



Bitcoin Referral System using Secured Blockchain Technology

Shrikant Nagure, Aarti Pratap, Aishwarya Bhanage, Neha Shinde, Saurabh Deshpande

Abstract: Bitcoin has emerged as necessary cash software systems. For making the use of bitcoin we are using blockchain for various security reasons and transactions. Mining adds records of past transactions to the distributed ledger referred to as Blockchain, permitting users to achieve secure, strong agreement for each dealing. Mining in addition introduces wealth among the kinds of the latest units of currency. They consider miners to validate transactions. Cryptocurrencies need robust, secure mining algorithms. During this paper, we tend to survey & develop the particular Bitcoin referral system, platform in distinction employed by major Cryptocurrencies platform. We tend to assess the techniques, quick withdrawals, users/admin dashboard, referral system, combination & different several terms.

Keywords : Block Chain, Wallet, Referral, Compounding, etc

I. INTRODUCTION

A survey has given us an idea that Bitcoin — the world's first cryptocurrency — was introduced in 2009, and since Then, over one thousand tradable tokens have inherited existence. However, for associate degree a whole state unnoticed on the tremendous likelihood that the remaining of the world had been enjoying. Using Cryptocurrency is the good alternative to use in today's world. Suppose we've got to try to an enormous dealing, and by doing it by a centralized authority, it's going to charge some quantity of cash on our dealing. In this cases if we tend to use Cryptocurrency like Bitcoin for creating dealing of larger quantity, it'll not charge extra money to transfer a bitcoin value of larger amount(1 bitcoin = in lakhs, it varies daily) they will be viewed as an internet marketplace for the complete cryptocurrency network.

These way of transactions measure vital, as a result you'll be able to exchange 2 bitcoins(fast, usually suburbanized digital currency on next-gen block chains) instead of RS and giving charges to interact them.

The ways to get some would be through mining, or sites wherever you'll be able to trust and exchange multiple transactions (buy/sell). Cryptocurrency Referral System exchange platform has to be developed wherever bitcoin costs ought to be updated daily and invest through dashboard. Today, you'll be able to hardly obtain a newspaper, activate a TV, hear a voice communication, or refer to a any type of communication without Internet. Overall, it's modified for the higher. Point, click and invest — these Three very little words add up the attraction of investors. Victimization nothing over a web affiliation associate degree an account with an internet broker(site), one will simply invest in Bitcoin referral system with mere keystrokes. Bitcoin commonly defined as cryptocurrency, A virtual currency or digital currency- it's kind of cash that's fully virtual. It's like an internet version. You'll be able to use it to shop for product and services.

However, not several retailers settle for bitcoins and a few countries have prohibited it. The physical bitcoins you see square measure unworthy while not the personal codes written within them. Every bitcoin is essentially a file that is keep in a very digital wallet app on a sensible phone or PC folks will send bitcoins to your digital wallet, and you'll be able to send bitcoins to others. Each single dealing is recorded publically list referred to as block chain. Their square measure 3 ways to others get bitcoins.

- 1) Buying bitcoins victimization real cash
- 2) You will sell things and lets other pay you with bitcoins
- 3) Or they will be created solving some mathematical puzzles using a powerful PC

II. BITCOIN

Bitcoin is one among cryptocurrencies. Cryptocurrencies are virtual currencies which uses cryptography for security purpose. All these currencies including bitcoin does not exist in physical form

A. Bitcoin Mining

Mining is a record-keeping service done through the use of machine method power. Miners keep the blockchain consistent, complete, and unchangeable by continuously grouping new broadcast transactions into a block, that's when broadcast to the network and verified by recipient nodes. . To be accepted by the rest of the network, a replacement block ought to contain a proof-of-work (PoW).

Manuscript received on February 10, 2020.

Revised Manuscript received on February 20, 2020.

Manuscript published on March 30, 2020.

* Correspondence Author

Shrikant Nagure*, Master degree, Engineering in Information Technology.

Aarti Pratap, Pursuing BE(COMPUTER) in RMD Sinhgad School Of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.

Aishwarya Bhanage, Pursuing BE(COMPUTER) in RMD Sinhgad School Of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.

Neha Shinde, Pursuing BE(COMPUTER) in RMD Sinhgad School Of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.

