JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BITCOIN WALLET: A PERFECT COMBINATION WITH BLOCKCHAIN AND SECURITY

Ms. Sayali Parab
Department of Information Technology
SES's L. S. Raheja College of Arts & Commerce
Mumbai, India

Mr. Chayan Bhattacharjee
Department of Information Technology
Chikitsak Samuha's Patkar Varde College
Mumbai, India

Abstract

E-wallets become a traditional method of banking these days since we have entered the age of digital banking, with which we can see several security loopholes specific to payment gateways, where the hackers steal the money from credit or debit cards by diverting the OTP to themselves. Traditionally, a Bank is a financial institution that receives deposits and grants loans to its stakeholders. Finance is a stream of banking that involves settlement and controls the withdrawals and deposits. When a currency in the form of cash is deposited into a bank, it is taken care of by the finance process. We mainly focus on answering the most Bitcoin queries including privacy and double-spending. Furthermore, as blockchain has potential applications far beyond bitcoin, we draw future insights where applications based on blockchain are provisioned in the market in order to be totally or partially independent of the centralized systems and we provide a questionnaire helping organizations for better using the blockchain feasibilities.

Keywords: *Blockchain, Cryptocurrency, Crypto-wallet, Bitcoin, Bitcoin wallet, E-wallet, Banking*

I. Introduction

The blockchain is one of the most talked-about topics in the corporate and academic world. A Distributed and network-based technology "Blockchain" is a place in which information is stored in a Digital form in a Shared Distributed Database. The word Blockchain means the storage of data into digital blocks and forms a chain so that every time a new record is added to a block it becomes a part of an existing chain. In order to keep a record, blockchain uses a ledger-based system such that all the transactions are recorded onto it and it is accessible by everyone making it a public ledger. Cryptocurrency is one of the key reasons this technology has become really famous. Bitcoin is the first Blockchain technology to use crypto-money. The virtual currency such as Bitcoin doesn't require any existence of central authority to facilitate the transaction and its processing. A wallet is a software program that stores public and private keys and interacts with the blockchain to allow users to send and receive digital currencies and monitor their balance. For security reasons, it is important to have a backup, regardless of the wallet you use, to avoid the loss of digital assets. There are many examples where people lose their wallets, but if they don't have backups; they lose digital funds as well. In this paper, we might get a complete overview of Bitcoin Wallets and how Blockchain plays a vital role in this uprising crypto trend.

II. Research Elaboration

This paper demonstrates how a Bitcoin wallet plays a vital role in transactions using Blockchain Technology. In this work, Blockchain technology addresses the problem of cryptography consensus. And if there is a method to ensure financial activity and transaction actions are stored in a particular database without the central authority's intervention. It analyses the main design and technological features showcased by blockchain and presents scenarios into which blockchain applications can be applied. Problems such as safeguarding the confidentiality transparency and speed of user transactions should be resolved by using blockchain technology.

This paper explores the challenges and opportunities posed by banking through the introduction of blockchain technology. Blockchain technology will turn the global financial strategy to achieve sustainable development using systems that are more effective than they are at the moment. Along with the initial release of Bitcoin in 2009, the first ever Bitcoin wallet, the Bitcoin-Qt wallet, was also introduced. The wallet operated as a full client. Initially, this process was rather speedy due to the limited history of the blockchain, but synchronization time gradually increased as blockchain data grew. Despite this, the wallet proved useful as it allowed users to send and receive coins, along with features such as an address book and digital transaction signing, which verified their ownership of a particular public key.

As the blockchain ecosystem continues to evolve, new use cases and applications are emerging, increasing the need for secure and user-friendly wallet solutions. Despite their growing importance, blockchain wallets remain a complex concept for many, often misunderstood or underexplored. There is a misconception that wallets are digital vaults for storing cryptocurrencies. Although wallets allow users to initiate transactions, monitor account balances, and effectively manage their blockchain-based digital assets, in reality, what they actually own are only the private keys that provide control and authority over these digital assets within the blockchain ecosystem.

