Fluttercoin: A Peer-to-Peer Electronic Currency with Proof-of-Transaction

TheKidCoin
(thekidcoin@gmail.com)

March 3rd, 2014

Abstract. One of the descendants of Bitcoin, Fluttercoin sets itself apart as the first crypto-currency to provide transactions as a proof of participation. Proof-of-transaction adds an additional layer of blockchain and transactional security by allowing economic participants to prove they were involved in a transaction. This system verifies the coinbase of every proof-of-work block, and validity of a proof-of-transaction reward or lack thereof. The result, secures the blockchain as all unmodified nodes will reject invalid blocks that should or shouldn't have included a proof-of-transaction rewards.

Introduction

Since the inception of Bitcoin, mining reward has been reserved for the miner. Miners as of this writing range from individuals to corporate operations, and require specialized hardware and energy consumption to solve proof-of-work blocks. This system effectively eliminates most individuals from participating in mining, and instead forces them to participate through investment, gifting, or payment acceptance.

Another issue with the current model is the possibility that an attacker can modify transaction order or data via 51% attacks or similar. While there have been improvements to Bitcoin's system, most notably Proof-of-Stake minting, it does not go far enough.

Proof-of-transaction sets out to solve both issues.

Proof-of-Transaction

Proof-of-work, introduced with Bitcoin provides the initial catalyst for mining and spending coins, and it is later replaced to an extent by Proof-of-stake, which provides rewards for securing the network through proof of coin ownership.

With the advent of Proof-of-transaction, we now allow adopters the network to generate partial proof-of-work mining rewards in return for verifying their participation in the previous block's transaction record.

In addition, proof-of-transaction adds a layer of security by eliminating the possibility to re-order or modify large chains of block transactions because doing so would possibly cause a block to be rejected by all other behaving nodes, resulting in the attacker effectively forking onto their own incompatible blockchain.

Proof-of-Transaction Reward Generation

Proof-of-transaction rewards are decided essentially on acceptance of a new block by the network. On each block, the previous block's transactions, and each address contained in said transactions, within the system parameters, are evaluated for a reward by comparing each address to the previous block's hash.

Take for example a block with 2 addresses included in a transaction that sent 1000 Fluttercoins from one Jack to Jill:

Previous block hash:

0000001ca505f2ebf7417a2be81b027c2f6fb6bee300c82e06c4b393d312b0ef

Jack's Address
FH2DRtWHQ5FfP2LeCWEteqvZKbunSfVqS1

Jill's Address
FRwNpW6e59SVhJqmZXFyPLRGFkwihBJvfB

We first start by converting each address we evaluate into a hex format, until either all addresses have been evaluated, or a match is found:

Jack's Hex Address:
6d74453438706a724d375378396b4a616375697175 4d354667697771 4a3147526179

Jill's Hex Address:
7s098a37636f9a878076336b4a8760737d18378737673a7126f763707b8262c376c2f

If the above example, the search term for each above address is as follows:

Jack's Search Term:
179

Jill's Search Term:
c2f

Each exact term is used to search for a match in the above previous block's hash:

Jack's Search for 179 in 0000001ca505f2ebf7417a2be81b027c2f6fb6bee300c82e06c4b393d312b0ef
Result: false

Jill's Search for c2f in 0000001ca505f2ebf7417a2be81b027c2f6fb6bee300c82e06c4b393d312b0ef
Result: true

The result is a match for Jill's search term, resulting in Jill's address FRwNpW6e59SVhJqmZXFyPLRGFkwihBJvfB being rewarded 50% (2500 Fluttercoins) of the next block's proof-of-work reward of 5000 Fluttercoins.
In order for the above block to be accepted by the network, the search is done on each node accepting the block, looking particularly for the coinbase size, coinbase reward, and address involved in the coinbase. If there is any deviation, which would happen through re-ordering of transactions or modification of transactions, the block is rejected by the network.

Additional Consideration of Proof-of-Transaction

One of the considerations in implementing something like proof-of-transaction is the fact that there are those who would seek to exploit this system for their gain. Measures were put in place to prevent such automated spamming of the blockchain for this purpose. They include parameters which as of this writing set a transaction value greater than 500 Fluttercoins, maximum transactions of 10 per block, and a maximum number outputs per transaction of 10. In the case of transaction outputs, if the limit of 10 is exceeded, only the first 5 outputs are considered. These measure and all future measures with regard to proof-of-transaction seek to eliminate the possibility of simply flooding a block with transactions sending to many addresses in the hopes of mining a proof-of-transaction reward.

Conclusion

It is my hope that proof-of-transaction will provide an additional layer of security, while also allowing participants in the economy to unknowingly participate in securing and being rewarded for their adoption of Fluttercoin as an electronic currency.

Acknowledgement
I would like to thank all the adopters and supporters of Fluttercoin, as well as those without whose brilliant work this project wouldn't be possible, including but not limited to the developers of all crypto-currencies before Fluttercoin.