DESIRE

CRYPTOCURRENCY

What is Desire?

DESIRE is a new P2P digital currency designed to unite all not indifferent people for earnings, exchange and transfer of money to any point of the world, bypassing centralized payment systems.

Instant transactions, anonymity is an undeniable advantage of this currency. To ensure your anonymity uses the mixing technology, which makes it impossible to track the sending and receiving destinations.

DESIRE

MasterNode’s

One of the struggles with Bitcoin's public ledger known as the blockchain is that coin's aren't fungible. Once a coin hit's the network it's entire history can be traced forward or backwards. For the sake of the discussion we describe Bitcoin as a single tier network (much like a wired network with no vlan's) and we describe DESIRE as a multi tier network. This is an important distinction. The base of this multi tiered approach lies in the hands of network clients called Masternodes . In the crypto-currency world we consider a network client a computer with the wallet software running. In terms of Bitcoin all clients of the network are considered equal. The more nodes (or clients) up and available to communicate the stronger the mesh of peer to peer connections is for broadcasting transactions, mining blocks, and coming to a consensus on the ledger. The power of DESIRE comes from a rudimentary adjustment to this basic premise of all clients on the network are created equally. Inside the DESIRE network clients that have had a single 1000 coin deposit can then in turn attach themselves to another node on the network forming a Masternode bond between their local wallet (with the 1000 coins) and the node on the network with no coins but a full copy of the DESIRE software running and responding to clients on the DESIRE network. Just like the server hosting this webpage is running software that allows your browser client to talk to it and serve it webpages these Masternodes perform services to support and strengthen the DESIRE network. The reason for developing this Masternode connection between a local node and a remote node is done for security and reliability. This allows the 1000 coin deposit to remain locked in place and secure. It doesn't have to remain online and accessible it can be safely put away until needed. It also allows the computer responding to client requests on the DESIRE network to be at a high bandwidth facility. This makes Masternode’s highly available and extremely accessible to DESIRE network clients. Once a wallet has been loaded with a 1000 DESIRE and started as a Masternode as long as it remains healthy and responsive to the network for a set period of monitoring it will eventually get entered into the main Masternode list. This is a list of nodes that have all passed this Proof of Service test and that are considered healthy for the network to rely on to sign blocks, relay messages and provide tier two services like fungibility protection. At this point there is two proof of concept offerings for Masternode’s that have passed this Proof of Service test. These are InstantX and Darksend or what some like to simply call Mix.

Instant X

By utilizing Masternode quorums, users are able to send and receive instant irreversible transactions. Once a quorum has been formed, the inputs of the transaction are locked to only be spendable in a specific transaction, a transaction lock takes about 4 seconds to be set currently on the network. If consensus is reached on a lock by the Masternode network, all conflicting transactions or conflicting blocks would be rejected thereafter, unless they matched the exact transaction ID of the lock in place.

This will allow vendors to use mobile devices in place of traditional POS systems for real world commerce and users to quickly settle facetoface non commercial transactions as with traditional cash. This is done without a central authority.

DESIRE

Private Send

PrivateSend is the feature that gives DESIRE user's full privacy when they use it. It is an improved and extended version of the CoinJoin. In addition to the core concept of CoinJoin, we employ a series of improvements such as decentralization, strong anonymity by using a chaining approach , denominations and passive ahead of time mixing.

By having a decentralized mixing service within the currency we gain the ability to keep the currency itself perfectly fungible. At the same time, any user is able to act as an auditor to guarantee the financial integrity of the public ledger without compromising others privacy.

PrivateSend uses the fact that a transaction can be formed by multiple parties and made out to multiple parties to merge funds together in a way where they can’t be uncoupled thereafter. Given that all PrivateSend transactions are setup for users to pay themselves, the system is highly secure against theft and users coins always remain safe. Currently to mix using PrivateSend requires at least 3 participants.

To improve the privacy of the system as a whole we propose using common denominations of 0.1 DESIRE, 1 DESIRE, 10 DESIRE AND 100 DESIRE. In each mixing session, all users should submit the same denominations as inputs and outputs. In addition to denominations, fees should be removed from the transactions and charged in bulk in separate, sporadic unlinkable transactions.

PrivateSend is limited to 1000 DESIRE per session and requires multiple sessions to thoroughly anonymize significant amounts of money. To make the user experience easy and make timing attacks very difficult, PrivateSend runs in a passive mode. At set intervals, a user’s client will request to join with other clients via a Masternode. Upon entry into the Masternode, a queue object is propagated throughout the network detailing the denominations the user is looking to anonymize, but no information that can be used to identify the user. Each PrivateSend session can be thought of as an independent event increasing the anonymity of user’s funds. However each session is limited to three clients, so an observer has a one in three chance of being able to follow a transaction. To increase the quality of anonymity provided, a chaining approach is employed, which funds are sent through multiple Masternodes, one after another.

Join the cryptocurrency desire, today . . .

DESIRE