International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Anonymous E-Cash Transaction is using Bitcoin

Sanket Subhash Mane

Department of MCA, YMT College of Management, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT

Crypto-currency is variety of digital and virtual currency on a technology is understood as Blockchain. Bitcoin is understood as peer to peer payment network. Bitcoin victimization payment dealing not needed central authority permission. Here all managing and validatory dealing anonymously payment network system.

Bitcoin shows new ways that E-cash dealing system. E-cash send directly to one user to second user. While not interrupted by the another user. Here even have quicker and minimum fees to transfer e-cash. Exploitation Bitcoin all the transaction cryptograpically secured. Bitcoin not provide very safe privacy guarantees, payment communication are saved in a public decentralized ledger.

KEYWORDS: *Blockchain, Bitcoin, Anonymous, privacy*

How to cite this paper: Sanket Subhash Mane "Anonymous E-Cash Transaction is using Bitcoin" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.4-7, URL: www.ijtsrd.com/papers/ijtsrd30222.pdf

IJTSRD30222

INTRODUCTION

Blockchain produce chain of block. Blockchain it holds the hash value of previous block. It contains combination list of dealing data. it contain value of nonce and Hash. Hash is alphanumerical value. Using hash value identify a block.[6]

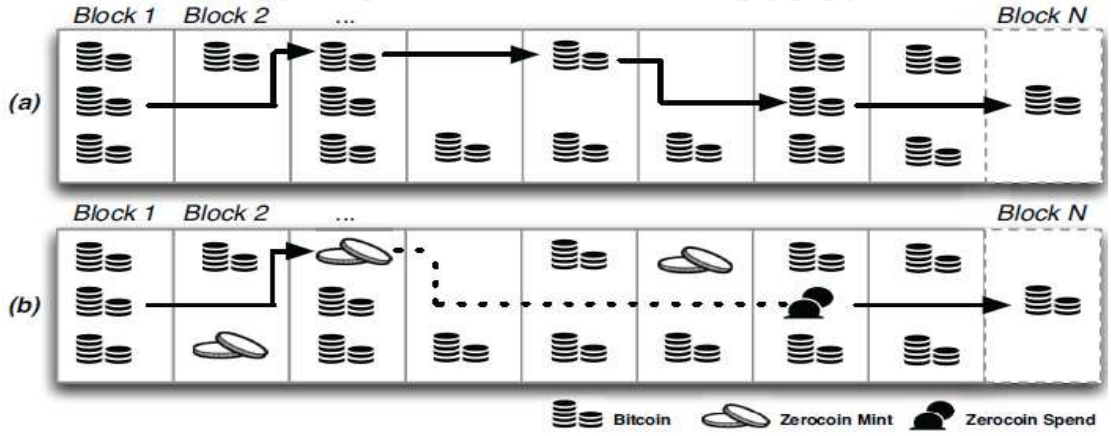


Fig. Two example blockchains. Chain(a)illustrates an ordinary Bitcoin exchange history, with every exchange connected to a former exchange. Chain(b)illustrates a Zerocoin chain. The linkage among mint and spend (spotted line) can't be resolved from the square chain information.

Sotoshi Nakamoto shows bitcoin on 31 October 2008 in a paper. After all the currency is open for public Bitcoin is early decentralized digital currency. Allows users to transfer E-cash peer to peer without an intermediate (banks, etc). User has full management of its Bitcoin. Bitcoin used for purchases, E-commerce transactions, investments, payments to shop for products.

It came into existence by person or group of people called satoshi nakamoto. Bitcoin helps to transferring assets is faster than regular fiat currencies. It has lower transaction fees. It has cryptographically secured. It has entire transaction cryptographically sign and sender and receiver also secure.

Bitcoin is that the most open financial set-up to this point. You'll be able to create payments with Bitcoins 24/7 everywhere the planet, even wherever there's no banking industry. Bitcoin is onymous, and anyone will open its notecase via the net with none verification or credit history. It's particularly useful in underbanked regions and third-world countries wherever most of the people struggle to induce access to cash.