Saurabh Deshpande, Pursuing BE(COMPUTER) in RMD Sinhgad School Of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Bitcoin Referral System using Secured Blockchain Technology

The system used depends on Adam Back's 1997 anti-spam theme, Hashcash. [failed verification, The prisoner desires miners to hunt out selection cited as a these days, such once the block content is hashed along, with these days the result is numerically smaller than the network's downside target eight.

This proof is easy for any node at intervals the network to verify, but terribly long to come back up with, as for a secure science hash, miners ought to try many different these days values before meeting the four downside target. A

pocketbook stores the information necessary to interact bitcoins. whereas wallets ar generally delineate as a vicinity

to hold or store bitcoins, attributable to the character of the system, bitcoins unit of measurement indiscrete from the blockchain dealing ledger. A pocketbook could be a heap of properly made public jointly factor that "stores the digital credentials for your bitcoin holdings" and permits one to access them. Bitcoin uses public-key cryptography, throughout that two cryptanalytic keys, one public and one personal, unit of measurement generated. A pocketbook could also be a set of these keys There unit of measurement several modes that wallets can operate in. they have associate inverse relationship with regards to trustlessness and method desires.

Third-party net services referred to as on-line wallets offer similar utility but might even be easier to use throughout this case, credentials to access funds unit of measurement keep with cyberspace pocketbook provider rather than on the user's hardware. As a result, the user ought to have complete trust at intervals the on-line pocketbook provider.

B. Finance in Bitcoin

As from the fig 1 we can see there is rise in users , that are using bitcoin for transaction. Even the people that deal with bitcoin knows about its use. As per Analysis it will be growing continuously until it meets the criteria of not adding blocks anymore. Basically, at first market the developers and miners are having availability of bitcoins, and hence they can trade the bitcoins to those who are demanding for it, like the investors.

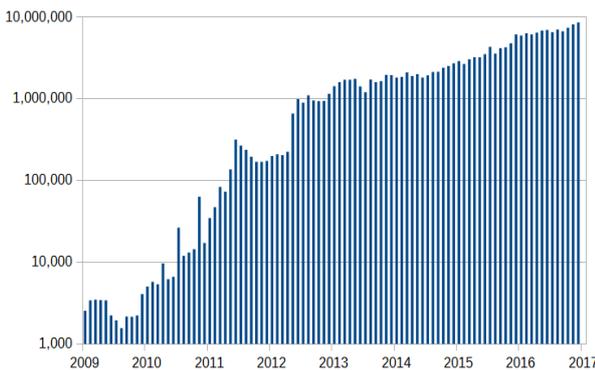


Fig 1: Number of Bitcoin transactions from 2009 to 2017

III. BLOCKCHAIN

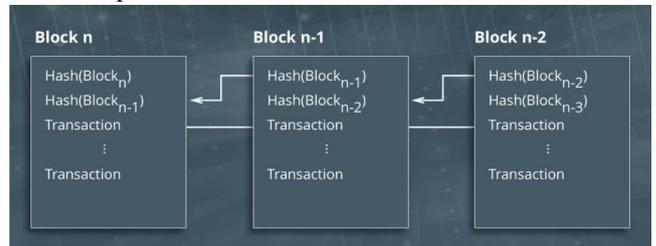
Blockchain are originally the database of collection of blocks containing the details of transactions between the two parties. The blocks are interconnected with one another and having the precise timestamp it's the shape of p2p (peer to peer) communication once the transactions are stored completely within the blockchain database then it became irreversible. These can be understood as an open and distributed ledger

that is capable of recording. Programming of this ledger can be carried out so that transactions can be called automatically. This technology has the power to scale back the usage of the foremost powerful feature of the present transaction method i. e the middle man. As we all know that digital money has attracted a substantial amountof individuals and services with the assistance of digital ledgers. It has a possible impact on the bulk of transaction related practices that the transaction processes like loans, bonds, stocks everything has been digitalized but the most problem is that the fee taken by the like banks, financial firms, etc. blockchain technology and bitcoin tends to unravel this problem by providing the p2p transaction process.

