Enhancing Cryptocurrency Security

Vivek Jaswal
Chandigarh School of Business, Jhanjeri
vivekjaswal14@gmail.com

Abstract:

Cryptocurrency, a decentralized frame of computerized cash, has picked up ubiquity around the world. In any case, its broad selection has brought consideration to noteworthy security concerns. This paper presents a exhaustive examination of cryptocurrency security, distinguishing key challenges and proposing arrangements to support the security of advanced assets. The paper starts by talking about the foundational innovation of cryptocurrencies, specifically blockchain, which offers straightforwardness and unchanging nature but is defenceless to assaults such as 51% assaults and double-spending. It at that point digs into security dangers related with cryptocurrency capacity and trade stages, counting wallet vulnerabilities and hacking incidents. Current security best hones, such as multi-signature wallets and cold storage solutions, are analysed, alongside rising innovations like zero-knowledge proofs and homomorphic encryption. Furthermore, the part of administrative systems in advancing cryptocurrency security is investigated, highlighting the require for a adjusted approach that energizes advancement whereas securing investors. In conclusion, guaranteeing the security of cryptocurrencies is basic for cultivating believe and widespread adoption. By tending to vulnerabilities and executing vigorous security measures, partners can relieve dangers and open the complete potential of advanced monetary forms. This paper contributes profitable experiences to the continuous discourse on cryptocurrency security and recommends roads for future inquire about in this energetic field.

1. Introduction:

Cryptocurrency, a troublesome constrain reshaping the monetary scene, has captured worldwide attention with guarantees of decentralization and borderless exchanges. However, in the midst of its brilliant rise, concerns over security linger expansive, undermining the solidness and dependability of advanced resources.

1.1 In this investigate endeavour, we set out on an in-depth examination into cryptocurrency security, pointing to dismember its complexities, distinguish vulnerabilities, and propose strong solutions.

1.2 At the centre of cryptocurrencies lies blockchain innovation, a decentralized record framework hailed for its straightforwardness and permanence.

1.3 Be that as it may, this exceptionally innovation is helpless to a heap of security dangers, counting 51% assaults, double-spending, and agreement component vulnerabilities.

1.4 Understanding these dangers is urgent to bracing the security of computerized currencies.

1.5 Moreover, the environment encompassing cryptocurrency capacity and trade stages is overflowing with dangers. From defenceless wallets to visit hacking occurrences focusing on trades, clients confront a horde of challenges in shielding their resources. It is basic to analyse these dangers comprehensively to plan viable security measures.

1.6 In reaction to these challenges, the cryptocurrency community has created different security best hones and grasped rising advances. Multi-signature wallets, cold capacity arrangements, and progressions in cryptographic strategies offer promising roads for upgrading security.

1.7 Additionally, the part of regulatory systems and industry measures cannot be downplayed in cultivating a secure and reliable environment for cryptocurrency transactions.

1.8 By diving into the subtleties of cryptocurrency security, this investigate looks for to contribute to the continuous discourse and propose significant techniques for bracing the keenness of advanced resources.

1.9 In doing so, we endeavour to clear the way for a more secure and resilient cryptocurrency ecosystem.

2. Technique to handle cryptocurrency :

As the scene of cryptocurrency security proceeds to advance, it is basic to investigate and propose inventive frameworks and procedures to moderate dangers and improve the security of computerized resources.

2.1 Decentralized Identity Management: Decentralized identity management frameworks leverage blockchain innovation to supply clients with secure and irrefutable computerized identities. By empowering people to control their character and individual information, these frameworks diminish the chance of personality robbery and unauthorized get to to cryptocurrency wallets. Actualizing decentralized character arrangements can improve the generally security pose of the cryptocurrency ecosystem.

2.2 Multi-Factor Verification (MFA): Multi-factor confirmation includes an extra layer of security to cryptocurrency accounts by requiring clients to supply different shapes of confirmation some time recently getting to their reserves. This may incorporate a combination of passwords, biometric information, equipment tokens, or one-time passcodes. MFA essentially decreases the chance of unauthorized account get to, even within the occasion of compromised credentials.

2.3 Immutable Audit Trails: Immutable audit trails use blockchain's unchanging nature to form straightforward and tamper-proof records of cryptocurrency exchanges. By keeping up an permanent record of all exchanges, clients can effortlessly track and confirm the development of reserves, upgrading straightforwardness and responsibility inside the cryptocurrency environment. Permanent review trails give a vital instrument for identifying and examining false activities.

