Bitcoin security - Anti-Dust Attack

Ajin S
Master of Computer Application
Amal Jyothi College of Engineering koovapally,
Kottayam, India
ajins2022@mca.ajce.in

Ajith GS
Master of Computer Application
Amal Jyothi College of Engineering
koovapally, Kottayam, India
gsajith@amaljyothi.ac.in

***Abstract*— Bitcoin is a sophisticated decentralized payment method that preserves all compact data in a populace ledger linked to the blockchain. Many different attacks have targeted Blockchain applications like Cryptocurrency, primarily Bitcoin cryptocurrency, including double-spending, Distributed denial-of-service (DDOS), and Dust attack. The given system is against dust attacks is described in this work. It protects Bitcoin availability and pseudo-invisibility against attackers who deliver all transactions in order to consider the data and link transactions to a specific user. The suggested system alerts users to these types of illicit transactions and provides them the option of accepting or rejecting them.**

***Keywords*- Bitcoin; Blockchain; Cryptocurrency; Dust Attack Privacy; Security; Threats.**

I. INTRODUCTION

Blockchain is becoming another most important industries for both individuals and businesses. Various sectors are showing a lot of interest in this technology. It is mostly used in cryptocurrencies as it redefines the concept of blockchain trust; In order to relying on a third party to complete the transaction, the two parties now have to rely on each other. The adoption of cryptocurrency systems, particularly Bitcoins, has risen as a result of the advancement of this technology. However, blockchain-based cryptocurrencies, like bitcoins, have security vulnerabilities that will be the focus of this article.

Problem Statement

There are still certain security concerns as blockchain and its applications continue to proliferate. The innovative nature of blockchain's decentralization and self-organization, on the other hand, has already resulted in security issues. Many cyber-threats, such as DDOS, Double- Spending, and Dusting assault, have lately targeted Bitcoin cryptocurrency. In this paper, we will show how to prevent the Dust assault, which is one of the most dangerous attacks against the Bitcoin system. When attackers try to attack the fake uniquely the user, which is the most crucial feature of Bitcoin cryptocurrency, it is known as a dust attack. Dust transactions use a small number of transactions transferred to millions of addresses in the system. Since a bitcoin wallet can have multiple addresses, the cyber attacker will perform a similar analysis to try to link them all to the same wallet, with the aim of revealing the identity of the owner.

The main donation are summarized as follows:

- The given DUST-MASK, system is a Bitcoin security system against dusting attacks.
- This given system (DUST-MASK), secures Bitcoin against dusting attacks by finding the smallest number of transactions being sent and protecting the opportunity by adding an approval flow, which will give the user the choice to accept or reject any transactions.

The given system (DUST-MASK) secures the user by giving awareness of those kinds of threats, and random transactions.

Finally, the suggested approach (DUST-MASK) aims to safeguard Bitcoin's pseudo-anonymity from attackers that transmit dust transactions in the hopes of analyzing the information and revealing the user's uniqueness. The remainder of the paper is laid out as follows: The second half begins with a review of some comparable past works. Second, part 3 will cover what blockchain technology is, as well as blockchain applications and the Bitcoin system, as well as numerous Bitcoin attacks. After that, in part 4, the adversary model will be explained, including dust attack and Bitcoin gaps. Then, in Section 5, we'll go over our given DUST-MASK and its drawbacks. Finally, the research will be completed, with no further work required.

II. LITERATURE REVIEW

The paper introduces blockchain as a novel technology and discusses its security concerns. The blockchain has created a new mode of interacting in which a trusted third party is no longer required to convey information between two parties. Data in a blockchain system is divided into numerous connected blocks, which improves database security. Data will be encrypted using the user's private key before being stored in a block, and the key will be encrypted to be second-hand as an identification for the user to secure anonymity. Moreover, several restrictions in blockchain may compromise the security of the device. Because of the small block size, it's subject to DDOS assaults, and because there's no third-party intricate, if a user drops his unique key, there's no other way to recover it.

