Grenze International Journal of Engineering and Technology, June Issue

Blockchain Dynamic Wallet Crash Recovery

Siddharth Raj K S[1] and Dr Kotadi Chinnaiah[2]
[1]Computer Science and Engineering, GHRCE, Affiliated to RTMNU, Nagpur, Maharashtra, India
Email: satyamengg21@gmail.com
[2]M.Tech, Ph.D., Asst. Professor, Department of CSE, GHRCE, Affiliated to RTMNU, Nagpur, Maharashtra, India
Email: kotadi.chinnaiah@raisoni.net

Abstract*— This paper is entitled to perform a fact-finding analysis on the Crypto Currency digital wallet data crash and dynamic recovery of the wallet transactions along with the data of exchange associated to it. The Crypto currency like Bitcoin (BTC) which is being listed on the Initial Coin Offerings (ICO) exchange contains wallet addresses that uniquely identifies a sender and a receiver of a transaction which is being broadcast over the Internet. Such broadcast data which is mined is recorded in the form of a chain of blocks called Blockchain. The Blockchain Technology is a tamper proof software which is developed in cryptography that does not allow to modify any private or public entity even though it is owned. The Crypto currency (BTC) which has been trading on the exchanges is impacted by some market influencing factors. Such that the exchange which has been in use since it's inception is being crashed majorly more than six times that had created tragic situations in the History. It influences the trade but reacts when huge fluctuations that occur due to market trends in FOREX trading directly or indirectly. Due to indirect provoking of the market which is clinching through the media analysis or by the intruder software programs that run or mobile applications that used to communicate rapidly through the social media like YouTube, X, Telegram and Facebook are the key applications that are playing a vital role. By the People of having an individual intention to get profit from alerting the minds of Capitalists, Investors, Customers, Merchants, and the common Public to sell out instantaneously to invoke a price drop on the Crypto currency market that could cause a major crash, Fig 1: shows sharp cuts in price drop that occurred in the History as well. Actually, the Blockchain is decentralized, unlike the other fiat currency shares listed on the IPO like SEBI, NASDAQ, and DOC are controlled centrally by the respective entities. But the public oriented markets don't have controls set up or no such pretending controls are incorporated. Unless the system's wallet is manually deleted or the wallet data file is corrupted due to some other reasons, it can be dynamically recovered and restored until the file is corrupted. Such recovery technique is called "Cold Storage" that keeps the private keys out of reach of hackers. This is often accomplished by keeping the private keys offline. The credentials that are necessary to spend bitcoins can be stored offline in several ways. So that before transferring an amount (BTC), it is essential to confirm the receiver's active wallet otherwise it won't return back. However the Blockchain security and futures are already regulated by the Exchange Regulatory Commissions. It is essential conduct regular audits to power up the present mechanism as the technological trends and demands are growing up rapidly despite the negotiable issues and renowned network conditions in place.

I. INTRODUCTION

This Cryptography was developed and designed in the Software Technology called Blockchain, which has been

Grenze ID: 01.GIJET.10.2.92_2

introduced and started trading in the year 2009 with the start of Bitcoin as a base crypto currency. The Blockchain wallet address was designed and developed from scratch with an idea of Block-By-Block “Mining” process and introduced to the world by Satoshi Nakamoto who is one of the great Japanese cryptocurrency inventors. The word Bitcoin was originally defined and value of it was determined in a published white paper on 31 October 2008. It’s a compound of the words Bit and Coin. Thus, the smallest unit of the Bitcoin is represented as 1 BTC = 100 million Satoshi.

The digital system of General Ledger accounting (GL) is as of the Financial Banking which is a Digital Ledger Technology (DLT), is in the form of Blocks connected over the Internet. The connected Block’s wallet address uniquely identifies an authorized owner which appended owner’s digital signature in the form of a message broadcast. The cryptography stores and preserves the created Block’s sender, receiver and transaction value with the time stamped digital signatures associated. As it has been growing rapidly from day-to-day trends of the Marketing and Trading needs of the people all over the world by creating a huge demand for services as well. It’s been a time-stamped decentralized series of fixed records that contains data of any size controlled by large notwork of computers.

