International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Innovative Investment Pattern on Peer 2 Peer Transaction of Bit Coin-An E-Wallet

Mrs. Keerthi. B. S[1], Dr. N. Selva Kumar[2]
[1]Ph.D. Research Scholar, [2]Associate Professor
School of Commerce, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT
An E-wallet bases on peer to peer transaction which allows the online transaction directly from payer to payee without the help of any financial institution. The reason behind avoiding third party is lack of trust and the malpractices happens nowadays especially a country like India annexing everything with aadhar and making the confidential matters of every individual is transparent to all over the country which costs extra spending too. The important decision is symbolize by the longest chain, which has the furthermost proof-of-work attempt invested in it. Basically the contract will be made in the particular transaction cost and the same will be protected with the transaction at a low priority and thus the confirmation will be made rapidly. But the chain based proof of work gives sequential witnesses to a largest pool of work. This can be initiated with a minimal amount of networking systems which are cost effective and easy to maintain on all kinds of transactions.

Considering this passive investment strategy in which the investors can purchase and hold this for a longer period of time. The fluctuation with the market experiencing is known for holding in the Bit coin, in which the investor will create the trend in the booming market always.

Keywords: *Peer to peer, networking, wallet, Digital signatures, transaction, Chain process, etc*

I. INTRODUCTION

According to legend, Satoshi Nakamoto began working on the Bit coin concept in 2007. While he is on record as living in Japan, it is speculated that Nakamoto may be a collective pseudonym for more than one person. Bit coin.org is born! The domain was registered at anonymousspeech.com, on18th August 2008 as site that allows users to anonymously register domain names and currently accepts Bit coins.

Later in 31st October 2008 Nakamoto publishes a design paper through a metzdowd.com cryptography mailing list that describes the Bit coin currency and solves the problem of double spending so as to prevent the currency from being copied.

On November Satoshi Nakamoto designed a project with the bit coin with the help of source forge.

The first transaction took place on Jan of Bit coin currency, in block 170, takes place between Satoshi and Hal Finney, a developer and cryptographic activist.

WHO IS SATOSHI NAKAMOTO?

Satoshi Nakamoto was the inventor of the Bit coin protocol, publishing a paper via the Cryptography Mailing List in November 2008.

“Satoshi” means "clear thinking, quick witted; wise". “Naka” can mean “medium, inside, or relationship”. “Moto” can mean “origin”, or “foundation”. Those things would all apply to the person who founded a movement by designing a clever algorithm. The problem, of course, is that each word has multiple possible meanings. We can’t know for sure whether he was Japanese or not. In fact, it’s rather presumptuous to assume that he was actually a ‘he’.

We’re just using that as a figure of speech, but allowing for the fact that this could have been a pseudonym, ‘he’ could have been a ‘she’, or even a

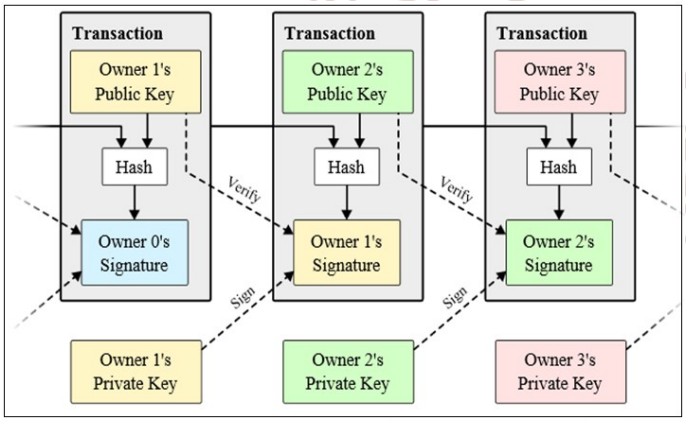
'they'. The *New Yorker'*s Joshua Davis believed that Satoshi Nakamoto was **Michael Clear**, a graduate cryptography student at Dublin's Trinity College.

PEER TO PEER VERSION OF ELECTRONIC TRANSFER:

This is the version of electronic transfer where one party can transfer to another party without the help of financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network times tamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. Most of the CPU power is controlled by the nodes on the networking system. Messages which delivers to the node will act as proof in the long network loops as a chain process.

Transaction Techniques:

The double spent system is entirely eradicated in this because after each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. This is model for the transaction methodology designed by Satoshi



The evidence for the transaction:

The evidence of work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it.