III. Types of Wallets

There are two types of blockchain wallets based on private keys: hot wallets and cold wallets. Hot wallets are like normal wallets that we carry for day-to-day transactions, and these wallets are user-friendly. Cold wallets are similar to a vault; they store cryptocurrencies with a high level of security. Hot and Cold wallets can be further broken down into 3 types:

1. Software Wallets
2. Hardware Wallets
3. Paper Wallet

1. Software Wallet: A software wallet is an application that is downloaded on a device; it could be a desktop or a mobile device, or it could be a web-based wallet that can be accessed online. Breadwallet, Jaxx, and Copay are popular software wallets. Software wallets can be further divided into Desktop Wallets, Online Wallets, and Mobile Wallets.

2. Hardware Wallets: A hardware wallet is a type of cold storage device, typically like a USB, that stores the user's private key in a protected hardware device. These wallets are similar to portable devices that can be connected to the computer (plugged in). As noted earlier, they are less prone to malicious attacks and are hack-proof. Ledger, Trezor, and KeepKey are the top hardware wallets on the market. To make a transaction your hardware wallet must be connected to your computer.

3. Paper Wallet: A paper wallet is an offline process for storing cryptocurrencies. This wallet is a printed paper that has both your private key and public key, which are accessed using a QR code. Since these wallets are safe, they are widely used for storing large amounts of cryptocurrencies. Bitcoin Paper Wallet and MyEtherWallet are two widely used paper wallets. A paper wallet works with your software wallet to transfer funds from your software wallet to the public address shown on your paper wallet. First, you park your funds in a software wallet, then you transfer the funds from your software wallet to the public address printed on the paper wallet.

IV. Wallet Implementation

The wallet implementation of a Desktop Software cold wallet implementation and working with tokens can be done as given below:

- Add token: associates a token with a selected account.
- Delete token: removes an associated token from a selected account.
- QR code generation for receiving payment: creates *.png file or allows scanning from the screen. Payment: load a pre-recorded QR code, enter the transfer amount (mandatory>0, accuracy is automatically adjusted), and (reason) text.
- Biometric identification. - Chronological report of token transaction ledgers for a selected account.
- Users exchange data and information (transactions) through the Test App and the Mobile Test App, most of which are files with different formats. Transactions between users are confirmed by keys and names, which are in turn managed by the wallet.

To make a token transfer, the receiver generates a QR code containing its blockchain account name and token symbol for payment. This QR code is sent to and loaded by the sender. Then the sender is able to enter the desired number of tokens and payment description. This creates a transaction, i.e., a call to action ‘transfer’ from the system smart contract. Then a request is sent to the macOS secure enclave with the sender's account name. As a result, the sender's public key is obtained.