The Transactions received are defined by using a specific scripting language called machine code that consists of one or more inputs and one or more outputs. When a user sends Bitcoins to a designated wallet address is an input and the amount of Bitcoins transferred over the network which displayed at the receiver’s end is an output.

There is no chance of double spending as an input of each transaction must refers to a previous unspent output of the transaction in the blockchain. The use of multiple inputs corresponds to the use of multiple coins in a digital transaction. Since these transactions can have multiple outputs as users can send the Bitcoins to multiple recipients in one transaction. Any input Satoshis not accounted for an output in the transaction outputs become the transaction fee. Though the transaction fees are optional the miners can choose which transactions to process and prioritize those that pay higher fees.

Miners may choose transactions based on the fee paid relative to their storage size, not the absolute amount of money paid as a fee. The fees are generally measured in Satoshis per Byte and the size of a transaction is dependent on the no of inputs used to create the transaction and the no of outputs.

The size of the Block in the Blockchain was originally limited to 32 Megabytes. But the size of the Block was ideally declared as 1 MB and was introduced to the world by Satoshi Nakamoto in 2010. Eventually, the limit of the Block size of 1 MB has created problems of increased transaction fees and delayed processing time of the transaction.

This Tamper Proof Technology called “Blockchain” introduced a digital Wallets system as Cards in the financial system or Banking sector for storing the transactional data of the blocks. The Blockchain does not allow anyone like owned parties or Governments to modify the recorded data. It means that it is almost impossible as it is ridiculously huge in size and getting approval from millions of data owners of the blocks to conduct a minor change. Even if it is a valid change, 51% of the stakeholders need to approve within the short span of time of execution. So, the technology itself it doesn’t allow anyone to modify, and hacking is exceedingly difficult as of now.

The digital Wallet software has been targeted by hackers because of the lucrative potential for stealing of Bitcoins. A software technique called "cold storage" keeps private keys out of reach of hackers; this is accomplished by keeping private keys offline at all times by generating them on a device that is not connected to the internet. The credentials necessary to spend bitcoins can be stored offline in several different ways, from specialized hardware wallets to simple paper printouts of the private key.

Now a days, due to availability of rapid communication mechanism, a tweet from the popular application X is also causing a damage to the Bitcoin trading. Exchanges like HitBTC, Bittrex, Bitfinex, Bitstamp, Crypto.com, Coinbase, Zebpay, Binance, OKCoin provide highly varying degrees of safety, security, privacy, and control over your funds and information. Perform due diligence and choose a wallet where to keep the Bitcoin before selecting an exchange. Sample Wallet Address is:

3PM9kfZdeq5D1Rm7tzAXEDdFbKdGETJ5SK

The "Hardware wallet" is a computer peripheral that signs transactions as requested by the user. These devices store private keys carry out signing and encryption internally, and do not share any sensitive information with the host computer except already signed (and thus unalterable) transactions. Because hardware wallets never expose their private keys, even computers that may be compromised by malware do not have a vector to access or steal them. The user sets a passcode when setting up a hardware wallet. As hardware wallets are tamper-resistant, the passcode will be needed.

- **FACT FINDING ANALYSIS ON THE CRYPTO TRADING**

A. Is this happening due to Big Stakeholders BTC or Traders who hold a nod of trade game in a short period?

No. For instance, if the situation demanded by the speculation of the media or free publicity of the people involved then the size of the crash would be heavier. Later it can be analyzed when a sharp curve drawn by the fluctuation occurred. Though it is not directly proportional to the loss of that issue, it influences much more. As such, it is a bit difficult to analyze the facts and figures and the members involved. It is difficult to express the actual size of the crash that occurred by the no of people involved. The traders need to pay active attention to react quickly to the price drop.

B. What should be done when Bitcoin is crashing?

The market situation can mislead when you trade proactively so that be cool for a while to find the reach of it. Such that the statistics on the market trends can guide you in deciding to move forward. More speculations by the media can cause you more damage to the crypto market and your funds indirectly.