You can pay Bitcoins within the same ways that you pay ancient digital cash – from a PC, an itinerant or a positive identification. Unlike order currencies, Bitcoins area unit deflationary, that means that their worth is ready to understand intentionally. Bitcoin is that the most transportable quality ever-created and might be transferred through satellites or perhaps radio waves. Despite makes an attempt to change offline Bitcoin payments, use of the currency still mostly depends on web accessibility. As Bitcoin continues to be in development, the group action speed and charges tend to vary betting on mining potency and network congestion. Changing Bitcoins into act incurs fees that area unit usually pricey. Besides everything, there's an absence of security behind the dealings of Bitcoin. There's no guarantee to shield your Bitcoins from human error (passwords), sure technical bugs (hard Drive corrupt, Virus). Bitcoin users have full management of the financial operations. They keep safe and private details, therefore there's no likelihood of taken MasterCard and visa numbers. But, All Over, Bitcoin still is not fully safe to process of how to bitcoin transaction used. Bitcoin transaction among peers[7]

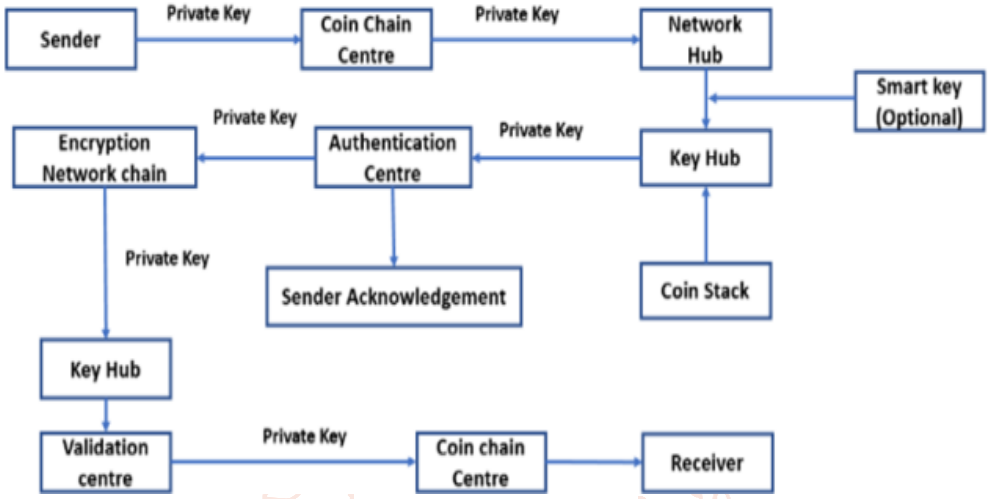


Fig. Bitcoin transaction

Literature Review

"Decentralizing Privacy: Using Blockchain to Protect Personal Data" author is Guy Zyskin, Oz Nathan, Alex, research paper Private records, and touchy records in popular, have to not be relied on in the arms of third-parties, where they are at risk of assaults and misuse. the Blockchain knows the users because the proprietors in their private information. Organizations, in turn, can focus on collect records without being overly worried approximately well securing and compartmentalizing them.[2015]

"Bitcoin: A Peer-to-Peer Electronic Cash System" in this paper author Satoshi Nakamoto research say, We've proposed a gadget for electronic transactions without relying on believe. We started with The usual framework of cash made from digital signatures. Here in research paper all network have their have proof of work to record a all customers history of transactions. Here easy payment authentication. Combining and splitting values explained privacy which algorithm used how to work in bitcoin this explain.[March 2009]

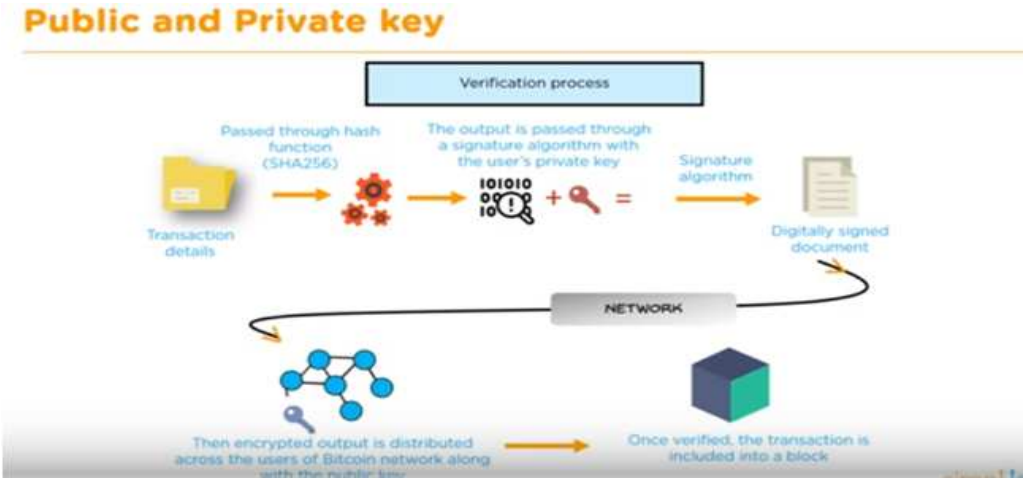
"Bitcoin is a popular peer-to-peer crypto-currency supplying vulnerable anonymity" author is Xiangxue Li and Yu Yu in research paper shows some points to related anonymous like Bitcoin is a popular peer-to-peer crypto-currency supplying vulnerable anonymity. Over the past few years, a big quantity of pioneering paintings focused on mixing transaction that a collection of customers alternate their bitcoins to interrupt the links, but, none of them fulfill all requirements. In this paper, protocol primarily based on the trick of cryptographically secure DKG. It offers stronger anonymity and is compatible with Bitcoin architecture. Subsequently, we analyse the protocol in all respects. **[**December 2017]

"A Survey on Anonymity and Privacy in Bitcoin like Digital Cash Systems" author is Merve Can Kus Khalilov and Albert Levi In this paper shows the survey which analyses anonymity and privacy studies in Bitcoin-like E-cash systems. In this paper have privacy and anonymity. On this category, author examined and supplied taxonomy for 25 studies, and extracted nine strategies and five effects from these research. Cryptographic have some problems to task getting problem. Here also shows the anonymity and privacy way to improve.[2018]

"Zerocash: Decentralized Anonymous Payments" author is BitcoinEli Ben-Sasson*, Alessandro Chiesay*, Christina Garmanz, Matthew Green in this paper Zerocash provides such anonymity, by using hiding consumer personal data, transaction amounts, and account balances from Public view. Bitcoin's scripting language with zk-SNARKs that allow rapid verification of expressive statements. **[**2014**]**

Research Methodology

Nameless manner without a name, Many Bitcoin offerings authentic id, linked profiles can be now not an anonymous with the aid of a ramification of aspect channels that's the cause of unlinkablility want. Unlinkability defines as very tough to connect special addresses of the identical user, difficult to hyperlink exceptional transactions of the same consumer and difficult to link sender of a charge of its receipt. [smartlearn]



Right here bitcoin nameless communication network used Tor browser. Tor is nameless conversation network. anonymouse use of sender and receiver communication is not connected. Tor utilized by regular users, Journalist, malware and other unlawful manner. Tor is funded by way of U.S. Branch and others. Bitcoin is relaxed and nameless virtual forex. Bitcoin can't be easily tracked back to you and are quicker and safer opportunity to other donation strategies.

Here have Basecoin is similar to altcoin. Basecoin may be into zero coins and again breaks link among original and new basecoin. Zerocash is untraceable e coins all the transaction is in the envelope. Ledger simply files life of transactions. No person realize.

Bitcoin is depending on blockchain. Every Bitcoin block memorializes a fixed of transactions which are amassed from the Bitcoin broadcast Network. Bitcoin used blockchain features. Here are the features is SHA-256 Encryption here all the encryption is done by algorithm, Blockchain uses cryptographic keys to relaxed identities and hash function to make the blockchain immutable public and personal key the usage of data switch and security the use of keys.

It uses SHA 256 stands for the number of bits it takes up in memory securing, hashing and algorithm. Hash value is unique. Value return by hash function its called hash value its impossible to decode original message using hash itself. It doesn't disclose hash value. SHA 256 is one way function here reverse is not possible that's make very secure. [3]

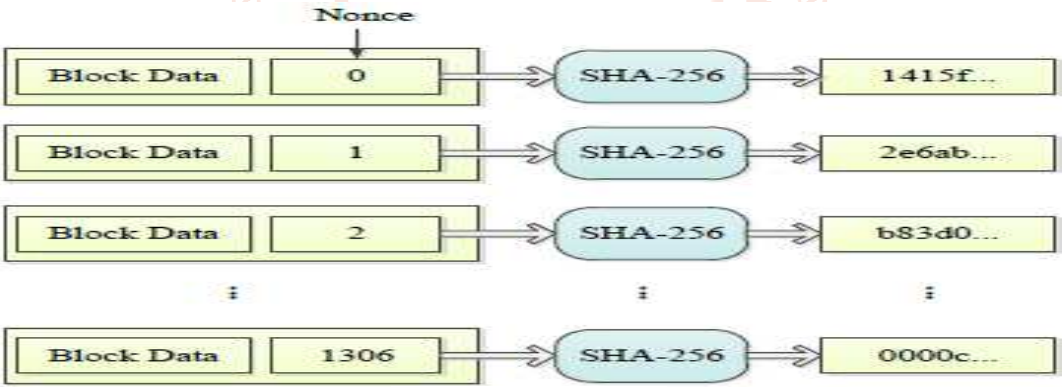


Fig. Hashcash example

Cryptography uses public and private key to encrypt and decrypt data. but private key is only user knows. So user is become anonymous.[8]

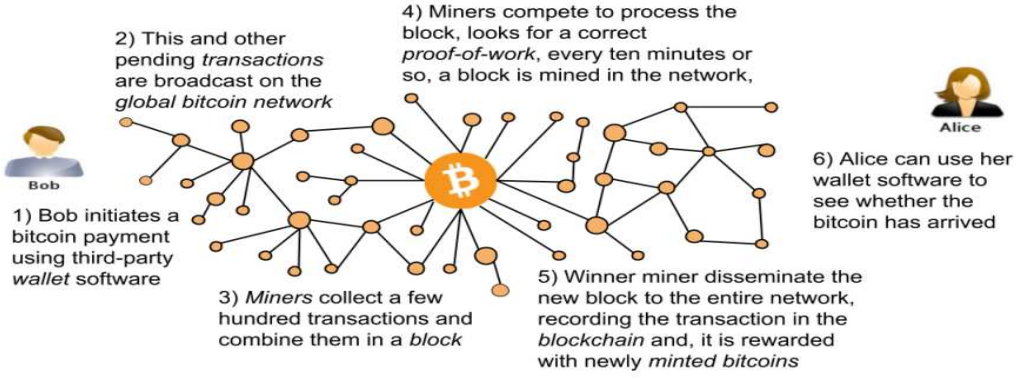


Fig. 4. Bitcoin transaction processing steps

Fig. Bitcoin transaction processing steps

Proof of work using get solution of problem and represent the decision. I2P using anonymous transaction is done. In zero knowledge protocols, blending is accomplished in a couple of transactions, consequently hyperlinks between transactions are incomplete. Secure At ease Multiparty Computation (SMC) allows a group of users. Users compute the cost of a public function the usage of their non-public Statistics, even as they maintain their inputs personal

Coutu is created the network of transactions approach. Transactions have input and output data have a amount V is show authorised person. Here all the values is constructed using hash tree. All block have counter values this all increased until the hash fulfils these necessities. The Bitcoin detail holds that this prize ought to be decreased each year, in the long run being wiped out through and through. [6]

```
Input:
 Previous tx: 030b5937d9f4aaa1a3133b...
 Index: 0
 scriptSig: 0dcd253cdf8ea11cdc710e5e92af7647...

Output:
 Value: 5000000000
 scriptPubKey: OP_DUP OP_HASH160
 a45f2757f94fd2337ebf7ddd018c11a21fb6c283
 OP_EQUALVERIFY OP_CHECKSIG
```

This is bitcoin transaction done through public and private key.

Future Enhancement –

Sometimes bitcoin public addresses shows their name and addresses here identity reveal and your internet protocol address also match. Bitcoin transaction is saved in public ledger. Anyone access personal information, all those issues create, which is why we use bitcoin mixture. Bitcoin mixture is used to hide id. We used in paper Tor browser search and transaction of currency to anonymous. This also we review in papers. Here another one concept to use in research paper use logless vpn to study. All this have subject to study related in bitcoin used. Here we also used always new transaction address in blockchain to use study material.

Conclusion-

Here have transaction information of bitcoin and bitcoin role in our life. The paper discussed way used to anonymous. E-cash should insure a user personal data from his network when conducting financial transactions. customer view. Here we have privacy protection. Here algorithm SHA 256 algorithm used. Cryptocurrency using hides user data. All the anonymous transaction used cryptocurrency.

References-

[1] Guy Zyskind MIT Media Lab and Oz Nathan Tel-Aviv University Cambridge, Alex Sandy Pentland MIT Media Lab Cambridge "Decentralizing Privacy: Using Blockchain to Protect Personal Data".

[2] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" satoshin@gmx.com Available: www.bitcoin.org/bitcoin.pdf

[3] Mere Can Kus Khalilov and Albert Levi "A Survey on Anonymity and Privacy in Bitcoin like Digital Cash Systems" 2018.

[4] Xiangxue Li and Yu Yu "Bitcoin is a popular peer-to-peer crypto-currency supplying vulnerable anonymity". December 2017.

[5] Ben-Sasson, Alessandro Chiesay, Christina Garmanz, Matthew Greenz, Ian Miersz, Eran Tromerx, Madars Virzay "Zerocash: Decentralized Anonymous Payments from BitcoinEli Technion, eli@cs.technion.ac.i. 2014.

[6] Aviel D. Rubin, Matthew Green, Christina Garman, Ian Miers," Zerocoin: Anonymous Distributed E-Cash from Bitcoin ".

[7] Raja Sreedharan, Rejikumar and Drishti Marwaha, Singapore University of Technology and Design, Kochi, Amrita Vishwa Vidyapeetham, India "A literature review on Bitcoin Arunmozhi Manimuthu".

[8] Mauro Conti, Sandeep Kumar E, Chhagan Lal, IEEE, Sushmita Ruj, IEEE "A Survey on Security and Privacy Issues of Bitcoin".