2.4 Smart Contract Auditing Tools: Savvy contracts are self-executing contracts with the terms of the assertion specifically composed into code. In any case, vulnerabilities in shrewd contract code can lead to security breaches and money related misfortunes. Keen contract reviewing devices utilize mechanized examination procedures to distinguish potential vulnerabilities and security blemishes in shrewd contract code, permitting engineers to correct issues some time recently sending contracts on the blockchain.

2.5 Quantum-Resistant Cryptography: With the coming of quantum computing, conventional cryptographic calculations may gotten to be helpless to assaults. Quantum-resistant cryptography utilizes cryptographic primitives that are flexible to quantum assaults, guaranteeing the long-term security of cryptocurrency exchanges. By joining quantum-resistant cryptographic calculations into blockchain conventions and cryptocurrency wallets, the biological system can futureproof itself against developing threats.

2.6 These proposed frameworks and advances speak to fair a see into the assorted cluster of procedures accessible for upgrading cryptocurrency security. Proceeded investigate and development in this field are fundamental to remain ahead of advancing dangers and protect the astuteness of digital resources.

3. Introduction to Loyalty and Reward Points Programs

3.1 Dedication and Prize Focuses Projects (LRPs) act as a method for organizations and brands to connect with purchasers over and over, cultivating well established connections and empowering brand faithfulness. These projects boost purchasers to pick explicit items or administrations presented by a brand or gathering of brands over contenders.

3.2 Sorts of Faithfulness and Award Focuses Projects

LRPs come in two essential structures: single business programs and multi-business programs. Single business programs, similar to American Aircrafts' Benefit program or Starbucks Prizes, issue focuses straightforwardly from a similar business. Then again, multi-business programs, like LoyaltyOne's Air Miles or Compensation in Germany, include an outsider guarantor for focuses.

3.3 Measurements and Patterns in Dependability Program Participation

Studies show a huge pervasiveness of dependability program participation, with roughly 80% of Americans signed up for some type of remuneration program. The typical US family partakes in 29 dedication programs, and 71% of program individuals express receptiveness to joining extra projects. These figures reflect significant development in devotion enrollments over late years.

3.4 Contextual investigation: HotelBrand's Steadfastness Program Redesign

HotelBrand, a worldwide inn network confronting fierce opposition in the cordiality market, looks to redo its current dedication program to improve client centricity and recover piece of the pie. With roughly 30 million clients and 40 billion focuses available for use, HotelBrand expects to make a seriously captivating and versatile faithfulness program to meet developing purchaser needs.

3.5 Challenges in Redesiging Unwaveringness Projects

The update of reliability programs presents different difficulties, including framework overhauls, upgrading buyer experience, and overseeing expenses and time imperatives. High liquidity in exchanges requires powerful framework equipped for dealing with expanded exchange volumes and guaranteeing a consistent client experience across versatile applications.

3.6 Blockchain Answers for Dedication Projects

Blockchain innovation offers promising answers for tending to the difficulties looked by dedication programs. By utilizing blockchain, organizations can upgrade security, straightforwardness, and versatility in their steadfastness programs, along these lines working on generally speaking effectiveness and consumer loyalty.

3.7 Advantages of DigitalBits Blockchain for Faithfulness Projects

DigitalBits blockchain gives one of a kind benefits to dedication programs, offering minimal expense, versatile

arrangements with high exchange speeds. The stage's adaptability takes into consideration the making of tweaked unwaveringness programs customized to the particular requirements of brands like HotelBrand.

3.8 HotelBrand's Reception of DigitalBits Arrangement

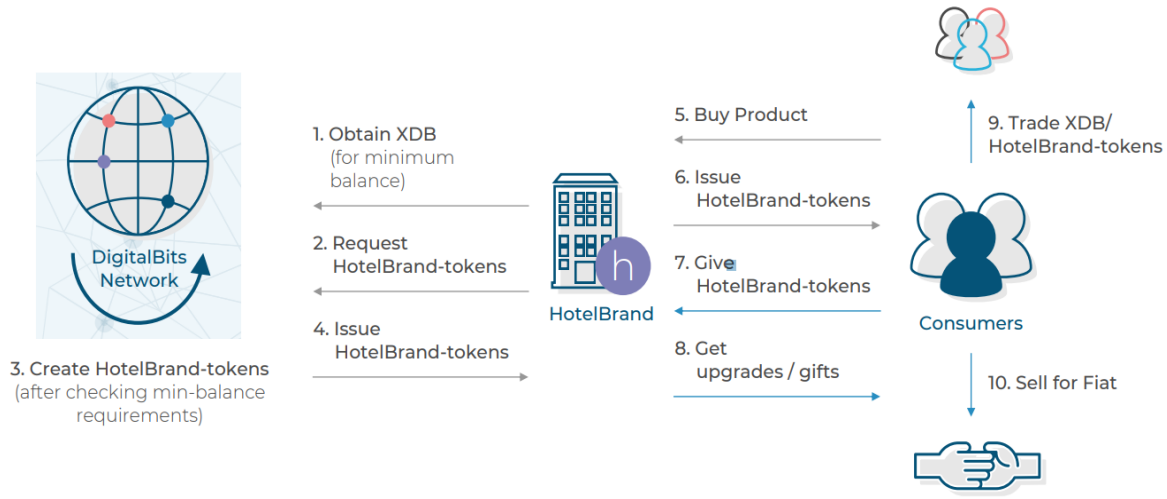
HotelBrand investigates the capability of DigitalBits blockchain to renew its steadfastness program. The stage's capacity to make brand-explicit tokens at negligible expense and its dynamic versatility make it an alluring answer for HotelBrand's worldwide activities.