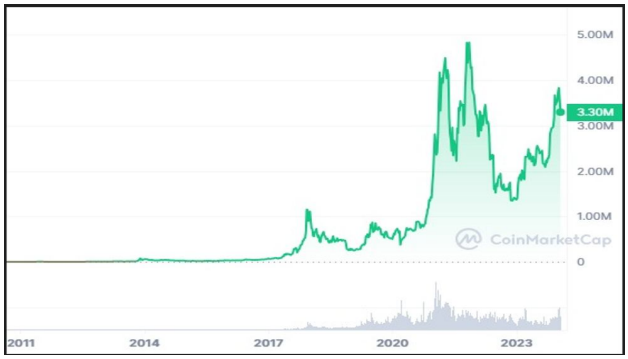

Fig. 1Bitcoin Crash History - Bitcoin to INR Chart- Recent Trends Analysis Map

C. Block Mining and Security

The block is secured, and each block relates to each other by the SHA256 Hashing Mechanism of 64-bit Cryptographic Code which protects it from tampering by an unauthorized person. It means that each block contains details of the registered owner of the Block. Every block will contain its own Hash and the Hash of the previous function so that it cannot get tampered with. This fingerprinting will use the chain of the blocks together.

II. LITERATURE SURVEY

In the recent past, the Bitcoin significant price tumbled several times and crashes experienced, the most notable being in the years 2017-2018 and 2021-22 Bitcoin bubble. This was a time when the Bitcoin price skyrocketed to nearly $20,000 in December 2017 and $64,000 in November 2021, crashed and the price fell to $3000 and $19,000 correspondingly in the subsequent years. It is impossible to know for sure what will happen to Bitcoin's price in 2023, important to remember that market cycles are a natural part of any asset's growth and decline. Market influencing factors like increased regulatory scrutiny, changes in investor's sentiment, and increased competition within the cryptocurrencies is all potentially impact Bitcoin's price in the future. It's worth noticing that Bitcoin has shown resilience in the face of market volatility in the recent times.

A. When the Crypto crash reported initially

In June 2011, The first major crisis occurred for Mt.Gox few months after Karpele took over. Mt.Gox claimed that the compromised user account exploited to make the price of Bitcoin fall from $17 to just cents in a couple of minutes, reported in ARS technical. This crash was exclusive for the Mt.Gox when the hack didn't affect the underlying Bitcoin Protocol. Another report published that 25,000 coins were presumed missing or stolen from 478 different user accounts of BTC. These coins valued at over $8.5 million at the time. Then, Mt.Gox admins took the exchange offline while they tried to rectify the situation.

B. Recent Big Crypto crashes reported

It noticed that the year 2022 has been the landmark for the big crypto crash reported that the people know. A historic bull run started within the same year, but the fanfare cut short while the price drop started sharply. The

protocols like Terra buckled and dropped sharply under the pressure. What followed a cascading ripple through the entire industry that took down hedge funds, lenders, and countless protocols. As of the fall of 2022, the second crypto winter (the first is being in 2018) has been started by the prices and are still languishing near the bottom of the market. Only time will decide whether these prices are indeed with the market bottom for this cycle or if investors are in for more carnage over the coming months.

No doubt. The top casualty of the year 2022 sell-off has been the Terra Protocol. One crypto stable-coin is Terra's UST, maintained for years until it crashed in early May 2022. The BCC token crashed from an all-time high of $509 to just over $8 in a month. Billions of dollars wiped out in the blink of an eye, and Bit-connect ended up the but of the internet memes and jokes as the fraud was exposed.

The legality of bitcoin varies by region. Some governments have used Bitcoin in some capacity. Bitcoin has described as an economic bubble by a couple of recipients of the Nobel Memorial Prize quorum in Economic Sciences.

TABLE I BIGGEST CRYPTO CRASHES RECORDED IN HISTORY

Cryptocurrency	Date	Starting Price	Ending Price	Cause
Bitcoin (whole market)	Nov 2021 - June 2022	$69,044	$19,047	Sell off
Bitcoin (whole market)	Dec 2017 - Feb 2018	$19,665	$6,852	Sell off
$LUNA	May 2022	$116	$0.0001	UST deeper
Bitcoin	Feb 2014	$1,127	$360	Mt.Gox Hack
$BCC	January 2018	$509	$8	Bitconnect Shutdown
FTT (FTX token)	November 2022	$22	$0.87	Balance sheet leak

[a.] April 29, 2023 Upgrade Carried.

