**FlowCash: A Market Based Public Ledger**



Antony Vaknin

Antony@FlowCash.org

[www.FlowCash.org](http://www.(name).org)

**Abstract.** Recently, bitcoin and altcoins are becoming more and more centralized due to ASIC, DPoS and increased block size. In this paper I will present a new way to achieve the same ends while being more decentralized and arguably more secure. FlowCash has a novel way to decide when and what block to add to the blockchain which uses price system and biding to add blocks. By Defying a cost for data on the chain and letting block assemblers propose blocks that declare how much are they willing to pay to account T to include it in the chain create a market that is much more efficient than PoW and PoS and adds only the most valuable blocks to the chain. It is less susceptible to attacks cause an invalid block will be discarded and the amount the attacker paid to add the block will be taken as punishment for spamming the network making the attack very costly.

**1. Introduction**

Bitcoin was envisioned by Satoshi to be a peer to peer cash system that is extremely decentralized having each user storing the chain and mining using his CPU. As the difficulty of mining increased mining became more centralized with pools and GPU mining. Than came the age of ASIC where most of the hashing power of the network being centralized in a few mining pools. Other projects tried to solve this problem by employing different hashing algorithms (e.g. Ether hash) or moving to Proof of stake which is less susceptible to this problem. That led to the problem of nothing at stack where users can vote on 2 different versions of the truth with no effort undermine the very thing blockchain was design to solve. Another popular solution is DPoS where token owners vote who gets to mine blocks making the system more efficient and usable by losing some degree of decentralizing. No project is focused on making a system that is based on the ability of the average user to host the blockchain. The biggest limits when it comes to p2p systems are bandwidth and storage, the common user doesn’t have a 170GB of storage to keep the whole blockchain on his computer and ultra-fast connection to sync that amount of data. All solutions so far try to balance within this constrains with Bitcoin being very bandwidth light needing to sync every 10 minutes to Ethereum 15 seconds and to some project trying to achieve few seconds to fractions of a second block time. Bitcoin’s other major problem is the high cost of mining consuming about 60 TWH per year and growing with no real value.

1

**#.Transactions, Records & Account’s Rules**

The types of data that can be submitted to be stored on the chain are:

1. **Transaction** – an order to transfer money from account X to Y. contains at minimum sender recipient amount time and signature. Changes the state of accounts balances, data will be discarded after compression block is found. Minimum cost per byte 0.0001 FlowCash
2. **Account Rules**- limits on account such as: minimum cost per byte 0.1FlowCash
   1. Specific block assemblers that are allowed to transfer money from the account
   2. Max amount to be transferred at once/per day
   3. Sidechain accounts that keep the money of sidechains and allows users to move from chain to chain without having to exchange the coin since the sidechain have 100% reserves.
3. **Record**- There are many kinds of records: minimum cost per byte 0.1 FlowCash
   1. **Maps to Accounts** - every user can purchase a map to his account in order to make it easier to use the protocol and save on transaction size (e.g. account T stands for *Treasury* the account to witch block assemblers send their bids to)
   2. **Custom Maps**- any user may want to declare a map for useful things such as links, IPs, DHT, standard account rules, assembler groups and more.
   3. **Other Data**- publishing text or other information that cannot be censored and accessible to every FlowCash user.

**#. Limits that Constructs the Market**

In order to make the Proof by Market function there has to be scarcity of space on the leger that the block assemblers will have to compete for. Public leger space is extremely valuable since its redundant, accessible anywhere the problem however is that the larger it gets the fewer people that will have a copy of it. FlowCash strives to be as decentralized as possible meaning having as many full nodes to provide redundant and censorship resistant service. For that reason the size of the blockchain is allowed to grow at a steady rate that will allow most users to use the whole chain.

The amount of growth allowed to the ledger will be voted by all currency holders at the time independently or by representatives with a liquid democracy mechanism.

**#.Liquid Democracy**

Since all accounts on the system that hold funds on the main chain have to be registered on the blockchain and on the accounts map one necessary attribute will be the to choose a representative to vote on its behalf this is a right granted to any account size proportional to its holdings. The right passes from any account to any account that it may mark. The votes will be casted on the blockchain addressing budget proposal of account T and laws and blockchain changes. Account may choose to cast the vote to T account making it blank.