So if a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

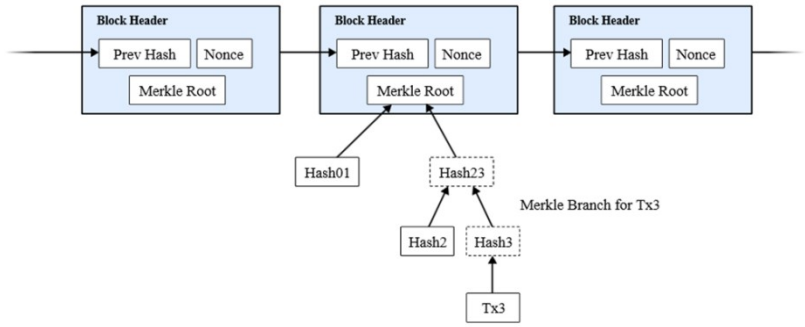
Steps to run networks used for the Bit coin:

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Easy payment transactions in Bit coin:

The user should keep a copy of the block headers of the longest proof. This act as a query to the network nodes until which satisfies the longest chain. The payee can't check his own transaction by himself where as it is possible only by the way of linking the chain in the network nodes until it resolve.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

DIFFERENT TYPES OF WALLETS IN BIT COIN:


Arcbit


-Armory


Bit coin core


Bit coin Knots


Bitgo


Bither


Electrum


Green address


mSinga

HOW TO USE BIT COIN:

1. Inform yourself- Start with a sign

Bit coin does not require merchants to change their habits. However, Bit coin is different than what you know and use every day. Before you start using Bit coin, there are a few things that you need to know in order to use it securely and avoid common pitfalls.

2. Processing payments

You can process payments and invoices by yourself or you can use merchant services and deposit money in your local currency or Bit coins. Most point of sales businesses use a tablet or a mobile phone to let customers pay with their mobile phones.

3. Accounting and taxes

Merchants often deposit and display prices in their local currency. In other cases, Bit coin works similarly to a foreign currency. To get appropriate guidance regarding tax compliance for your own jurisdiction, you should contact a qualified accountant.

4. Gaining visibility

There are a growing number of users searching for ways to spend their Bit coins. You can submit your business in online directories to help them easily find you. You can also display the Bit coin logo on your website or your brick and mortar business.

5. Contract

A sales contract might be used to ensure that specific terms are met to lessen the chances of a misunderstanding. For instance, the party sending payment is responsible for paying any transaction fee that might be necessary. A contract might specify that a transaction fee must be paid and what amount, so as to prevent the situation where the transaction is considered a low priority transaction and thus isn't confirmed quickly.

6. Submit your business and paying taxes:

With Bit coins, there's likely to be some difference between the values of BTC when you received them as payment, versus when you go to exchange them for another currency like USD, should you decide to do so. This scenario, likewise, would be no different if

you accepted foreign currency or gold as payment. Under some scenarios, it might make sense to book the dollar value of BTC income as it is received, and then to book any difference incurred when it is exchanged for fiat currency. Under others, it might make sense to book the whole thing at the time of exchange.

CONCLUSION:

This peer to peer wallet will be great helpful wallet in future to safe guard our hard earned money without been looted by the financial institution, government and other hazardous forces in the developing countries like India. Because lay man hard earned money is not been properly protected and utilized proper by the earning person. If these type transactions happened to everyone get equalized chance to utilize the wealth of the nation in all the circumstances.

REFERENCE:

1. Gurusamy S (2004), "Financial Servicecs and Markets", Thomson Asia Pvt. Ltd, New Delhi-110014, PP.55-67.
2. Kapoor V. K. (1983), "Banking Services", Himalaya Publishing, New Delhi-110002, PP 34-46.
3. Khan. M. Y (2004) "Financial Services", Tata Mc Graw – Hill Publishing Co. Ltd, New Delhi-110002, PP 45-62.
4. R. C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, April 1980, PP 122-133,.
5. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, 1991, PP 99-111.
6. Ron, D., Shamir, A.: Quantitative analysis of the full Bit coin transaction graph. In Sadeghi, A.R., ed.: Financial Cryptography and Data Security. Volume 7859 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 6–24
7. Chaum, D. L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM 24(2) (Feb 1981) 84–90