The environmental impact of Bitcoin is significant as the Proof-of-work algorithm for Bitcoin mining designed to be computationally difficult to hack it, which requires the consumption of increasing quantities of electricity, generation of which has contributed to climate change.

III. DESIGN, MODELLING, AND IMPLEMENTATION

The Bitcoin nodes are growing up and roaming around the world. It may be due to crashing or intentional shutdowns and start-ups. Entirely, Bitcoin exchange supports with the usual transitions. It doesn't crash even though it connected to a node that goes down, even though it goes down until it will connect to another fail-over node. The BitcoinD program which has designed is connected to BitcoinD nodes so that if one or several nodes are shut-down, the BitcoinD does not lose its connection to the broadcast internet. Also, it will find new peers in the area to get connected so that the Peer-to-Peer node connectivity is resilient to node crashes and other disruptions.

The Data encryption of SHA256 algorithm-based hash code represents the Hexadecimal code of 64-bit data is a Record-Keeping service as part of Cryptography. It has gone through the system processing power. The Miners often keep the Blockchain consistent, committed, complete, and unalterable by newly grouping broadcast transactions into a block that then broadcast to the Internet. Such mined block verified by recipient nodes that each block contains the SHA256 cryptographic hash code of the previous block, then attached to the blockchain node by the digital signature. To be accepted by the rest of the nodes of the broadcast network, the block mines a new block that must contain a proof-of-work(PoW). Usually, the PoW requires a group of miners to find a number called a nonce. So that when the block content hashed along with the nonce. Numerically, the result is smaller than the network's difficult target.

A typical SHA256 algorithm hash as the block hashes have many leading zeros.

Following is an example of Block Hash Code:

0000000000000000000590fc0f3eba193a278534220b2b37e9849e1a870ca369

A. What the Regulatory Commissions should do?

The Securities Exchange Commission, and CBDC doesn't have the regulations existing in the International Organization of Securities Commissions as it has issued a proper set of rules to prevent exaggerations over the crypt trading of funds and immediate price drop by market unusual speculations.

IV. Results And Conclusion

It can be achieved with prior planning on statistics and functional Cryptocurrency dependency analysis on all the investment strategies. Let's read the tendency of investors and create some automated trading strategies with a strong focus on risk management in it is considered crashes. It's known that the investment strategy is a trend-following system. It may be slow as it considered max 30 trades a year that out performs the market. As a result, speculates a hype that could cause the damage to the trading profit of funds such that "Don't be proactive and Don't be panic" at all times. Even then, it is necessary to put some essential controls on the impacted or proactive media to avoid making panic news regularly. At run time, there might be a chance of crash due to incomplete transaction commits during the execution. Due to that, before transferring an amount (BTC), it is essential to confirm the receiver's active wallet address, otherwise it won't be return. If the transaction crash occurs due to network failure with the wallet, then it has to be followed to restore with the Wallet.DAT file found on the system immediate effect. If it is not, then go by the set of rules of the exchange to get the data file or security pass phrase code of 12 pass phrase whichever process used and restore it manually to get it done, for which the public and private keys are essential.

The ability to spend funds from a wallet comes from the cryptographic keys stored in the Wallet.DAT data file. Without those keys associated with the wallet, the Bitcoin client software doesn't support spending the funds from the wallet.

There have been no Trojans or other malware that specifically have targeted the Bitcoin wallet just yet, but many believe such a situation will likely occur.

An algorithm designed to recover the crypto market from a price tumbling situation or huge crash. The more severe the crash, the longer it will wait before trading again after the crash:

A. Algorithm

a) Read the Tendency of the market.
b) Go ahead with the positive intent of promotions to attract and do a remediation process to keep the nod.
c) Stay calm and Let them decide to sell or see a dip as an opportunity to buy more, and needed to act accordingly.
d) Assess the situation of the market repeatedly.
e) Remember that volatility is a play of the game.
f) Evaluate the scope with statistical analysis.
g) Evaluate it and determine how to act in the future accordingly
h) Change of guard needs time to control, instead.

