrieved Feb 8, 2024 from https://www.bitdegree.org/crypto/learn/crypto-terms/what-is-immutable

Bloomberg. (2023, Oct 19). *Bloomberg L.P. About, Careers, Products, Contacts*. Bloomberg L. P. Retrieved Feb 8, 2024 from https://www.bloomberg.com/company/

CoinMarketCap. (2024). *Top Cryptocurrency Exchanges by Trading Volume*. CoinMarketCap. Retrieved Feb 8, 2024 from https://coinmarketcap.com/zh/rankings/exchanges/

Ethereum. (2023, Aug 15). *Intro to Ethereum*. Ethereum. Retrieved Feb 8, 2024 from https://ethereum.org/en/developers/docs/intro-to-ethereum/

GeeksforGeeks. (2022a, Nov 16). *Blockchain Structure*. GeeksforGeeks. Retrieved Feb 8, 2024 from https://www.geeksforgeeks.org/blockchain-structure/

GeeksforGeeks. (2022b, Mar 09). *Hash Functions and list/types of Hash functions*. GeeksforGeeks. Retrieved Feb 8, 2024 from https://www.geeksforgeeks.org/blockchain-structure/

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, *163*, 102635. https://doi.org/10.1016/j.jnca.2020.102635

Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *ACM SIGACT News*, *33*(2), 51-59. https://doi.org/10.1145/564585.564601

Han, R., Foutris, N., & Kotselidis, C. (2019). Demystifying crypto-mining: Analysis and optimizations of memory-hard pow algorithms. 2019 IEEE international symposium on performance analysis of systems and software (ISPASS), Madison, WI, USA.

Marsh, S., & Dibben, M. R. (2005). Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side. In *Trust Management* (pp. 17-33). https://doi.org/10.1007/11429760_2

Milutinović, M. (2018). Cryptocurrency. *Ekonomika*, *64*(1), 105-122. https://doi.org/10.5937/ekonomika1801105M

National Cancer Institute. (2020). *Pseudonym*. Qeios. https://doi.org/10.32388/oi9cnu.

NIST. (2023, June 16). *Hash Functions*. NIST. Retrieved Feb 8, 2024 from https://csrc.nist.gov/projects/hash-functions

Osipovich, A. (2021, Jul 20). *Crypto Exchange FTX Valued at $18 Billion in Funding Round*. WSJ. Retrieved Feb 8, 2024 from https://www.wsj.com/articles/crypto-exchange-ftx-valued-at-18-billion-in-funding-round-11626800455

People's Bank of China. (2021). *Circular on Further Preventing and Disposing of the Risks of Speculation in Virtual Currency Trading*. Central People's Government of the People's Republic of China. Retrieved Fen 8, 2024 from https://www.gov.cn/zhengce/zhengceku/2021-10/08/content_5641404.htm

Reiff, N. (2024, Jan 13). *Why Is Bitcoin Volatile?* Investopedia. Retrieved Feb 8, 2024 from https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126. https://doi.org/10.1145/359340.359342

Schär, F. (2022). *Defi Promise and pitfalls Fabian Schar*. IMF. Retrieved Feb 8, 2023 from https://www.imf.org/en/Publications/fandd/issues/2022/09/Defi-promise-and-pitfalls-Fabian-Schar

Tether. (2024, Feb 5). *What are Tether tokens and how do they work?* Tether. Retrieved Feb 8, 2024 from https://tether.to/en/news

The Associated Press of NPR. (2022, Nov 14). *The downfall of FTX's Sam Bankman-Fried sends shockwaves through the crypto world*. NPR. Retrieved Feb 8, 2024 from https://www.npr.org/2022/11/14/1136482889/ftx-sam-bankman-fried-shockwaves-crypto

Torpey, K. (2023, October 20). *Why FTX's Plan To Refund 90% of Recovered Assets Doesn't Add Up To 90% of Customer Losses*. Investopedia. Retrieved Feb 8, 2024 from https://www.investopedia.com/why-ftx-plan-to-refund-90-percent-of-recovered-assets-doesnt-add-up-to-90-percent-of-what-customers-lost-8362556

Tutorialspoint. (2024). *Cryptography Hash functions*. Tutorialspoint. Retrieved Feb 8, 2024 from https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Wallace, K. A. (1999). Anonymity. *Ethics and Information Technology*, *1*(1), 21-31. https://doi.org/10.1023/A:1010066509278

Wikipedia. (2024, Jan 15). *Legality of cryptocurrency by country or territory*. Wikipedia. Retrieved Feb 8, 2024 from https://en.wikipedia.org/wiki/Legality_of_cryptocurrency_by_country_or_territory

Wu, J., Liu, J., Zhao, Y., & Zheng, Z. (2021). Analysis of cryptocurrency transactions from a network perspective: An overview. *Journal of Network and Computer Applications*, *190*, 103139. https://doi.org/10.1016/j.jnca.2021.103139

Yaffe-bellany, D. (2022, Feb 13). Divorcing couples fight over the kids, the house and now the crypto. *The New York Times*. https://www.nytimes.com/2022/02/13/technology/divorce-bitcoin-crypto.html

Yaffe-Bellany, D., Goldstein, M., & Moreno, J. E. (2023, Nov 3). Sam Bankman-Fried Is Found Guilty of 7 Counts of Fraud and Conspiracy. *The New York Times*. https://www.nytimes.com/2023/11/02/technology/sam-bankman-fried-fraud-trial-ftx.html

Zhao, W. (2021, Sep 13). *Amsterdam Airport Lets Travelers Swap Leftover Euros for Crypto*. CoinDesk. Retrieved Feb 8, 2024 from https://www.coindesk.com/markets/2018/06/21/amsterdam-airport-lets-travelers-swap-leftover-euros-for-crypto/

Zuckerman, G., & Osipovich, A. (2020, Nov 12). *How FTX's Sam Bankman-Fried Went From Crypto Golden Boy to Villain*. WSJ. Retrieved Feb 8, 2024 from https://www.wsj.com/articles/how-ftx-sam-bankman-fried-went-from-crypto-golden-boy-to-villain-11668199208