POSITRON

VISIONARY CRYPTOCURRENCY

Positron Anonymous Transaction Technology

Prepared by Cryptowest / Dave McEnery Jr.

Abstract:

Decentralized digital currencies allow for financial transactions to be sent instantly, without the use of third parties, anywhere in the world. The socioeconomic impact that results from this technology changes the way we pay for goods and services. With decentralized currencies, every transaction is recorded in a public ledger called the blockchain. While these are only records of funds being generated, sent, or received; forensic analysis of this data allows for the identities of those involved to be revealed. This is problematic for activists, journalists, and countless others living in oppressive regimes. Positron proposes a solution to this that will make tracing payments nearly impossible. The system will implement a series of “Masternodes” that clutter transactions in the blockchain, creating a unique “Ramchain” technology that allows the ”Masternodes” to get involved with transactions. This will not be a layer on top of the blockchain or a series of mixer nodes, but instead a flurry of inputs in a particular transaction that masks its true destination.

Introduction:

Financial privacy is a highly sought after privilege. Many individuals wish to freely spend (or save) their wealth without the permission, scrutiny, or derision of a third party. Credit poses a problem in this respect, because the money doesn’t exist, and so in order for an individual to have unrestricted control of their finances, they need to own money that has a quantifiable presence in the digital ecosystem.

The usefulness of cryptocurrencies is staggering. Through their utilization, individuals are able to transfer their wealth worldwide directly, without intrusive fees or third party intervention.

Most transactions take minutes, and can happen day or night. Despite a lack of physical presence in our so called “reality”, their digital presence is akin to cash. Cryptocurrencies can be stored in wallets and used to pay for goods and services.

A perfect economic model would allow for absolute trust between all parties involved in any transaction. For example, a customer that wants to buy a snack from a vending machine would be trusted to insert their payment into the money box. Unfortunately, in the real world, people cannot be trusted. Without the locks, payment mechanism, and glass screen securing the snack products and money box, nobody would pay for the snacks as they could be simply stolen along with any revenue collected. Due to situations like these, businesses are forced to take precautions to secure their funds, which naturally incur expenses. For the vending machine model to work, every product and form of money being held in the vending machine must be secured. Also, the coins and single dollar bills collected by the vending machine would need to be taken to a bank, which counts a large amount of coins for a fee. There is no way to avoid giving a bank a significant cut of your revenue. Risk management is a requirement in today’s world, and the steep fees it carries are unnecessary.

Positron eliminates many of the risks and costs involved with doing business. The vending machine will not have to handle any cash or pay any bank fees after receiving payment. The wealth earned goes directly to the owner’s wallet. The vending machine no longer has to be secured to prevent deposits from being stolen, which substantially reduces the risk of theft. There are no costly electronic banking devices required, and the risk of a chargeback being initiated is no more. The consumer also has options. If the snack is stale, they can provide proof of their payment on the blockchain showing they paid for it, giving them the opportunity to be compensated.

The global economic impact of paying for products or services internationally amplifies the utility of cryptocurrencies. Traditionally, there are currency conversion fees, waiting periods, privacy concerns, bank fees, and other inconveniences. Cryptocurrencies are absolved of these problems. The only issue thus far is making cryptocurrencies as common world-wide as physical cash is today. This document will attempt to present a solution by explaining a new form of anonymous technology called Positronium.

What is Positronium?

Positronium is the underlying technological core of Positron allowing it to host a blockchain with a diverse amount of inputs, making it nearly impossible for one to distinguish the two parties involved in a transaction. This technological aspect was developed exclusively for Positron, an *anonymous technology that is designed to clutter the blockchain with so many inputs, it is nearly impossible to find who is sending coins to each other.* Created specifically for the Positron digital currency, the intention is to give an optional layer of privacy to user transactions.

Our long term goal with Positron is to help crowdfund projects with blockchain technology to the public, and develop new cryptocurrencies for people with only the most brilliant and innovative ideas. Backing and funding projects with cryptocurrencies has monumental potential. This will not be a cookie cutter factory of cryptocurrencies, it will be the cream of the crop. Only the coins we truly believe in and truly expect to succeed will have a prominent position in the Positron network.

Project choice will be voted on by TRON masternode owners, official TRON artists, official developers, and the community.