It's for sure that there is No Chance of the Cryptocurrency BTC down to zero as the awareness in the traders gradually increased since then. Due to the Bitcoin system continues to run forever, there is a need of at least one computer node running the Bitcoin client program, the BitcoinD executable, which is also a server, a daemon process) that mined (creating new blocks). In general, there are many thousands of active nodes running.

Future Scope

The significance of the SEC's ruling on Ethereum (ETH) classification extends beyond the cryptocurrency market. The SEC ruling holds significant importance of the regulations and use of blockchain technology. The SEC ruling on Ethereum may influence regulation of other cryptocurrencies in the future.

Cloud computing generally deals with a large amount of data, as a result of which data maintenance could be difficult. So that there may be a risk of data security in the entire system of a fail-over technology service. There could be a chance of collapse if no backup of data maintained instantly. Lost data can't be recovered in any system whenever the fail-over system is not maintained to meet the requirements. Mainly Cloud Computing, Artificial Intelligence, Machine Learning, Data Science, and Deep learning are the scope of development in Blockchain Technology that could then grow to overcome the existing pitfalls and could handle the Robotics in providing the excellent services.

Acknowledgments

We would like to thank the editors (IEEE) and all the anonymous reviewers for your helpful comments and suggestions for this paper.

REFERENCES

[1] "Unicode 10.0.0". Unicode Consortium. 20 June 2017. Archived from the original on 20 June 2017. Retrieved 20 June 2017.
[2] "Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency". Daily Tech. Archived from the original on 20 January 2013. Retrieved 30 September 2012.
[3] Nakamoto, Satoshi (31 October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org. Archived (PDF) from the original on 20 March 2014. Retrieved 28 April 2014.
[4] "Bitcoin Core 23.0". Retrieved 31 May 2022. "Statement of Jennifer Shasky Calvary, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy" fincen.gov.
[5] Financial Crimes Enforcement Network. 19 November 2013. Archived from the original on 9 October 2016. Retrieved 1 June 2014.
[6] Dissecting the performance of chained-BFT. 1 March 2021, Fangyu Gai, Ali Farahbakhsh, Jianyu Niu, Chen Feng, Ivan Beschastnikh, Hao Duan
[7] "Bitcoin source code – amount constraints". GitHub. Archived from the original on 1 July 2018.
[8] Antonopoulos, Andreas M. (2014). Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media. ISBN 978-1-4493-7404-4.
[9] "El Salvador's dangerous gamble on bitcoin". The editorial board. Financial Times. 7 September 2021. Retrieved 7 September 2021. On Tuesday, the small Central American nation became the first in the world to adopt bitcoin as an official currency.
[10] "Central bank digital currencies" (PDF). BIS. March 2018. Retrieved 21 January 2023.
[11] "Bitcoin Declared Legal Currency in Central African Republic". Bloomberg.com. 28 April 2022. Retrieved 28 April 2022.
[12] "Who is Satoshi Nakamoto?". The Economist. The Economist Newspaper Limited. Archived from the original on 21 August 2016. Retrieved 23 September 2016.
[13] Davis, Joshua (10 October 2011). "The Crypto-Currency: Bitcoin and its mysterious inventor". The New Yorker. Archived from the original on 1 November 2014. Retrieved 31 October 2014.
[14] Vigna, Paul; Casey, Michael J. (2015). The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order (1 ed.). New York: St. Martin's Press. ISBN 978-1-250-06563-6.
[15] "Bitcoin". OxfordDictionaries.com. Archived from the original on 2 January 2015. Retrieved 28 December 2014.
[16] Joshua A. Kroll; Ian C. Davey; Edward W. Felten (11–12 June 2013). "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries" (PDF). The Twelfth Workshop on the Economics of Information Security (WEIS 2013). Archived (PDF) from the original on 9 May 2016. Retrieved 26 April 2016. A transaction fee is like a tip or gratuity left for the miner."
[17] Wolff-Mann, Ethan (27 April 2018). "'Only good for drug dealers': More Nobel prize winners snub bitcoin". Yahoo Finance. Archived from the original on 12 June 2018. Retrieved 7 June 2018.
[18] Orcutt, Mike (19 May 2015). "Leaderless Bitcoin Struggles to Make Its Most Crucial Decision". MIT Technology Review. Archived from the original on 18 October 2017. Retrieved 22 June 2017.
[19] Rainer Bohme; Nicolas Christin; Benjamin Edelman; Tyler Moore (2015). "Bitcoin: Economics, Technology, and Governance". Journal of Economic Perspectives. 29 (2): 213–238.
[20] Krause, Elliott (5 July 2018). "A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help". The Wall Street Journal. Archived from the original on 9 July 2018. Retrieved 8 July 2018.
[21] Simonite, Tom (5 September 2013). "Mapping the Bitcoin Economy Could Reveal Users' Identities". MIT Technology Review. Retrieved 2 April 2014.
[22] McMillan, Robert (6 June 2013). "How Bitcoin lets you spy on careless companies". Wired UK. Conde Nast. Archived from the original on 9 February 2014. Retrieved 3 April 2020.
[23] Gervais, Arthur; O. Karame, Ghassan; Gruber, Damian; Capkun, Srdjan. "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients" (PDF). Archived (PDF) from the original on 5 October 2016. Retrieved 3 September 2016.
[24] "MtGox gives bankruptcy details". bbc.com. BBC. 4 March 2014. Archived from the original on 12 March 2014. Retrieved 13 March 2014.
[25] Jeffries, Adrianne (19 December 2013). "How to steal Bitcoin in three easy steps". The Verge. Archived from the original on 27 July 2019. Retrieved 17 January 2014.
[26] Arapinis, Myrto; Gkaniatsou, Adriana; Karakostas, Dimitris; Kiayias, Aggelos (2019). A Formal Treatment of Hardware Wallets (PDF) (Technical report). University of Edinburgh, IOHK.
[27] Sparkes, Matthew (28 September 2022). "Bitcoin has emitted 200 million tonnes of CO2 since its launch". New Scientist. Retrieved 23 October 2022.
[28] "Bitcoin prices remain below $600 amid bearish chart signals". nasdaq.com. August 2014. Archived from the original on 14 October 2014. Retrieved 31 October 2014.
[29] Biggs, John (8 April 2013). "How To Mine Bitcoins". Techcrunch. Archived from the original on 6 July 2017.
[30] "Bitcoin Developer Examples". Bitcoin. Retrieved 21 October 2018.