A. Some basic but Important algorithms of Blockchain

1. Proof of Work (POW):

In order to confirm transactions miners solve the puzzles and by solving it a new block is formed the complexiy of a puzzle depends on the how many are the number of users, the current power and the network load. For providing security block contains its previous hash



If a miner is able to solve the complex puzzle then, the new block is formed. And as the result the transactions are placed in this block and considered to be confirmed. [3]

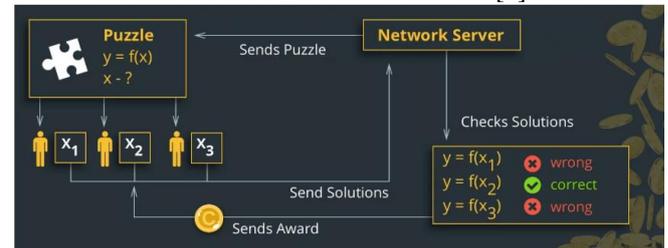


Fig 3.1: Example of POW

2. SHA 256

SHA – 256 algorithm is a algorithm that is used in blockchain to produce a constant hash of 256 bits every time. This algorithm is basically from the field of encryption [5]

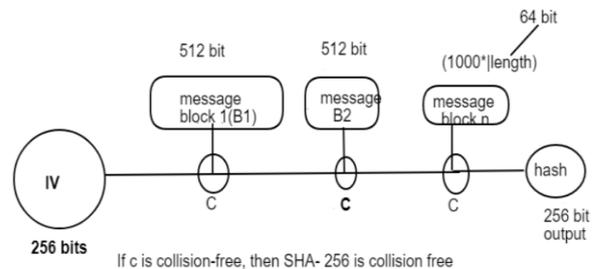


Fig 3.2: SHA Example

3. Digital Signature:

A digital signature is a technique that binds to the digital data. This binding may be independently verified by receiver in addition as any third party. Digital signature is a cryptographic value that's calculated from the info and a secret key known only by the signer[6].

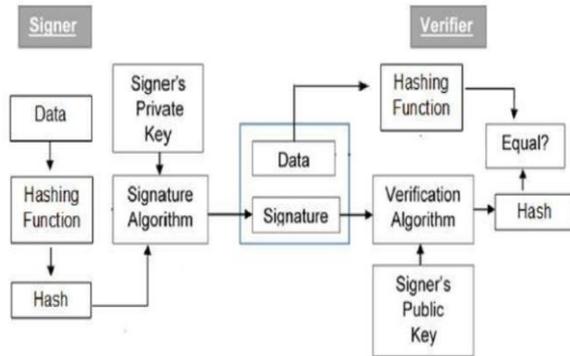


Fig 3.3: DigitalSignature Example

A. Blockchain in finance:

A. Asset Management

Asset management with Traditional trade processes may not be as swift because it got to be or may be manual and should be choked with risk – these items is difficult in terms of cross border transaction and for non-standard investment products, e.g. loans. the centre persons and brokers keep their copy of transaction which can create inconvenience and errors. Blockchain technology would help in making process entirely streamline by providing an automatic trade lifecycle. this may end in substantial decline in infrastructural cost, efficient and effective transparency and data management moreover faster processing cycles.

B. Insurance Processing

Some great challenges of insurance sector is listed as Fraudulent claims, manual processes, fragmented data sources which ends up in the reduction of customer satisfaction. Creating policies within the type of smart contracts supported blockchain helps in insurance. It offers complete control, transparency and traceability for each claim and can lead to automatic pay-outs.

C. Global Payments

the world payment sector is large yet it's slower, costly and highly at risk of errors which makes it untraceable resulting in concealing. The blockchain reduced the time of cash transfer to other countries by providing the \$64000 time payment transfer.

D. Compliance

Financial establishments across the globe area unit in command of obliging and reportage on kind of needs from their native regulator grasp Your client (KYC) maybe key demand here however the tactic are going to be unbelievably time overwhelming and lack the automated client identification technology and integration required by groups to expeditiously do their work. Blockchain technology may provide a digital single supply of ID data permitting the seamless exchange of documents between

banks and external agencies. This might possible result in automatic account gap, reduced resource and price, all while maintaining the privacy of data that's lawfully needed.

IV. PROPOSED SYSTEM

This proposed system states about its vital modules of the system. Although bitcoin is now gaining importance in the market, its rate depends highly on inflation. Sometimes it is not possible to get the expected revenue. This system deals with the people who in advance holds bitcoin. As of now considerate amount of people holds bitcoin, but what is its use if only they are owning bitcoin and not getting, much from it. If the same bitcoins are invested in this system, it can generate a lot of revenue on daily basis. This system is providing various options such as compounding, to generate a considerate amount of percentage on daily basis. Also providing security by creating front end fake wallets. It give secure bitcoin payments by ensuring secure payments through using latest encryption techniques. The transaction will only happen after 3 check verification only. This system is globally accessible, so its benefit can be taken by customers almost all over the world. Another type of security that it will be providing that, this system is legally registered and no means of any illegal or fake working. So no need of worrying about your investment. Also it gives you one more way to earn more bitcoins on your invested bitcoin, by means of referral. Referral in sense it means, when u register your account with this system it will provide you a unique referral link. By sharing this link, those whoever registers using your link, you will be liable by some percentage of their invested bitcoin, it can be referred as you are getting commission. The referral amount will be based on 4 - level tree. In such a way this system is very beneficial for those who wants to use bitcoin and get benefit from it.