Future Goals of Positron

Positron encourages development of new open source cryptocurrencies that improve upon each other with new features. This encourages the sophistication and improvement of cryptocurrencies as a whole. This is similar to the current system employed in academia, where graduate students are tasked to pursue a relatively unknown topic. Upon completion of a series of experiments, their results are scrutinized by senior members with graduate degrees. Based on whether they have contributed useful and truthful results, they are given graduate degrees themselves which allow them to pursue other topics of interest. When many people earn graduate degrees, the community has more insight into the field than previously. With the TRON crowdfunding platform, we will be able to have a similar system where developers are constantly trying to improve the technology behind cryptocurrency and perfect it to the point where it becomes easy to use and secure. The amount of developers that carry empty promises in order to turn over a quick profit will be significantly reduced and the field of cryptocurrency will generally move towards a more advanced state.

Document Scope:

This is not a marketing brochure or invitation for investment. This document exists for educational and technical purposes only. If there are examples that begin to discuss economic or ideological issues, it is for context only. In the following sections, certain objects will not be citable, as this document explains original development. If certain sections are left wanting, the development team behind Positron can be contacted directly.

Definitions:

RAMCHAIN: Communication protocol designed for Positron that allows peers to communicate information to masternodes. This allows individuals to initiate transactions with others, by finding a masternode and showing it a list of inputs and outputs.

MASTERNODE: These special nodes are created by individuals who want to assist in creating anonymous transactions. They can be found by

INPUTS: An input is a reference to an output from a previous transaction. Multiple inputs are often listed in a transaction. All of the new transaction's input values (that is, the total coin value of the previous outputs referenced by the new transaction's inputs) are added up, and the total (less any transaction fee) is completely used by the outputs of the new transaction. Previous tx is a hash of a previous transaction. Index is the specific output in the referenced transaction.

(from Bitcoin wiki: https://en.bitcoin.it/wiki/Transaction)

OUTPUTS: An output contains instructions for sending bitcoins. Value is the number of Satoshi (1 BTC = 100,000,000 Satoshi) that this output will be worth when claimed. ScriptPubKey is the second half of a script (discussed later). There can be more than one output, and they share the combined value of the inputs. Because each output from one transaction can only ever be referenced once by an input of a subsequent transaction, the entire combined input value needs to be sent in an output if you do not wish to lose it. If the input is worth 50 TRON but you only want to send 25 TRON, will create two outputs worth 25 TRON: one to the destination, and one back to you (known as "change", though you send it to yourself). Any input bitcoins not redeemed in an output is considered a transaction fee; whoever generates the block will get it.

(from Bitcoin wiki: https://en.bitcoin.it/wiki/Transaction)

TRANSACTION: A transaction is a transfer of Bitcoin value that is broadcasted to the network and collected into blocks. A transaction typically references previous transaction outputs as

new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction collected into a block.

Standard transaction outputs nominate addresses, and the redemption of any future inputs requires a relevant signature.

All transactions are visible in the block chain and can be viewed with a hex editor. A block chain browser is a website that lists every transaction included within the block chain in a user friendly interface. This allows anyone to view the technical details of transactions in action and for verifying payments.

(from Bitcoin wiki: https://en.bitcoin.it/wiki/Transaction)

Requirements for a successful anonymous transaction:

- There must be no risk to the individual who initiates a transaction (the sender) of theft or fraud of their coins.
- Must not benefit certain users, above what is already promised for running masternodes.
- Must be user friendly for mass adoption by the public.
- Sending coins anonymously must be optional.
- Must not cost the user any hidden fees beyond what is required to pay the network transaction fees.
- Must not cost a significant amount in transaction fees.
- Must not exclude any specific individual from participating from using Positron anonymous technology.
- Must not compromise the speed and security of the network, or end user's hardware.
- Transactions must be truly anonymous. They must not be easily traced back to the sender.

Example of anonymous transaction taking place:

Frank wants to send Maria 100 Positron coins.

Frank chooses the “Positronic Anonymous Send” functionality in his wallet, and enters Maria's receiving address.

Frank's wallet creates a large amount of sending addresses, each primed to send 100 coins to another batch of receiving addresses his wallet creates. In this list, only one of the receiving addresses really belongs to Maria.

Frank's wallet does a broadcasted scan of the network in order to find a Masternode. Once he receives a response, his wallet communicates his list of inputs and outputs over the Ramchain protocol. The Masternode does not know who the real receiver is; only Frank knows. The payment is mixed with a large list of other addresses that send the same amount of coins to his wallet.

The Masternode prepares the transaction by creating an even larger list of send addresses primed to send 100 coins to receiving addresses it creates.