3.9 HotelBrand-Tokens: A Contextual investigation

Using HotelBrand-Tokens on the DigitalBits organization, HotelBrand upgrades its devotion program, offering clients consistent prizes and motivations for their support. The contextual analysis outlines the down to earth execution and advantages of blockchain innovation in faithfulness programs.

3.10 Conclusion

The redesign of unwaveringness and prize focuses programs is fundamental for organizations like HotelBrand to stay cutthroat in the present market. By utilizing blockchain arrangements like DigitalBits, organizations can make more effective, client driven steadfastness programs that drive commitment and cultivate brand reliability.



(Fig. 1 Use- case of HotelBrand creating and using HotelBrand- Commemoratives on the DigitalBits network 1.) HotelBrand obtains the minimal XDB- commemoratives needed for participation in the DigitalBits network. 2.) produce HotelBrand- Commemoratives. 3.) HotelBrand- Commemoratives being created by DigitalBits network. 4.) HotelBrand- Commemoratives issued to HotelBrand; 5.) Consumer- Tom reserving a room offered by

HotelBrand. 6.) HotelBrand issuing the corresponding HotelBrand- Commemoratives;7.- 8.) ConsumerTom choosing to trade the commemoratives for a free room at HotelBrand. 9.) ConsumerTom choosing to trade some of her HotelBrand- Commemoratives or XDB- commemoratives with other consumers; and 10.) Consumer- Tom choosing to vend her HotelBrand- Commemoratives or XDB- commemoratives for edict currency or other cryptocurrency.)

4. Related Work

4.1 Understanding the existing challenges in creating and combining loyalty and rewards point (LRP) schemes is essential to addressing the problems with them. It is currently difficult to transfer or exchange points across other programs because the majority of LRP programs run independently within their individual systems. Customers who participate in numerous programs find this lack of interoperability inconvenient because it requires them to carry separate cards or download different apps on their devices.

4.2 Creating a single platform for LRP programs presents a number of difficulties, including those related to scalability, cost, and time. Because of the complexity and uniqueness of their current infrastructure, businesses encounter difficulties while merging their systems. Furthermore, concerns around security and the require for gifted staff assist complicate endeavors to open up LRP programs to more noteworthy interoperability.

4.3 By providing a decentralized platform for promoting the exchange and exchange of devotional foci, blockchain technology offers a possible solution to these problems. However, there are obstacles to existing blockchain-based arrangements, including Decentralized Apps (Dapps) created on Ethereum. These include high exchange fees, comparatively slow confirmation times, and the requirement for support for various local tokens.

4.4 Forks of Stellar, like as DigitalBits, present a possible alternative to traditional blockchain configurations. DigitalBits provides faster exchange speeds, lower fees, and support for creating bespoke tokens, addressing many of the shortcomings of Ethereum and other platforms. Its benefits, like multi-asset support and legitimate compliance, make it a compelling substitute for companies trying to enhance their LRP initiatives.

4.5 In summary, incorporating blockchain technology provides an effective solution to the problems facing LRP initiatives. Platforms such as DigitalBits provide the flexibility, efficiency, and adjustability needed to create a biological system that is more reliable and compatible.

(Table. 1)

	DigitalBits	Stellar	Ethereum
Blocktime (w/ Confirmations)	2-5s	2-5s	5m to 1h+
# of Confirmations	1	1	30
Processing Method	Validation	Validation	Confirmations via Mining / PoW
Transaction Costs	Very Low	Very Low	High
Multi-Asset	Built-in	Built-in	Custom App via Smart Contracts
Distributed Exchange	Built-in	Built-in	Custom App via Smart Contracts
Compliance Mechanism	Built-in via compliance server	Built-in	No
Inflation	No	Yes	Yes
Mining	Pre-mining	Pre-mining	PoW & PoS
Certified Token Issuer	Yes	No	No
TNCS	Yes	No	No
Automatic Algorithmic Native Token Distribution	Yes	No	Yes

5. Achieving Key Goals in Crypto security:

5.1 To analyse the vulnerabilities and security dangers inalienable in blockchain innovation and cryptocurrency ecosystems

5.2 To recognize and evaluate the dangers related with cryptocurrency capacity and trade stages, counting wallet vulnerabilities and hacking incidents.

5.3 To assess current security best hones and developing advances pointed at relieving cryptocurrency-related risks

5.4 To propose inventive frameworks and procedures for upgrading the security of advanced resources, such as decentralized personality administration, multi-factor confirmation, permanent review trails, savvy contract inspecting apparatuses, and quantum-resistant cryptography.

5.5 To examine the part of administrative systems and industry benchmarks in advancing cryptocurrency security and cultivating believe inside the ecosystem.

5.6 To contribute profitable experiences to the continuous discourse on cryptocurrency security and give noteworthy proposals for partners, counting engineers, speculators, controllers, and users.

5.7 To encourage information dispersal and awareness-raising exercises pointed at teaching users about the significance of cybersecurity within the setting of cryptocurrency transactions.

5.8 To investigate potential roads for future, investigate and advancement within the field of cryptocurrency security, tending to rising dangers and innovative headways.

Conclusion:

In conclusion, this term paper has given a comprehensive outline of cryptocurrency security, diving into the complexities of blockchain innovation, vulnerabilities in capacity and trade stages, current security best hones, rising innovations, administrative systems, and industry measures. Through our investigation, we have distinguished noteworthy challenges confronting the cryptocurrency environment and proposed inventive arrangements to improve the security and integrity of computerized assets. Cryptocurrency security may be a issue that requires a collaborative exertion from partners over different spaces. From designers and financial specialists to controllers and clients, each plays a pivotal part in cultivating a secure and trustworthy environment for cryptocurrency exchanges. By understanding the inherent dangers and actualizing strong security measures, partners can mitigate dangers and unlock the complete potential of advanced monetary forms. Moreover, proceeded investigate and development in ranges such as decentralized character administration, multi-factor confirmation, keen contract reviewing, and quantum-resistant cryptography will advance fortify the security pose of the cryptocurrency ecosystem. As the selection of cryptocurrencies proceeds to develop, so as well must our commitment to security and versatility. By tending to vulnerabilities, supporting for clear administrative systems, and grasping mechanical progressions, able to open the total potential of computerized monetary standards whereas defending the interface of all members. Together, ready to construct a future where cryptocurrencies serve as a trusted and secure medium of trade, driving advancement and financial strengthening on a worldwide scale. This conclusion summarizes the key findings and recommendations presented in the research paper, providing insights into the importance of cryptocurrency security and the steps needed to enhance it.

References:

- S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.
- S. Guler, Secure Bitcoin Wallet, Master’s Thesis, KTH, School of Information and Communication Technology, Stockholm, Sweden, 2015.
- S. Eskandari, D. Barrera, E. Stobert, J. Clark,” A First Look at the Usability of Bitcoin Key Management”, Internet Society, doi:10.14722/usec.2015.23015, 2015.
- O. Boireau, “Securing the blockchain against hackers”, Network Security, 2018(1), 8-11. doi:10.1016/S1353-4858(18)30006-0, 2018.
- T. Bamert, C. Decker, R. Wattenhofer, S. Welten, “BlueWallet: The secure Bitcoin wallet”, Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8743, 65–80, 2014.
- J. H. Mosakheil, “Security Threats Classification in Blockchains”, Culminating Projects in Information Assurance, 2018.
- Internet: A. Rosic, 5 high profile cryptocurrency hacks. https://blockgeeks.com/guides/cryptocurrency-hacks/, 2017.
- R. Juzenaite, “Security vulnerabilities of cryptocurrency exchanges”, Infosec Instittute, 2018.
- Internet: J. Kirk, Cryptocurrency exchanges lost 882 million to hackers. https://www.bankinfosecurity.com/ cryptocurrency-exchanges-lost-882-million-to-hackers-a-11624, October 2018.
- G. Karame, E. Androulaki, Bitcoin and blockchain security, Boston: Artech House, 2016.
- M. Conti, E. S. Kumar, C. Lal, S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin”, IEEE Communications Surveys & Tutorials, 20(4). doi: 10.1109/COMST.2018.2842460, 2018.
- M. Tanriverdi, M. Uysal, M. Üstündağ, “Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi”, Bilişim Teknolojileri Dergisi. 203-217. 10.17671/gazibtd.547122, 2019.
- Internet: J. Weiczner, Hackers Stole $50 Million in Cryptocurrency Using ‘Poison’ Google Ads. http://fortune.com, 14 February 2018.
- T. Volety, S. Saini, T. Mcghin, C. Z. Liu, K.-K. R. Choo, “Cracking Bitcoin wallets: I want what you have in the wallets”, Future Generation Computer Systems, 91, 136–143. doi: 10.1016/j.future.2018.08.029, 2019.
- R. Houben, A. Snyers, Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion, Brussels: European Parliament, 2018.
- Internet: Security: Threats, https://wiki.trezor.io/Security:Threats#Hacking_SatoshiLabs_servers.
- Internet: P. Marek, R. Pavol, V. Aaron, B. Sean, Mnemonic code for generating deterministic keys, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, 10 September 2013.
- A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypto-Currencies, California, USA: O'Reilly Media Inc., 2014.