**#.Proof by Market**

In FlowCash the way to add blocks to the chain is proposing a block. Block size is limited by the holders power while allows the chain to have dynamic block time intervals and size. The holders will target specific growth of blockchain size per day as they may see fit. There is also a minimum price per byte that every valid block must pay to enter the chain in order to prevent spam during time that their aren’t enough transactions or records to add to the chain. In case of very high demand as seen on bitcoin during January 2018 the votes may choose to authorize a temporary change to allow super large blocks to ease the delay time in times of need.

**#.Blockchain**

The technical form and structure of the block chain are not decided yet in my view a combination from a few projects and the new concepts on this paper will allow programmers to execute the concept. The account structure I have found most useful as reference is of Ethereum. Governance and budgeting example is the dash.

**#.Fork Prevention**

The key innovation in FlowCash is the proposal of blocks buy paying to add them to the treasury. This creates a strong incentive not to propose invalid blocks which will result in lost of funds to the abuser and will result in negligible spam and much more effective use of bandwidth and space. When forks do occur the chain which will hold most fees to treasury will be included. It is always possible to defeat an invalid block by including its fee as punishment for spamming. The fee that was included in the block proposal is the amount of punishment that a spammer would pay since it’s a valid transaction that is non reversable

**#.Sidechains & Shredded Chains**

Using the platforms accounts rules an account can be created for whole blockchains that will hold the users founds and allow for more throughput and innovation. This system will allow sidechains to transfer funds according to different base rules (higher speeds, delegates and more) while sharing the same monetary base. Ideally the FlowCash main chain will be used for storing universal data and allow for moving funds from chain to chain. FlowCash main chain cannot be decentralized if all users will use it for buying a cup of coffee or other small transactions but the monetary system that will sit on top of it will allow those transaction to accrue on sidechain denominated by FlowCash tokens.

**#.Probabilistic Payment**

In order to allow micro and pico payments which are needed for the IoT a new kind of transactions that will on the one hand do the payment immediately and on the other wont take space on the chain. The transaction is done by the receiver picking a number of large size hashing it and asking the sender to pick a number and sign then the receiver checks if the number he hashed qualify to win with the number the sender choose. If it did he would send the transaction with the number unhashed to be included in the blockchain. E.g. instead of paying 1 cent per video you may pay 5$ with the probability of 1:500 saving 499 transaction in the chain.

**#. Institutional Account**

It may be useful for many non tech savvy users to still have institutional accounts similar to checking accounts today with regulation and rules of their home countries. This users will have an account with an institution who has a chain account and their money will be guarded by the institution they may choose. The short comings would be in ability to vote and less secure claim for the funds while the positives will be much more similar experience to banks and credit cards that users are used to. A possible solution to deal with the negatives may be a court on chain.

**#. On Chain Judicial System**

By using the voters as the legislative power and the chain as the executive power it seems logical that if the chain where to have complex rules that a dispute resolving system may be needed. I propose a system that will solve 3 big problems that have no solution to date.

* Losing A Privet Key- there are many accounts on blockchains today that are locked forever because of this very problem. The solution involves the user registering in advance hashes of identification documents and the court will judged the claim based on the user posting the data unhashed. Another solution involves the **AutoRecovery** system.
* Buyers protection – a transaction may include a condition that its reversable by court rule.
* Exchanges and institutional fraud- their accounts will be subject to the court review by any claim of users. This will allow the users to have protection.

The structure of the judicial will be determined by the voters.

**#. AutoRecovery System**

Any account not in use for 5 years will be deleted any user may post to the chain a hash of a claim that he is the owner of the account in order to prevent first to file problem a few block later he have to post the claim. In order to prevent theft the claim includes a 10% deposit that will be confiscated if the claim was submitted very close to another with an older hash. In order to prevent spam the owner may post a transaction to himself signed with his key that will cause the claim to be nullified and trigger the deposit to be added to the account causing the thief financial damage.

**#. Account T**

In the above passages I referenced account T which stands for the treasury account. The treasury has no voting power and it serves as the treasury of a country would. A major problem with blockchain ICOs and mining is that they serve the very first people in the expense of later users this not the case here. The treasury will work in order to satisfy both current holders by investing in projects and budget proposals and will be obligated to prevent exchange rate manipulation to the best of its ability in time of lack of liquidity or bubble territory subject to rules, court opinion and institutional ability to hold reserves in trust of the treasury.