Decentral : A Decentralized Offchain Banking System

Uwe Cerron, Leo Shao
decentralteam@gmail.com

Abstract

In the absence of trust opportunities can be lost. A typical solution involves trusting a third party to mediate a transaction across parties for a fee becoming the single point of failure throughout the whole process [1]. Almost every sector in the economy that involves a third party runs the risk of loss to the consumer. A purely offchain peer to peer network may allow for trust free trade trust from one party to another without having to register the transactions on the Blockchain. Multiple signature technology may allow for the network to perform the roles of a decentralized arbiter and notary [4], combined with the ability to issue tokens representative of such funds it may provide a trust free mechanism for trade and investment.

The decentralized offchain network allows for the identification and distribution of cryptocoins and metacoins definitions on top of Bitcoin within the network and will only track the last state of ownership of the coins, through this only the last transaction to withdraw coins from the network will be recorded in the Blockchain. Through multisignature technology the network can act as an autonomous escrow agent for decentralized companies and software. Nodes within the network may choose any token integrated within the network as a payment fee for their escrow service. Due to the representation of cryptographic networks as tokens for access to services through decentralized applications we believe the Decentral tokens or “credits” may prove to be a generic token for payment among these networks. Without the need for access to the Blockchain, Decentral is an offchain network for smart contracts and tokens that can be traded with the properties of anonymity, fungibility, the ability to store and accumulate value of a single or a bundle of tokens which with the advent of decentralized applications may represent access to public goods.

I.History

Bitcoin is the first decentralized cryptographic network which has been a major accomplishment of concepts that originated since the 80s. Bitcoin introduced the concept of a proof of work ledger, provided a decentralized consensus protocol to organize transactions and used the proof of work algorithm as a mechanism to confirm them. The Bitcoin scripting system relies on a series of inputs and outputs. Each input is in a certain position, has a value and an address, and has a unique identifying txid number. The outputs can be one or many, and they are a list of addresses and values respectively. Lastly, signing is implemented using public and private keys for encryption which provides for an elegant solution to the ”Byzantine General problem” [6].

Since its inception Bitcoin has been plagued with scams and badly managed services. Examples such as a recent Bitcoin exchange that lost hundreds of millions of dollars are unacceptable. Multisig technology offers a solution to these events. These accounts can be traditionally used as an escrow requiring m of n signatures to confirm the spending of any input, but it may suffer from extortion, collusion, bad judgment, and the usual problems which arise should the third parties be involved.

Multi signature third party services include digitally signing contracts and transactions providing an extra layer of security for transactions, others plan to use it as mediators in the event of a dispute between the buyer and the seller. The arbitration aspect of their role would be to decide the fair outcome of a dispute[4]. However, the system still depends on a centralized entity or service to work as a third party.

As of today there are no decentralized systems in place that can allow for offchain trust free exchange of services without the single point of failure associated with a third party service, users of the service cannot obtain the guarantee that the service provider may not run with the user’s money. It is clear that the Bitcoin ecosystem is trending towards a trust free transactions ecosystem, a trust free entity is needed to escrow funds impartially without the risk of collusion.

This protocol system solves these problems in a very simple and discrete manner which will greatly reduce the risk of loss, allow for trustless smart contracts, and allow trade between perfect strangers even if the parties themselves cannot be trusted and with mainstream adoption it may provide a return on Bitcoin deposits without the risk inherent in a centralized entity. The system would be implemented as a decentralized offchain transaction system to address blockchain based cryptocurrencies need for speed, micro payments through no or low transaction fees and offer a possible investment framework through bitcoin backed tokens.

II.Architecture

The Decentral network will integrate with multiple cryptocurrencies starting with Bitcoin. Each network server will have an option to charge its escrow fee in the desired cryptocurrency of choice. Each server will have a table of colored coins definitions which are recorded in the Bitcoin Blockchain upon issuance, this way each node becomes a decentralized asset definition for the colored coins protocol. We plan on implementing an infinite divisible protocol where the 1 satoshi per token atomicity is no longer in place, but for now the Decentral Network will adopt the EPOBC color kernel.

