CryptCoin: An Innovative System for Fully Decentralized, Anonymous Transactions With A Unique Method of Public/Private Key Broadcasting

Draft, Rev. 01
(CryptCoin development team -- http://cryptco.org)
05/26/14

Abstract

CryptCoin is a new breed of Anonymous cryptographic currency based on X11 hashing algorithm with ongoing Proof of Work mining and sustained Proof of Stake minting, While other anonymous and pseudo-anonymous crypto-currencies take advantage of 'masternodes' and 'mixers', CryptCoin utilizes a more egalitarian way of anonymizing transfers from point A to point B, without charging users a fee for the feature.

Introduction

CryptCoins anonymous send function strives to be the industry standard amongst the other leading anonymous crypto-currencies on the market. Our team has been dedicated to creating a unique anonymous transfer method that has been demanded amongst the crypto community as a way to fill the void left out by Bitcoin. Our adversaries have come up with somewhat “anonymous” methods,

which use a centralized, “master node” system - we will stand out as the one and only unique fully autonomous anonymous design, *with no centralized control or monitoring*.

Specifications

Block Time: 90 seconds
Stake Interest: 2.75% per annum
Secure and Open Source

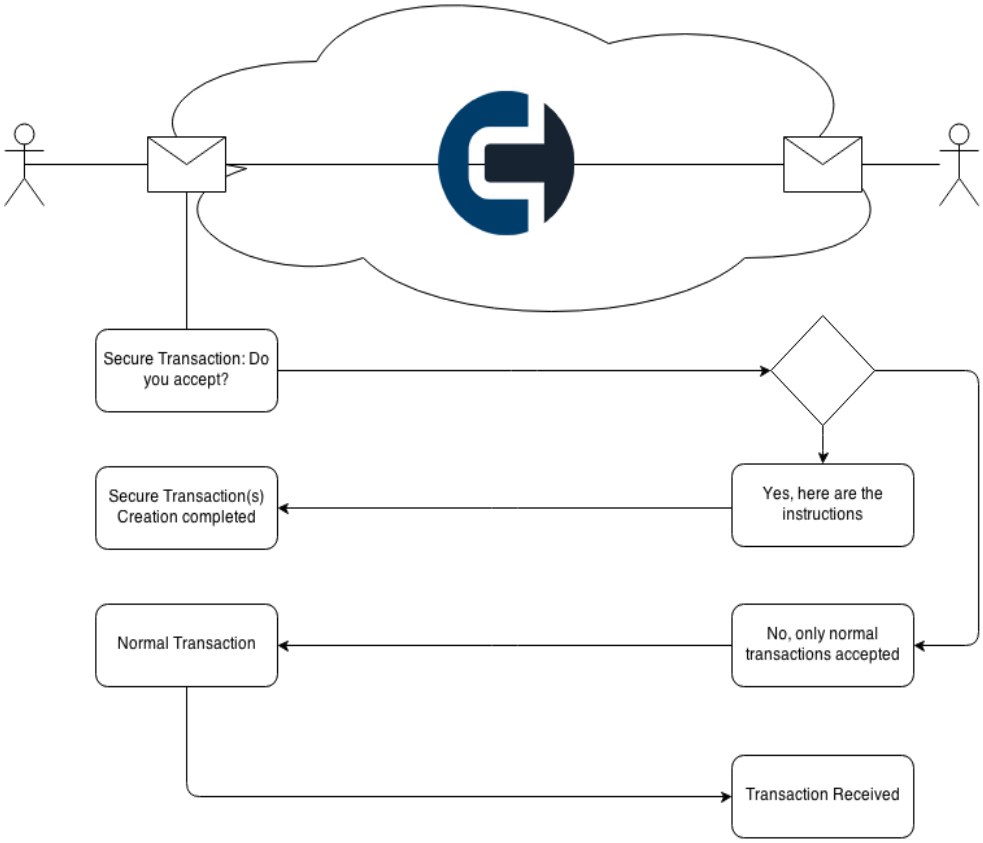
Distribution:
X11 Algorithm
Total Coins: 11,000,000

Block Rewards:
Block **1** to **2000**: 500
Block **2001** to **4000**: 250
Block **4001** to **12000**: 125
Block **12001** to **48000**: 62.5
Block **48001** to **368000** 31.25

Coin Minting and Mining

Cryptcoin utilizes a hybrid system of Proof of Stake and Proof of Work (x11) This ensures maximal blockchain integrity and ensures CryptCoin is highly energy efficient by making use of the reduced energy draw and heat output via the X11 hashing algorithm and little to no cost for operating a node via staking as well as incentive via minted coins by offering a stake interest of 2.75% per annum.

CryptCast: Decentralized, Anonymous Transactions via Public/Private Key Broadcasting



Please note that this is a simplified brief of the anonymous transaction feature. It is currently working in testing mode - upon release, a much more detailed technical explanation will be distributed. This is currently meant as a timely update for our current and future investors.

CryptCast Summary

Our flow-chart is meant to represent Cryptcoins unique anonymous transaction method. This method is currently one-of-kind and not found in any other cryptocurrency. It has been built from the ground up amongst our team of expert dedicated professionals. The anonymous send is innovative in the fact that its function requires no active ‘masternodes’ that require coins or partially anonymous mixers. Even with triangulation no one would never know who the owner of the public key is, capable of decrypting the message; it’s fool-proof and innovative. There will be NO fee for sending transfers as there are no masternodes that require payments. Transactions occur ONLY between two wallets with full decentralized anonymity. With the exemption of central masternodes from this anonymous system we have created a far more superior and free of charge based method of anonymous currency transfers.

CryptCast Synopsis

- Wallet A wants to send an anonymous transaction to Wallet B.
- Wallet A (sender) encrypts a message towards Wallet B (recipient) by using private/public key concept, with Wallet B's public key.
- The message is broadcasted through the nodes connected to Wallet A, and will reach Wallet B via the broadcasting system that already exists in the Bitcoin protocol.
- Wallet B is the only one that can decrypt the message with Wallet B's private key.
- Wallet B receives the request for secure transaction from Wallet A.
- The message contains the total number of transactions that are capable of transmitting, and the total amount of coins.
- E.g., if Wallet A wishes to send 3 transactions and Wallet B accepts it, it returns 3 new addresses (encrypted message with pubkey of wallet A.)
- The message is again broadcasted till it reaches wallet A.
- Wallet A decrypts the message, receives the new addresses and creates 3 transactions for each IN transaction it has, sending them to each new address it got from the new wallet.
- Multi-transaction time-delay will be optional for maximum anonymity if speed is not required.
- If Wallet B does not accept any type of secure transaction, it encrypts again a message with decline response
- Wallet A then has the option of sending plain, non-secure transaction, or to not send it at all.

References

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient).
(http://www.links.org/files/decentralised-currencies.pdf)

S. King (2012): PPCoin: Peer-to-Peer Crypto-Currency with Proof of Stake
(http://www.peercoin.net/assets/paper/peercoin-paper.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.
(http://www.bitcoin.org/bitcoin.pdf)