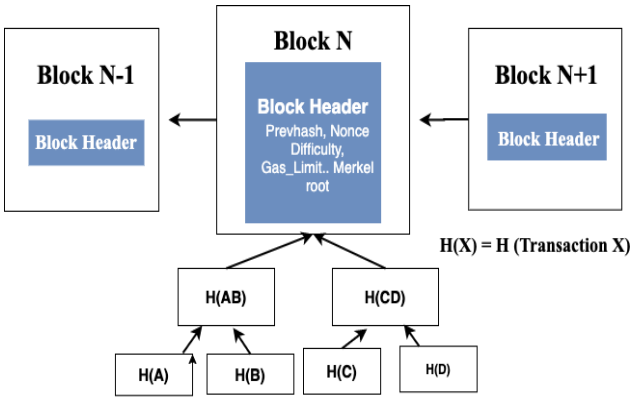
The developer barred the different types of assaults attacking Bitcoin, where different cyber attacks are used to learn about the identities of individuals at the back of it. Furthermore, not all bitcoin attacks covertness; some also destinated availability. Attacks against bitcoin availability include DDOS, Eclipse, Block Withholding Attack, and Double Spending Attack. It's when an attacker uses Block Withholding techniques to try to gain additional bitcoins by attacking the bitcoin network's pools. Last but not least, the author

DOI: 10.5281/zenodo.6383689
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

presented a method for preventing and defending against such attacks on the Bitcoin cryptocurrency.

The Anti-Dust schema was created by the author in order to avert dust assaults on cryptocurrency. The proposed system breaks the transactions into two different parts: a primary activity pool and a dust transaction pool; once a transaction is comprehensible as a dust attack, it will be dropped. The transaction will be forwarded to the dust, and once the transaction pool is full, it will be damaged. Which aimed to experiment, which allowed a maximum acceptance time of 215 sec for all different transactions.

By providing a systematic investigation on the transaction graph, the research contended whether cryptocurrency users are concerned with the pseudo-uniqueness feature are provided by the cryptocurrency system or not, and in order to convey whether a blockchain user is distressed with the pseudo-uniqueness, the author popularized three metrics, The first will link the



Different aspect of uniqueness care with prevalence's, the second will find that the location is distressed about uniqueness if it reaches zero equity, and the next will be concerned with an address's aim, with an address being few concerned if it hides its purpose or which organization it belongs to. In order to admits the collective uniqueness concerned with the trend of all Bitcoin addresses, in here the researcher used macroscope analysis on Bitcoin transactions. The macroscope analysis detected that most of the addresses accentuate Bitcoin's simplicity while ignoring uniqueness problems, as well as bitcoin buyer and miner addresses that do not care about uniqueness because of their aim. Finally, the report found that the amount of cryptocurrency, such as its amount, finds it whether or not cryptocurrency users are distressed about uniqueness.

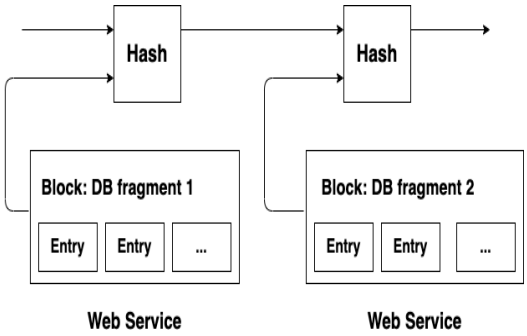


Figure 1: How Blockchain

works Blockchain Applications

Apart from the traditional method of creating a presentation layer and maintaining data in multiple data centers, blockchain will make it clear because every user will be able to create managed information and maintain a copy of it in many different blocks. Blockchain commence with cryptocurrencies, advanced through the domains of assets and credit, and finally identify its way into the area of data and communication. With the rapid growth of blockchain technology, many businesses are consent technological supremacy, thanks to one of the most important applications.

Bitcoin System

Bitcoin is a practical arrangement and decentralized digital cash that many authentic groups, such as governments and banking sectors, use to the deportation of transactions between two clients. The holder of bitcoin can allocate it at any time and anywhere without the need for a credible third party, and no one can regulate bitcoin because it is an open decentralized system.

Blockchain

It is a user to user network that provides error-tolerance qualities. Blockchain can be defined as a data store, transmission. It provides a decent movement of data in a decentralized aspect, without the need for any trusted third-party. It was first Introduced in 2008 to help create the cryptocurrency system. In 2010, it was accomplished that the blockchain technology is much more than just a tool for storing cryptocurrency.