Using Bitcoin's Blockchain scripting capabilities, the Decentral network can create a special transaction and post it on the Bitcoin network with special instructions that may require 7 out of 10 Decentral network servers to spend this transaction, with each Decentral server storing a private key you would need more than 3 nodes being offline or hacked before being unable to move the funds. For security purposes, an emergency withdrawal address will be implemented in order for the depositors to recoup their funds, by using the nlocktime feature of the Bitcoin protocol which allows for any transaction to be accepted after x amount of time, the funds will be transmitted to the withdrawal address automatically by the blockchain should more than n nodes become compromised or go offline. For metacoins on top of the Bitcoin blockchain Decentral will implement both Colored Coins and Counterparty protocols. Colored Coins provides a way to tokenize Bitcoins by marking transaction

outputs. These protocols do not possess the economic barrier to entry of requiring the purchase of a generic metacoin to buy the issued underlying asset unlike other metacoin protocols issued on top of bitcoin, this makes it an attractive protocol to issue new metacoins or tokens on top of the Bitcoin platform.

III.Protocol

The network will establish a reputation system, which will depend on server uptime, accuracy, reliability, relevance, identity and trustworthiness. The reputation system will not only depend on the money servers have, but on the quality of service each service provides. The protocol will make use of p2sh accounts extensively. If a transaction is broken or stopped from being completed. The users could take their coins back and attempt to transact again.

Proof of Trust

Nodes cannot be trusted to self-report the amount of funds they possess. The network must be able to audit and prove that the node is solvent. Using a combination that consists of proof of solvency [2], proof of guarantee and proof of trust, the network will be able to prove that every node is solvent. The requirements for proof of trust are not computationally expensive, but they must be dependent on the amount of trust a node can provide. A node's trust must be composed on its availability, solvency and security. Trusted nodes will be rewarded with fees from incoming and outgoing transactions.

Proposal for guarantee

In order for a Decentral node to provide a guarantee that it won't run away with a depositor's money they must deposit their own funds which will be held in escrow by the voting pool, this way should the node lose the funds for any reason the depositor gets reimbursed. The Decentral network requires a proof of funds for each and every node, should a node have less bitcoins than they are

supposed to, they will automatically lose their deposit. The amount of money that must go in and out a server must not exceed the deposit at any point in time.

IV.Incentives

Since the network will be comprised of specialized servers there must be an incentive for users to participate on the network. As more nodes connect to the network the difficulty of earning fees per server will vary depending on the quantity of transactions. A free market ecosystem will be established where the right to a node's fees are determined by the market, thus we expect the present value of credits, which represent the node's stream of payments to be calculated following the time value of money principle.

I.Tokens as Credits

Each node is capable of charging a fee on incoming and outgoing transactions, the credits represent access to all streams of payments from a Decentral server. Inherently its value will depend on the amount of payments a node receives. Credits may be traded for the cryptocurrency of choice in order to expand the server's guarantee increasing the amount of money a server can hold, thus expanding its earning capabilities.

II. Tokens as checks

The token may be traded off chain. Providing cheaper and faster transactions when compared to Blockchain based transactions. The token will allow offline usage in a similar manner to a check. The user could have a local checkbook on his phone. When said user wants to buy something locally he could just send message with the appropriate information. Whether or not the money exists will be up to the merchant to verify no different than when paying at any store, the

merchant must make sure that he gets the money and transfer it to a check he owns. In the future, offline transactions may be possible with modification to hardware devices.

III. Alternative uses

A user choosing to create a gambling application could issue a smart contract that was open and properly scrutinized. Anyone could then choose to invest into the application and make the contract only retrievable at the end of the year. This contract could then be tokenized and sold in pieces at any time.

V.Conclusion

We have proposed a system where electronic transactions can happen off chain. Throughout the paper we described and presented the potential an off chain escrow entity can have on cryptocurrencies. Our solution includes a proof of guarantee implemented through a p2sh transaction and a proof of trust. In this paper we have introduces a variety of uses to the network tokens. The universal token or ‘credits’ presented in this paper have all the properties of chaumian cash and the added property for accumulation of wealth throughout time or savings.

References

[1]Justus Ranvier , Lex-Cryptographia,http://bitcoinism.blogspot.com.es/2013/12/lex-cryptographia.html, 2013

[2]Olivier Lalonde, Proof of Solvency, https://github.com/olalonde/proof-of-solvency, 2014

[3] Digital Cash, http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html

[4]Dr. Washington Sanchez, Separation of Notary and Arbitration Services on OpenBazzaar,https://gist.github.com/drwasho/f1e0a9f5826f5cc4186e, 2014

[5]Mike Hearn,Micropayment Channels, https://bitcointalk.org/index.php?topic=244656.0 , 2013

[6] Satoshi Nakamoto, A Peer to Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf , 2008

[7]Gmaxwell, Salvaging refund protocols from malleability attacks with P2SH , https://bitcointalk.org/index.php?topic=303088.0 , 2013