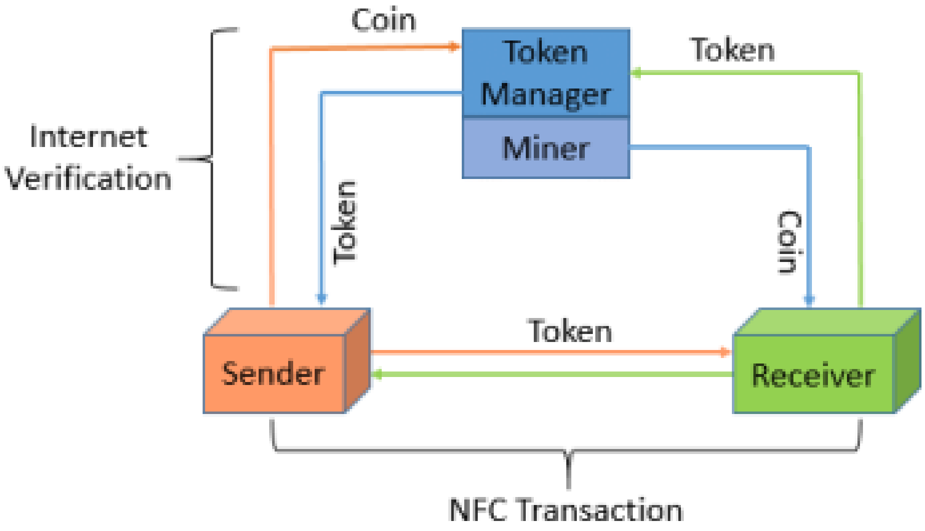
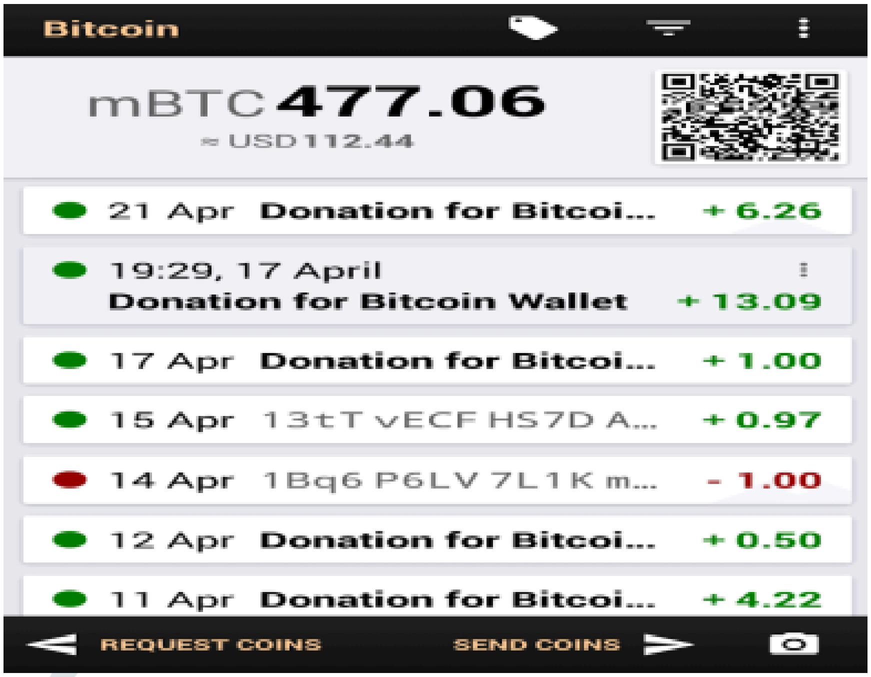


Fig 1: Working of Token

Blockchain wallet features:

- Easy to use. It’s just like any other software or wallet that is used for your day-to-day transactions.
- Highly secure. It is just a matter of securing your private key.
- Allows instant transactions across geographies. And these are barrier-free, without intermediaries.
- Low transaction fees. The cost of transferring funds is much lower than with traditional banks.
- Allows transactions across multiple cryptocurrencies. This helps you do easy currency conversions.



mBTC 477.06

≈ USD 112.44

21 Apr	Donation for Bitcoi...	+ 6.26
19:29, 17 April Donation for Bitcoin Wallet		+ 13.09
17 Apr	Donation for Bitcoi...	+ 1.00
15 Apr	13tT vECF HS7D A...	+ 0.97
14 Apr	1Bq6 P6LV 7L1K m...	- 1.00
12 Apr	Donation for Bitcoi...	+ 0.50
11 Apr	Donation for Bitcoi...	+ 4.22

Fig 2: Actual Blockchain record of a Bitcoin Transfer

VI. Analysis

We do require blockchain implementation in the core banking system so that we can ensure that each transaction is authenticated and it is initiated by the user itself. The adoption of this technology is very feasible and reduces the security overhead that comes with a traditional banking system such as centralization. Blockchain-based wallet systems and banking systems dismantle the centralization of data and store the data at several places since its key to success is the distribution of data across the network at the distributed databases. The data and customers both are very secure in the hands of the blockchain-based technology banking system.

VII. Conclusion

The adoption of technology depends on the requirements of the business here in this case is for the banking system. The no of profits margin derives from the adoption of technology. Most of the Banks around the globe have adopted blockchain as they value customers' privacy in the first place. There are always pros and cons related to each technology which is the same in the case of blockchain too. The only problem with technology is the cost. The cost drives the business's day-to-day operations, so this is where the banks have to think carefully before the adoption of this technology. The blockchain-based banking system becomes more proven when it is powered by blockchain

References

[1] Nagendra Singh Yadav, Vishal Goar, Manoj Kuri (2020). Crypto Wallet: A Perfect Combination with Blockchain and Security Solution for Banking, International Journal of Psychosocial Rehabilitation

[2] Ivan Popchev, Irena Radeva, Mirislova Dimitrivoi (2023). Towards Blockchain Wallets Classification and Implementation. Researchgate

[3] Simplilearn: (2023). What is Blockchain Wallet and How Does It Work?