[31] "MIT Announces $900,000 Bitcoin Developer Fund". Inc. 29 March 2016. Retrieved 21 October 2018.
[32] "Bitcoin Core devtools README – Create and verify timestamps of merge commits". GitHub. Retrieved 5 May 2018.
[33] "Bitcoin Core devtools README – Create and verify timestamps of merge commits". GitHub. Retrieved 5 May 2018.
[34] Tasca, Paolo (7 September 2015), Digital Currencies: Principles, Trends, Opportunities, and Risks, Social Science Research Network, SSRN 2657598.
[35] "Regulation of Cryptocurrency Around the World" (PDF). Library of Congress. The Law Library of Congress, Global Legal Research Center. June 2018. pp. 4–5. Archived (PDF) from the original on 14 August 2018. Retrieved 15 August 2018.
[36] Clinch, Matt (22 October 2015). "Bitcoin now tax-free in Europe after court ruling". CNBC. Retrieved 16 August 2022.
[37] X. Ji et al., "Overview of 5G security technology", Sci. China Inf. Sci., vol. 61, no. 8, pp. 081301:1–081301:25, 2018.
[38] “Fast B4B: Fast BFT for Blockchains (“Patent Pending”), Mohammed M Jalalzai, Chen Feng, Victoria Lemieux from The University of Columbia, arXiv:2109.14604v2 [cs DC] 11 Oct 2021.
[39] M. J. Fischer, N. A. Lynch, and M. S. Paterson, “Impossibility of distributed consensus with one faulty process,” J. ACM, vol. 32, no. 2, pp. 374– 382, Apr. 1985.
[40] “Fintech and ECommerce” Article published on March 14,2019, Mathew Beedham.
[41] “A History of Crypto Crashes”, George Hristov, Editor Shannon Ullman, Published on March 6, 2023.