V. SMART CONTRACTS

Smart Contracts are self-fulfilling contracts, in line with the terms you set. Smart contracts are also known as blockchain contracts and were introduced by a cryptographer and legal Scholar named Nick Szabo in 1994. It involves conversion of contracts to computer code, storing and replicating them [2]. This would produce a ledger feedback like the money transfer and receipt of the service or product. In the business scenario, small contracts automate how blockchain is employed within the same way transactions of Bitcoins are applied. What Do Smart Contracts Provide You With?

- Independence
- Transparency
- Secure
- Savings
- Accuracy

VI. RESULT

This system consists of various modules, such as Top-up, Referral, Compounding, Auto/Manual. The Proposed System is integration of these modules and some other Functionalities.

Bitcoin Referral System using Secured Blockchain Technology

For the testing purpose of system each module was tested separately and then integrated. As this system is based on real time crypto currency, we cannot take the risk of dealing with crypto currencies for purpose of testing, as it may result in loss of bitcoins or double sending of bitcoins. First Test network was created and all the functionalities were checked on it. After performing the functions of the system we got the result as follows, In top-up we got the exact amount of bitcoin that we choose, no extra and no less bitcoins were added to the account of user in the system. In referral module referral incentive is generated as per its level in level structure(level 1-5)

In Compounding module, the amount invested in system is compounded daily as per plan of 45days and revenue is generated based on invested amount. Auto/Manual is given for convenience of the user. This is used for both while compounding and withdrawal.

As a Result, this system works with real time crypto currency very well with the security provided by Block chain. All the modules work properly. Due to this system consisting of various module in single platform, it gets ease for the users to rely on this system, not depending on various sites or platform performing different functionalities. 7 transactions are allowed per user, per day in order to avoid malicious activities.

VII. CONCLUSION

As you can see, each different Transaction has slightly different advantages and disadvantages. Moreover some cryptocurrencies are accepted globally while some are specific to some countries or region. Today everybody wants to invest their time to invest in cryptocurrency platform and earn more profit on the cryptocurrency they have bought and is laying just as it is, by investing it in referral system. For this purpose we are using Bitcoin as a cryptocurrency, as it is widely accepted across countries, so that this system can be used by a majority of people, to earn more on their asset.

REFERENCES

1. Assoc.Prof. Dr.Huseyin Yilmaz, BilecikSeyhEdebali University, Bilecik/ Turkey, "A NEW FINANCIAL INVESTMENT INSTRUMENT: BITCOIN"
2. Aayushi Sinha, Kamlesh Sharma, Chirag Madan" Success of Blockchain and Bitcoin", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-5, January 2019
3. Pilkington, M ,Blockchain technology: principles and applications. , 2015.
4. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009, [online] Available: <https://bitcoin.org/bitcoin.pdf>
5. <https://informationsecurity395.wordpress.com/2017/08/28/sha-256-algorithm/>
6. https://tutorialspoint.com/cryptography/cryptography_digital_signature.htm

AUTHORS PROFILE



Prof. Shrikant Nagure, Completed his Master degree of Engineering in Information Technology Author is Apple Certified Support Professional OS X. Published Various papers in International Conference, poster in National Conference. Author Has published various Research papers in Various Journals. Conducted and Organized Workshops on Networking , iOS Development, Linux.

Retrieval Number: F8966038620/2020@BEIESP
DOI:10.35940/ijrte.F8966.038620
Journal Website: www.ijrte.org



Aarti Pratap currently pursuing BE (COMPUTER) in RMD Sinhgad School Of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.



Aishwarya Bhanage, currently pursuing BE (COMPUTER) in RMD Sinhgad School of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.



Neha Shinde, currently pursuing BE (COMPUTER) in RMD Sinhgad School of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.



Saurabh Deshpande, currently pursuing BE (COMPUTER) in RMD Sinhgad School of Engineering, affiliated to Savitribai phule university, pune, Maharashtra.