- N. Courtois, P. Emirdag, F. Valsorda, "Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events", IACR Cryptology ePrint Archive, 2014, 848, 2014.
- Technical Committee ISO/IEC JTC 1 SC 27, ISO/IEC TR 15446:2017 Information technology - Security techniques - Guidance for the production of protection profiles and security targets, Geneva, Switzerland, 2017.
- M. Gregg, CISSP Exam Cram, Fourth Edition. USA: Pearson IT Certification, 29 August 2016.
- Common Criteria Development Board, Common Criteria for Information Technology Security Evaluation Part 1, 2017.
- E. Karataş, "Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System", Bilişim Teknolojileri Dergisi, 11(4), 399-406, DOI: 10.17671/gazibtd.452686, 2018.
- S. Y. Kang, J. H. Park, M. K. Khan, J. Kwak, "Study on the common criteria methodology for secure ubiquitous environment construction", Journal of Intelligent Manufacturing, 23(4), 933-939, 2009.
- S. P. Kaluvuri, M. Bezzi, Y. Roudier, "A Quantitative Analysis of Common Criteria Certification Practice", Trust, Privacy, and Security in Digital Business Lecture Notes in Computer Science, 132-143, 2014.
- Bundesamt für Sicherheit in der Informations technik (BSI), Guidelines for Developer Documentation according to Common Criteria Version 3.1., 2007.
- A. Bialas, "Ontology-Based Security Problem Definition and Solution for the Common Criteria Compliant Development Process", 2009 Fourth International Conference on Dependability of Computer Systems, 3-10. Brunow, Poland, 2009.
- Common Criteria Development Board, Common Criteria for Information Technology Security Evaluation Part 3, 2017.
- Bundesamt für Sicherheit in der Informations technik (BSI), Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, 2014.
- F. X. Standaert, "Introduction to side-channel attacks", Secure integrated circuits and systems, 27-42. Springer, 2010.
- R. Sachova, M. M. Marcos, S. H. Revetti, Security of Mobile Payments and Digital Wallets, European Union Agency for Network and Information Security, 2016.
- Trusted Computing Group, Protection Profile PC Client Specific TPM, 2014.
- A. Garba, Z. Guan, A. Li, Z. Chen, "Analysis of Man-In-The-Middle of Attack on Bitcoin Address", ICETE 2018, 388-395. 10.5220/0006864003880395, 2018.
- Full Drive Encryption International Technical Community, Collaborative Protection Profile for Full Drive Encrytion Authorization Acquisition, 1 February 2019.
- Internet: A. Rosic, Paper Wallet Guide: How to Protect Your Cryptocurrency, https://blockgeeks.com/guides/paper-wallet-guide/, 2017.

- C. H. Kateraas, Threats to Bitcoin Software, Master's Thesis, Norwegian University of Science and Technology Department of Computer and Information Science, 2014.
- Internet: L. King, Bitcoin Hit by Massive DDoS Attack as Tensions Rise. www.forbes.com, 12 February 2014.
- K. Fanning, D. P. Centers, "Blockchain and Its Coming Impact on Financial Services", J. Corp. Acct. Fin, 27(5), 53-57. doi:10.1002/jcaf.22179, 2016.
- D. Dasgupta, J. Shrein, K. D. Gupta, "A survey of blockchain from security perspective", Journal of Banking and Financial Technology, 10.1007/s42786-018-00002-6, 2019.