III. BACKGROUND

DOI: 10.5281/zenodo.6383689
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

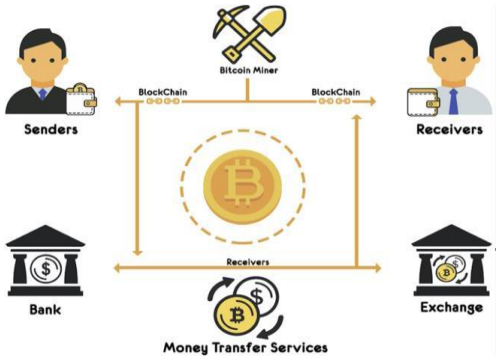


Figure 2: Blockchain Structure [6]

In Bitcoin users are briskly increasing over time, the Bitcoin technology became a destination of digital "bank-heists", they use whatever attack they could act in order to abduct the money.

Different Attacks on the Bitcoin System

Today, many online threats have been targeted at Bitcoin cryptocurrency. DDOS is one of the biggest attacks targeted in the Bitcoin; when attackers try to choke and shut down a network which makes its service disruptive for authentic customers by sending multiple requests to the server leading to serious threats that cannot be fully recovered. In addition, Sybil attacks, as malicious users targeted network, when a computer is hijacked to challenge multiple ownership of a network expected to control most of the computer's network usage, and with multiple ownership, the attacker can use it to continue cataclysmic activities by changing transactions or preventing transactions. and repetition; which can lead to a double

wasting problem. A double-off attack is when attackers spend an equal amount of Bitcoin on a variety of different transactions.

IV. ADVERSARY MODEL

A. Dust Attack

Dust attacks can be described as malicious behavior directed at cryptocurrency users and the secrecy of bitcoins by sending small part of coins to their wallets. As small amounts will be abandoned, the purpose of the Dust Attacker in this process is to admits user identity, this is done by collecting the data there, these small numbers - in different blocks - will be cooperated when the user creates something new.

The transactional process of these funds is pursued by the invaders by means of linking the expired addresses and the method of these funds try to existence the person behind it. After the cryptanalyst admits the existence of the person who get attacked, he starts the action of filing (pay for this bitcoins number or It will confess your identity).

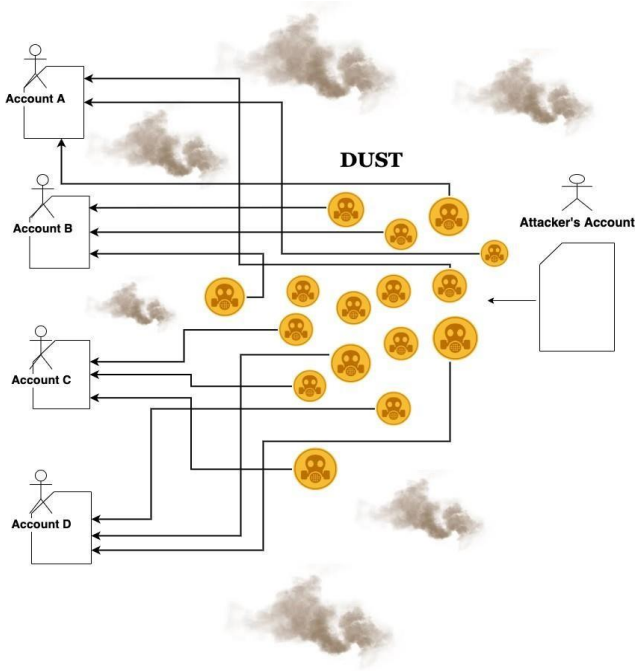


Figure 4: Dust Attack Diagram

B. Bitcoin system spaces

In the Bitcoin, users connected to the network get to see all transactions created by a user disclosed by the centralized blockchain, but privacy is protected because of how the bitcoin protects user uniqueness. However, you can still link other processes to any user due to different input functions that will verify that the function is performed by the same owner, and once the user key is announced, it will be able to display a few more functions in relation. to the same user.

I. PROPOSED METHODOLOGY

The method given in this research is used to give more security to Bitcoin programs from Dusting attacks. As it address to tamper with a fake user name by trying to identify user identity and affect availability by sending multiple dust jobs to the user. The new method is designed with the intention of protecting the system's high-risk malicious malware and access to the algorithm that will not upset the system efficiency

DOI: 10.5281/zenodo.6383689
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

Methodology & Design

1) Given secure bitcoin against dusting attack

The program will add an authorization algorithm on the user perspective; where any contract of more than 4 Satoshi's (where Satoshi is the bitcoin name) will delivered through the authorization stream, users have the right to accept or reject any Satoshi's amount from any unforeseen user. Activity less than 4.1 Satoshi's will be immediately rejected (see Figure 5). The number 4 was selected based on a number of studies conducted, in which they found that the amount - 4 or below is considered the minimum value in cryptocurrency systems.