At this time, the Masternode sends another broadcasted scan through the Ramchain, finding another Masternode who will repeat this process.

This method continues until many Masternodes have prepared hundreds or even thousands of inputs.

This whole process can take approximately 30 seconds, depending how many Masternodes are active.

Once the Masternodes have created enough inputs, they respond back to Frank's wallet, and his coins are then sent to Maria’s receiving address in the same transaction as the other prepared inputs.

Since the Positron maximum block size is only 40 megabytes, many inputs can be loaded into a single transaction. Anyone attempting to find the real transaction will have to sift through thousands of inputs that all look like the real one.

THREATS:

Listed below are possible threats to the Positron Anonymous technology.

Threat 1:

Every input but the actual destination is a fresh address, making it easy to tell who the actual receiver is because his address has transaction history.

Response: *This is easily evaded by having the receiver create a new deposit address. This can be done on most exchanges, and with any Positron wallet. Masternodes will start to recycle some of their freshly made receiving addresses over time in order to throw this off, so this issue will become less of a threat. It should be considered a "best practice" to always send to a newly created receiving address.*

Threat 2:

Malicious individuals fill the 40 megabyte block size with trash inputs. No room is left for the Masternodes to create multiple inputs.

Response:

*This would require an enormous effort. The Bitcoin network is only starting to see this as a concern, as their network is starting to see block sizes approach their 1 megabyte limit(**reference**). **Do keep in mind their block generation times average 10 minutes, whereas Positron block generation is targeted at 1.5 minutes. Positron's maximum block size is 40 megabytes, so combined with faster generation times, a malicious user would need to 'spam' a block with 40 times more data than the Positron network, in 1/7th the time. The worst case scenario is that the Masternodes are not able to complete their work, and coins are never sent. The sender will have to wait 2 minutes and try again.***

While having such a large block size could have long term negative effects on the blockchain, it does not fit into the scope of this document.

http://bitcoinism.liberty.me/2015/01/21/economic-fallacies-and-the-block-size-limit-part-1-scarcity/

Threat 3:

The Masternodes are attacked with Distributed Denial of Service attacks (DDOS).

Response: *If every Masternode was attacked and not able to communicate with individuals looking to send coins anonymously, the Ramchain would fail to initialize and the transaction would never start. Coins would not get sent, and the individual would have to either wait for the Masternodes to come back, or send to the receiver without any cluttering.*

Threat 4:

Positron blockchain is attacked and forks.

Reponse: *This is a valid threat. Despite Positron checkpoint servers, it is still possible for an individual to maintain coin control dominance by obtaining over 50% of the coins and building stake age, while blacklisting their connection to certain nodes. This has a small chance of creating a different chain. The probability of this happening is very low, and would only affect parts of the network before the checkpointing server fixed the fork.*

Threat 5:

Masternodes do not do their job properly and no 'cluttering' takes place.

Response: *If the RAMCHAIN does not initiate any cluttering, the transaction will not take place. The sender must now choose to send the coins without use of the anonymous technology.*

Threat 6:

If an individual sends all their coins in one transaction, there are not enough coins left to initiate multiple inputs to pass along to the Masternodes.

Response: *This is an interesting threat. If the sender used the anonymous technology in the past, their coins are most likely already distributed into a variety of inputs from their wallet sending coins to multiple fresh receiving addresses. This will combine all their inputs into one large transaction, and the Masternodes will mimic this, creating even more of a mystery on the blockchain. Currently, the anonymous technology requires at least 3 inputs, so a transaction will fail if a fresh wallet address is created that holds all of the coins.*

Threat 7:

Malicious user obtains a Masternode for the sole purpose of identifying senders.

Response: *While this is always a concern, the Masternodes themselves don't know who the actual receiver of a transaction is. The malicious user will be able to find out who started the send, and will know the list of inputs it is sent, which will narrow the spectrum a bit. This is of course, if the malicious user is the first Masternode to receive the list of inputs from the sender.*

Summary

Positronium is new technology, built specifically for Positron. It is not a layer on top of the blockchain, nor does it mix coins. It simply protects the sender and receiver from being identified. There is very little threat to the end user or the network, and this service is optional. Individuals that make use of this technology to send coins will leave an enormous web of inputs on the blockchain, making it nearly impossible to find who the receiving party is. This allows Positron to be circulated like 'digital cash' be it for online or face to face transactions.

NOTES: The lead writer is still working on this and considers it incomplete. I'm releasing what's been edited so far. There will be an update soon.