National Conference on Innovations in Computing and Networks (NCICN) - 2019
© 2019 IJSRSET | Volume 5 | Issue 9 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099

Peer Cash A Blockchain Based Cryptocurrency

Bindu Sivasankar*[1], An Suhail A Neema Sathar[2]

*[1]Assistant Professor, Department of Computer Science and Engineering, Younus College Of Engineering and Technology, Pallimukku, Kollam, Kerala, India

[2]B Tech Student, Department of Computer Science and Engineering, Younus College Of Engineering and Technology, Pallimukku, Kollam, Kerala, India

ABSTRACT

PeerCash is an decentralized application built on Ethereum blockchain technology. Decentralization means that there is no concept of having admin. Blockchain is a decentralized, distributed ledger secured technology which is immutable and verifiable. Every events in blockchain is recorded on blocks and it is encrypted using cryptography hashing. The advantage of PeerCash is that we can completely avoid the middle man from the web shopping payment system. That is we can completely remove the bank from interfering with our payment system and the buyer and seller can directly proceed their transaction and make their purchase. PeerCash transactions is completely recorded on blocks and the transactions is secured. So we can call PeerCash as a cryptocurrency. This paper describes about this application.

Keywords : Blockchain, Ethereum, Cryptocurrency, Cryptography

I. INTRODUCTION

Today's world is at our finger tips. Everyone wants to fulfill their requirements at their door step whether it be food or commodities. Online web shopping is such an application. We can just pick the item that we want and simply just pay the bill for the items to reach your hands. For this we use secured payment systems such as credit cards, debit cards, net banking, paypal etc for this. These payment sytems are good enough, but they lack certain things because we are living in the era of best technology. But they are not properly utilized. The problems is that there is no decentralization in these payment systems. This is a crucial problem for our privacy and security. Here the centralized systems are a bank, a centralized server etc. Therefore, we propose a system known as PeerCash.

A PeerCash is a digital cashing system which is completely peer to peer (i.e, people to people) that works on payment system of web shopping. Hence the name PeerCash. It works on the Blockchain technology. Blockchain is the technology that is used behind every cryptocurrencies that exist today. [1]

Blockchain is a distributed ledger which records all transactions. Once it is written, it cannot be rewritten. It is immutable. Blockchain is a decentralized network, which is a distributed database that is hosted on millions of computers simultaneously. Every system in the network are called as nodes. Nodes work together in groups to make the network secure. Every record is said to be called as blocks and it is connected as a chain in a chronological order, hence named blockchain. Every transactions is encrypted using cryptography so that transactions will be generated and represented by a hash value.[3][4][5] PeerCash also works in the same way. Every transactions is secured using cryptography. The transactions should be final and no further changes can be done to it.

We use ethereum blockchain technology in PeerCash as it is one of the biggest public blockchain mainnet available in the whole world with maximum number of computers and maximum number of people acting as nodes.

Ethereum blockchain can be used for making decentralised applications. In Ethereum blockchain PeerCash is implemented as a smart contract.[2] A smart contract is digital value of the code. PeerCash allows to settle the main problem faced by the fiat currencies i.e, double spending. It is deployed on the blockchain as a smart contract and will be able to track the transactions by searching it on the Blockchain explorer. It will be displayed as hash value to provide security over the transactions. It won't be able to tamper the transactions

II. RELATED WORKS

Sathoshi Nakamoto[1] A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a 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, propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps 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. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at its own will, by accepting the longest proof-of-work chain as proof of what happened while they were gone.

VitalikButerin, Gavin Wood, Joseph Lubin[2] Like Bitcoin, Ethereum is a public blockchain network. They both rely on blockchain to operate. Think about the Internet. You can build lots of different applications on top of it like email, online shopping sites and Facebook. Well, in a way, blockchain technology is a new type of Internet where you can build lots of different applications. Bitcoin and Ethereum are just two examples. The major difference between Bitcoin and Ethereum, however, is their purpose. Whereas Bitcoin provides one specific function, peer to peer electronic Bitcoin payments, Ethereum offers a platform that enables developers to build and deploy other decentralized applications. You could, for example, build another Bitcoin type currency on Ethereum.

Ian Grigg[3] Current technologies for blockchain fall short of providing what developers and end-users need in order to contract together and to build large scale businesses. EOS, propose a performance-based and self-governing blockchain that provides an operating system for building large-scale consumer facing distributed applications. This paper outlines the context, vision and software architecture underlying EOS, which are building to serve a broad and diverse group of users with smart business.

David Schwartz, Noah Youngs, Arthur Britto[4] While several consensus algorithms exist for the Byzantine Generals Problem, specifically as it pertains to distributed payment systems, many suffer from high latency induced by the requirement that all nodes within the network communicate synchronously. In this work, present a novel consensus algorithm that circumvents this requirement by utilizing collectively-trusted subnetworks within the larger network, show that the "trust" required of these subnetworks is in fact minimal and can be further reduced with principled choice of the member nodes. In addition, it show that minimal connectivity is required to maintain agreement throughout the whole network. The result is a low-latency consensus algorithm which still maintains robustness in the face of Byzantine failures. It present this algorithm in its embodiment in the Ripple Protocol.

III. METHODS AND MATERIAL

PeerCash is developed on ethereum blockchain using a standard protocol known as erc-20 standard. Erc-20 is a token smart contracting, it has an interface. In smart contract an interface is added. In interface Peercash is actually what is doing, are Total supply, Account transafer (buyer to seller), balance to be displayed in account(deduction, addition). These are to be verified. The Total supply is fixed.

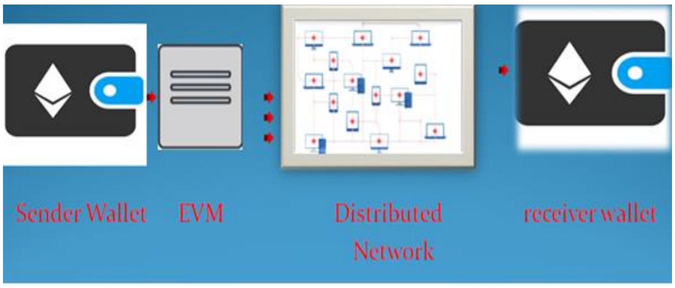


fig1.Design Of PeerCash

The above figure shows the design of PeerCash consist of sender wallet, a receiver wallet, an EVM and a distributed network. An EVM is an Ethereum Virtual machine. When a sender sends an amount of PeerCash to the receiver, it get passed through the EVM. Amount of coins sending is a smart contract. EVM will convert this smart contract to byte code and then pass to the distributed network. The distributed network consist of millions of computers, nodes. These nodes will check whether the transfer is correct to the actual reciever. If it is correct then they will write to the blockchain and the amount will be in receiver account.

PeerCash is using evolutionary prototypying model. It is tested in two testnet blockchains, that is Ganache Blockchain and Rinkeby Testnet. Ganache Blockchain is the private blockchain, which is given by ethereum for free use. Ethereum is using Solidity programming language. So first we write the code in solidity, that is the interface should be written. Then it is migrated to Ganache as a smart contract. Then we can test the smart contract using Node js. Rinkeby testnet is also working in the same way. These two testing needs to be complete only then we can completely deploy it into main blockchain.

How we can use PeerCash in web shopping. This is our next question? Ordinary payment gateways like debit card, credit, paypal etc... is using a centralized system. PeerCash is completely different from them. When going through the checkout page, after selecting a payment method they will direct us to their centralised server. In this case there is a financial institution. But in PeerCash we have wallet which can be used as extension. After clicking checkout and selecting PeerCash as payment method, the browser will securely ask to connect with the wallet. Here the browser connecting means , the seller account is requesting to pay the amount for purchasing. If the buyer accept this then it should be visible as a popup notification, and thus there is no need to direcyed int banks website.

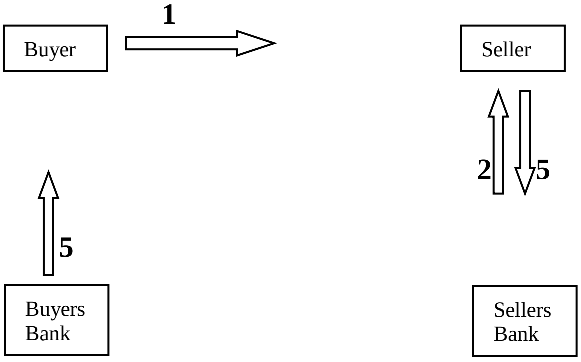
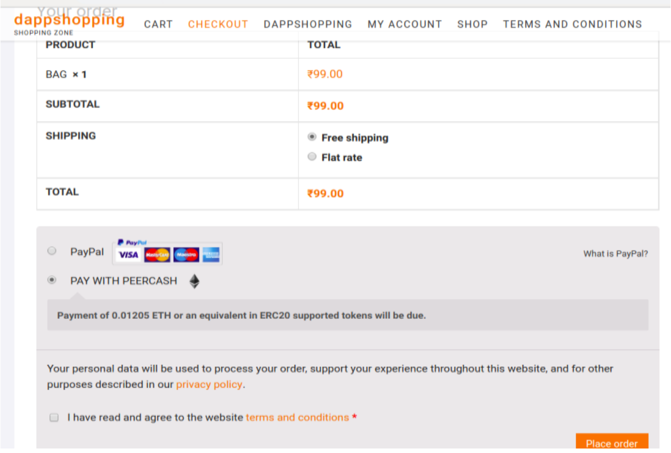


fig2. EXISTING SYSTEM

From the above figure,
1.The buyer makes a debit card purchase at checkout.
2.The debit card purchase to transmission of payment data from the seller to sellers bank
3. Transmission of payment data from buyers bank to the receiver bank
4.After receipt of payment of payment data, transfer of funds
5.Information is updated.

IV. RESULTS AND DISCUSSION

PeerCash is purely an extension based payment system for web shopping. PeerCash does not need any bank confirmations to make the payment done. It is directly peer to peer transaction system. It only needs the confirmation of the person who is using it. Buyer and Seller has equal rights and they acts as the banker for the transaction to be done. This also removes the third party to avoid the additional charges. Banks are levying high charges on the transaction basis. PeerCash removes the third party from this. PeerCash payment system allows to securely connect the browser with wallet by popup notification. Its only needs the confirmation of the user to connect the wallet with the browser. After connection we can securely pay for the order. It will take less time taken than the other payment system currently in use. It also implements the security, because there is no need to enter any information on the shopping site, it gets directly connected with the wallet. Every transactions is highly secured than other current payment system.



PRODUCT	TOTAL
BAG × 1	₹99.00
SUBTOTAL	₹99.00
SHIPPING	● Free shipping ○ Flat rate
TOTAL	₹99.00

○ PayPal

● PAY WITH PEERCASH

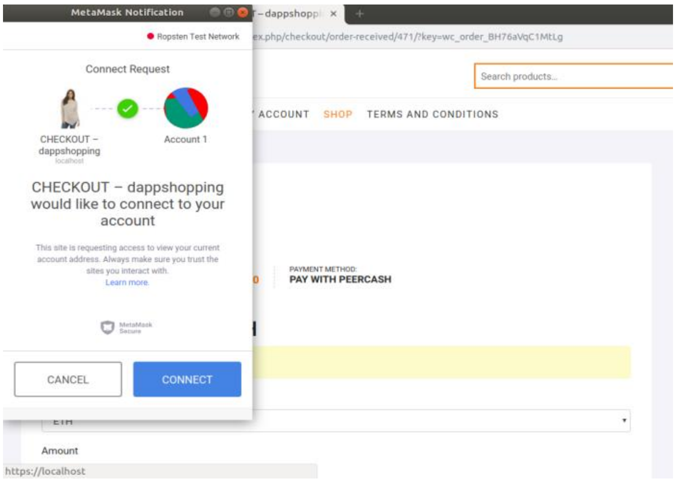
Payment of 0.01205 ETH or an equivalent in ERC20 supported tokens will be due.

Your personal data will be used to process your order, support your experience throughout this website, and for other purposes described in our privacy policy.

□ I have read and agree to the website terms and conditions *

fig3.Selecting PeerCash as payment option

The above figure shows that when we buy a product from web shopping, then we add it to the cart and chosen to checkout. Then we need to select Peercash as payment option and place the order.



CHECKOUT – dappshopping would like to connect to your account

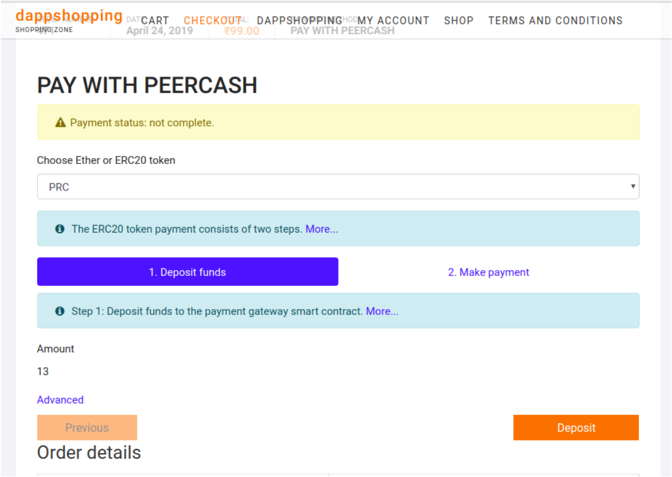
This site is requesting access to view your current account address. Always make sure you trust the sites you interact with.

PAYMENT METHOD:
PAY WITH PEERCASH

Amount

fig4.Browser asking to connect the wallet

The above figure shows that, after clicking the place order , the browser will ask us to connect with our wallet. That is the seller is asking to connect with our wallet. And then a popup window will open up.



PAY WITH PEERCASH

Payment status: not complete.

Choose Ether or ERC20 token: PRC

The ERC20 token payment consists of two steps. More...

Step 1: Deposit funds to the payment gateway smart contract. More...

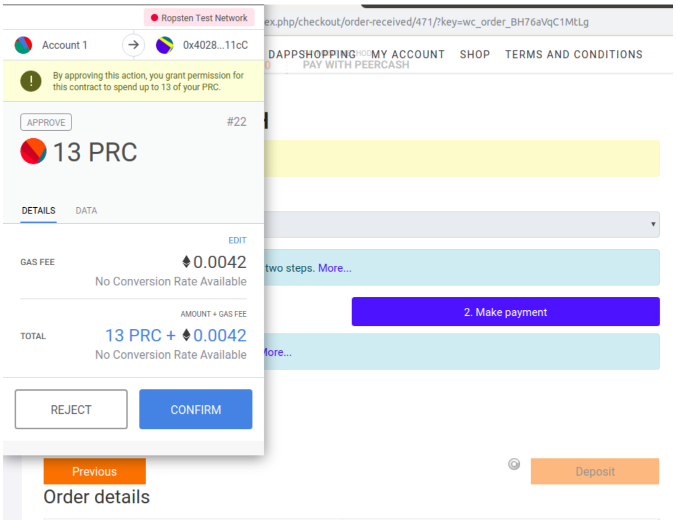
Amount
13

Order details

fig5. Pay with peercash

From the above figure it shows that, after clicking connect, the buyer has to go through two steps to pay the amount. First they need to deposit the fund and then pay blockchain fee. Depositing the fund means verifying whether the actual amount is getting correctly received by the seller. Only after paying the required blockchain write fees the amount will be credited. Otherwise Peercash will be back to the account and order will be cancelled.

The below figure shows that it is needed to confirm the deposit.



ex.php/checkout/order-received/471/?key=wc_order_BH76aVqC1MtLg

By approving this action, you grant permission for this contract to spend up to 13 of your PRC.

#22

13 PRC

GAS FEE ♦0.0042
No Conversion Rate Available

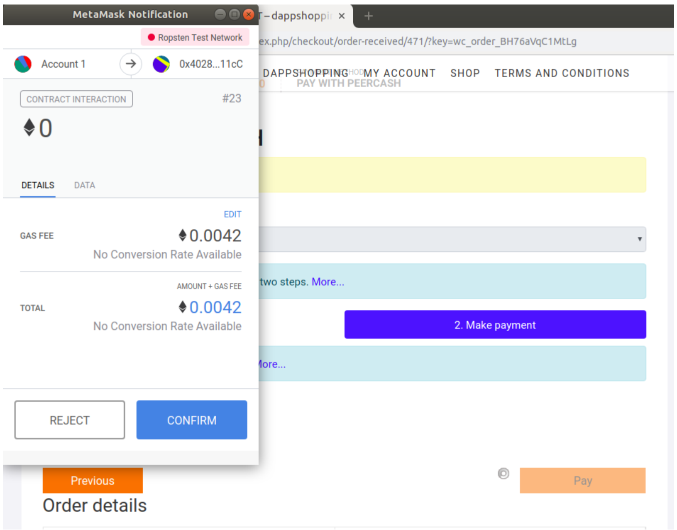
AMOUNT + GAS FEE
TOTAL 13 PRC + ♦0.0042
No Conversion Rate Available

two steps. More...

Order details

fig6.Deposit Confirmation

Below fig shows that after confirm it is needed to pay the blockchain fee to place the order successfully.



ex.php/checkout/order-received/471/?key=wc_order_BH76aVqC1MtLg

#23

♦0

GAS FEE ♦0.0042
No Conversion Rate Available

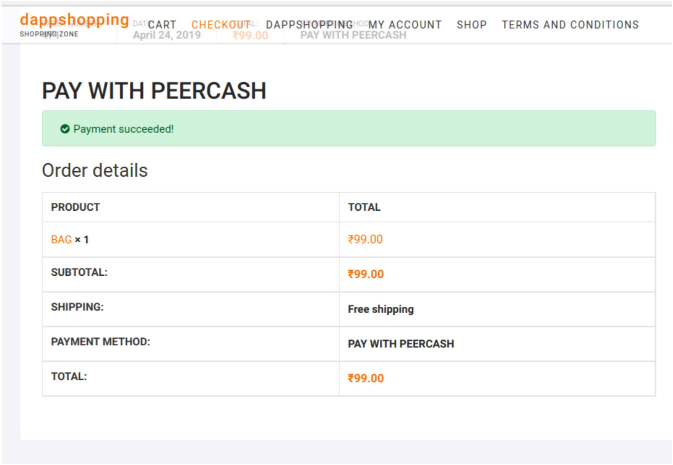
AMOUNT + GAS FEE
TOTAL ♦0.0042
No Conversion Rate Available

two steps. More...

Order details

fig 7.Paying the fees.

Below figure shows that the order is successful after successful payment.



April 24, 2019 ₹99.00 PAY WITH PEERCASH

PAY WITH PEERCASH

Payment succeeded!

Order details

PRODUCT	TOTAL
BAG × 1	₹99.00
SUBTOTAL:	₹99.00
SHIPPING:	Free shipping
PAYMENT METHOD:	PAY WITH PEERCASH
TOTAL:	₹99.00

fig 8. Order is Done

V. CONCLUSION

This paper has discussed a way of electronic payment system for online based shopping systems. One of the most significant outcome of this project is that we could remove the third parties behind the shopping payment systems and thereby created an fully extension based payment system , which takes trust over the account and shopping websites by providing security in the payment system without moving from the shopping website to external payment gateways.

VI. ACKNOWLEDGMENT

We sincerely thankful to our Principal Dr. P Sreeraj, for providing us the facilities in irder to go ahead in the development of our research. We express our deep and sincere to Dr. Nijil Raj N, Head of Computer Science and Engineering Department, Prof. Yasir A, Project Coordinator and guide Prof. Bindu Sivasankar, for valuable advice and timely instructions.

VII. REFERENCES

[1] SathoshiNakamoto, “Bitcoin: A Peer to Peer Electronic Cashing System,” www.bitcoin.org
[2] VitalikButerin, Gavin Wood, Joseph Lubin, “A Next Generation Application and Decentralized Application Platform”, www.ethereum.org
[3] Ian Grigg, “EOS An Introduction”
[4] David S, Noah Youngs, Arthur Britto, “Ripple Protocol consensus Algorithm”
[5] William Stallings, “Cryptography and Network Security: Principles and Practice”
[6] Alfred Menzes, Paul van Oorschot and Scott Vanstone, “Handbook Of Applied Cryptography”
[7] Chi Sung Laih, “Advances in Cryptology-ASIACRYPT 2003