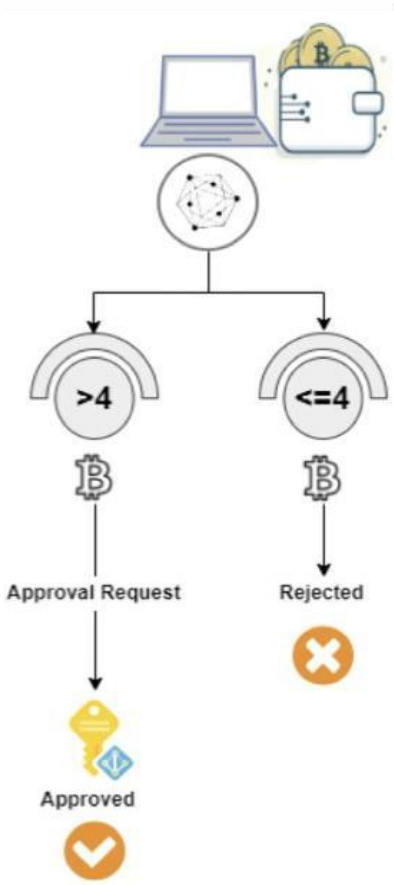


Figure 5: Proposed System Diagram

2) Suggested algorithm for bitcoin's security Improvement

The algorithm is developed to increase the guarantee of the Bitcoin. The provided algorithm speculates the value of the transaction as input into the following schemes; if the contract is less than or equal to Satoshi's, it will be dropped. Otherwise, the transaction will be favored, and the user will have the option to approve or reject the cryptocurrency transaction. The first component will conserves the system fr[illegible] and the authorizati[illegible] DDOS attacks (se

Algorithm 1 DUST-MASK System

```
Procedure Bitcoin(X)
    X ⟵ Transaction amount
    if X <= 4 Then
        RejectTransaction (X)
        DropTransaction (X)
        0 ⟵ X
    Else
        Approve Transaction (X)
    End if
End Procedure
```

Algorithm	Anti-Dust schema	DUST-MASK
Scheme	Protect user's pseudonymity from dust by evaluating the transacted amount: • if less than 1 satoshi decline • if more than 1 satoshi accept the transaction	As 1 to 4 Satoshi is considered a tiny amount it will not prevent attackers from doing such attack • Protect user's pseudonymity from dust by evaluating the transacted amount if less than or equal to 4 satoshi it will be declined • If more than 4 satoshi pass by the acceptance algorithm
Security Requirements achieved	Confidentiality	Confidentiality Availability

DOI: 10.5281/zenodo.6383689
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

VII. CONCLUSION

The paper conferred in this research is conducted to secure the cryptocurrency from Dusting attacks; aimed at disrupting the anonymous Bitcoin. Initially, cryptocurrency and blockchain technologies were introduced. In addition to explaining the Dust attack and its brunt on Bitcoin, which is one of the most widely accepted cryptocurrencies. Then we upgrade the Dust-mask system where we limit the number of works sent to users. The given method is given using two methods, a matched drawing, and a false code. The Dust-Mask system was designed to secure the system's access to DDOS service attack by blocking Dust sales on different accounts. In addition, adding multiple verification preference to accomplish more security.

VIII. FUTURE WORK

The proposed approach will be upgraded to have an additional Defense layer. In addition, the DUST-MASK algorithm provided for this paper will use duplicate authentication in such a way that the system will be more secure and efficient for the end-user.

IX. REFERENCES

[1] Andryukhin, A. (2019). Phishing Attacks and Preventions in Blockchain-Based Projects. 2019 International Conference on Engineering Technologies and Computer Science (EnT).

[2] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. 2017 4th International Conference on Systems and Informatics (ICSAI).

[3] Dusting Attacks Explained. (2019). Retrieved from https://youtu.be/_dPkAxRwvew

[11] Wang, Y., Yang, J., Li, T., Zhu, F., & Zhou, X. (2018). Anti-Dust: A Method for Identifying and Preventing Blockchain's Dust Attacks. 2018 International Conference on Information Systems and Computer-Aided Education (ICISCAE).

DOI: 10.5281/zenodo.6383689
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam