VF CASH, a Lightweight, Instant, and Free Peer-to-Peer Electronic Cash System

James William Fletcher
james@voxdsp.com
http://vfcash.uk

1. Introduction

The introduction of Bitcoin in 2009 has revolutionised commerce on the Internet [1]. No longer does the Internet rely exclusively on financial institutions serving as trusted third parties to process electronic payments. While the Bitcoin network works well enough for most transactions, it still suffers from the inherent weaknesses of its Proof-of-Work system [2]. Complete decentralisation is not entirely possible and, furthermore, mining pools and mining hardware manufacturers have taken a monopoly over the bitcoin peer-to-peer cash system to such an extent that, although it is a matter of debate, transactions can be considered potentially reversible [3]. What is needed is an electronic payment system whereby all nodes in the network have an equal say and an equal reward, and no node is rated any more trustworthy or reputable than another.

In this paper, I propose an IoT friendly solution to Proof-of-Work featuring free transactions, mined distribution, no increased risk of network spam, and a private decentralised network where only coin holders can access the current or past state of the blockchain.

2. Transactions

Transactions are stored in a minimal implementation unordered chain; this is commonly referred to as a directed acyclic graph (DAG) among cryptocurrencies [4].

Each transaction has a unique identifier, sender address, receiver address, amount sent, and a signature generated from the transaction structure data. Transaction structures in the final blockchain produce a blocks.dat file that is approximately 76.16% smaller than the equivalent produced by Bitcoin-Core.

Transactions are limited to a maximum value of 4,294,967.295 VFC per transaction. One VFC is a collection of 1,000 vfc units called ‘v’ (1,000v), this gives VFC three decimal places of divisibility.

$$1\ VFC = 1,000v$$
$$0.001\ VFC = 1v$$

The movement of VFC across the network can be tracked; timestamps and dates for the transfer of VFC are not specifically logged by the VF Cash client, although a rogue node in the network can make these kinds of logs. Due to the private nature of the network and the often convoluted block replay transfers causing potential shuffling of the transaction order over time, it would be safe to say that unless someone had made some sort of circumstantial reference logs in the past, then deducing past order of transactions down to specific timestamps would be near impossible.

Double spends are prevented by introducing a three-second transaction delay on all VFC that moves through the network. During this mandatory three-second interval, any double-spend attempts from a single address are thwarted. VFC always moves through the network at three-second intervals. While it is possible for many VFC transactions to move at three-second intervals simultaneously, no single transaction of VFC can ever exceed this limit, and no address may ever send two quantities of VFC to two different addresses within the three-second confirmation period. This significantly reduces the impact of spam on the network while also securing it from double-spend attacks.

In the event of a double spend, both transactions from the sending address are canceled while they are within the three-second confirmation period. Double-spend attacks on the network are recorded allowing node operators to track offending addresses and target receiver addresses.

3. Unordered Transaction Chain (UTC)

No particular order among transactions is required in the transaction chain. This is because only the final balance of an address must be known and not the transaction order from which it came to arrive at this final balance. The only circumstance when an unordered chain impacts upon the system negatively is caused by transaction replays.

A transaction replay that is not played back in the original order will need to be replayed a few times before it arrives at the destination node. This factor increases as the number of transactions on the UTC increases. Transaction replays happen at the master server and a user defined amount of other peer nodes on the user's command. Once a user is fully synchronized, it is unlikely to fall out of sync suddenly unless experiencing any downtime from the rest of the network. All nodes can fully synchronize with the network reliably over time without any major delays.

4. Network

The network is a private decentralised network, which means that access to the network is very limited for users who do not prove that they control a wallet containing VFC. Proof that a user controls VFC is exhibited by the user sending a valid transaction to one of the network peers, thus indexing your IPv4 address as a fellow network peer. Information about the network is only available at the discretion of a network peer, and peers are free to make the entire blockchain or peer list open to the public, while such a policy may not be advisable. If a node has zero network peers the initial transaction will have to be sent to the publicly known master server as this is the only entry point for new users without tracking down a node operator in private or using the `scan peers` function [5.1].

There is a maximum limit of 3072 peers for the entire network. If a peer becomes unresponsive for more than three hours, its assigned position on the peer list is lost and replaced by the next, not already listed network peer who makes a valid transaction on the network.

5. Peer-to-Peer Operation

When a new user joins the Bitcoin network, the user relies on four hardcoded DNS seeds [5] to detect the wider network. VF Cash, for all practical purposes, is very similar, except that with VF Cash, there is only one IPv4 seed address. An IPv4 seed is preferred over a DNS seed to minimise the risk of leaking the origin IP address when behind IP address anonymization networks [6] and for prevention against DNS spoofing [7].

[5.1]In the future, should the master server no longer be operational there is built-in functionality provided to scan through the entire IPv4 range looking for existing network peers. This is partially why IPv4 was chosen over IPv6 as the primary addressing system. IPv4 has a much smaller range to scan and thus takes a much shorter time, enabling a full IPv4 range scan in just one day to reconnect with existing VF Cash peers.

6. Node Incentive

The incentive to run a network node is distributed by an oracle. In this case, that oracle is the master server. Note that the master server is only needed for the initial distribution of VFC and acts as a common gateway for new nodes to verify themselves to the rest of the network. Once a node is verified, the master server no longer plays any role other than paying out network rewards. Network rewards are paid out at the discretion of the oracle. 4,294,967 was pre-mined on its creation, this budget is partly paid out to node operators and partly reserved for potential liquidity.

7. Mining

There are specific VFC public addresses that when discovered via the correct private key will contain between 1 and 11 VFC which can be secured to a private address. The amount of discovered or mined VFC will cause the maximum supply to increase over time.

Special addresses found through mining are called subGenesis addresses, for a public key to qualify as being a subGenesis address it needs to be taken from 33 bytes to 5 sets of 6 byte vector3's each component being 2 bytes (uint16_t) respectively. All 5 vectors are normalised and angles are checked against one another in some defined order producing 4 normalised angle values, any public-key where all 4 angle values are below 0.24 signifies a subGenesis address, this address can hold between 1 VFC and 11 VFC unless already claimed prior by another miner.

Mined addresses will hold more VFC if their averaged normal angle value of all four angle parts is closer to 0. For example, 0.24 is the highest angle value an address can hold, if all angles are 0.24 the address would have just the base 1 VFC amount. As the averaged angle decreases from 0.24 the value of the address increases until it reaches it's 11 VFC top at an averaged angle nearing 0.00.

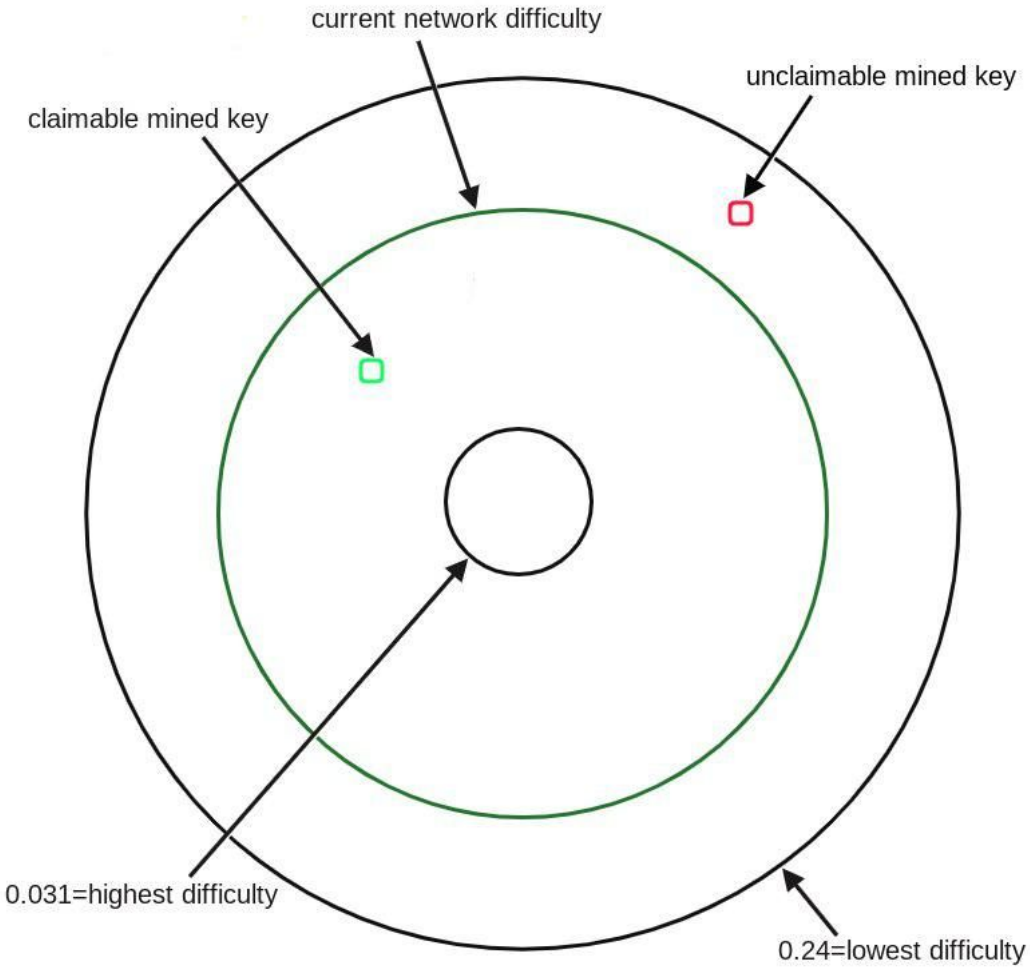

Illustration of mining difficulty provided by @amazongirl

Mining can be performed offline, the race is to who finds and claims the contents of the mined address first.

8. Mining Difficulty

Mining difficulty is controlled by participant peers/nodes in the VF Cash network, each node submits their vote which represents their desired network difficulty, this value is between 0.031 and 0.024 up to three decimal places. This creates 209 total points of difficulty between the low and high range.

The final network difficulty is the average of all submitted node difficulty values, but there is a twist, the size of the network in peers/nodes dictates the maximum amount of times a particular 'point of difficulty' can be voted on before excess votes are not included in the final average. The rule that governs the number of votes allowed per point of difficulty is; (where x is the number of network peers);

$$Max\ votes\ per\ point\ of\ difficulty: x * 1.23 / 209$$

As you can see from the above formulae that it would take a minimum of 340 peers before each point of difficulty could be voted upon twice.

Any excess votes on a point of difficulty serve as backing a voting position by a particular strength, for example, if only two votes are used in the network average for the difficulty point 0.031 but there are a total of 6 votes at this position you could say that the point of difficulty 0.031 is backed by 3x times. This gives the general populous of voters some security that even if half of the original voters change their voting position that the actual voting strength on 0.031 will remain unchanged, securing its position in the overall network average.

9. Inflation Tax (IFT)

While transactions do not directly affect your balance in VFC units, they do cause inflation to the general supply. Currently, this is a 1 VFC inflation per transaction. This Inflation is paid into the genesis address, which in turn is paid out to node operators by an oracle as 'rewards'. In the future this genesis address could be leveraged to reduce the inflation factor leveling the balance of the genesis address to near 0, assuming it was already far in credit. Or vice-versa.

10. Conclusion

This paper has proposed a simplified and lightweight system for electronic transactions that even low-end hardware can manage, such as IoT devices driven by ARM processor chips. Transaction order is not a problematic factor, allowing us to substitute the TCP protocol for the lighter weight UDP counterpart. The document has also described how the risk of double-spend attacks are reduced and how they can be mitigated by network operators. The entire network can remain completely operational independent of any centralised authority, and network rewards are fairly shared equally across all participating network nodes, only favoring nodes with better network uptime. Finally, since the network requires minuscule computational resources, transactions can be processed by node operators free of charge, and transaction rate limiting can be used to reduce network spam rather than imposing a fee on transactions to achieve a similar deterrent effect.

References

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", http://bitcoin.org/bitcoin.pdf, 2008
- [2] AdamBack, "Proof of work", http://www.hashcash.org/papers/hashcash.pdf, 12th June 2019
- [3] Olga Kharif and Alastair Marsh, "Binance CEO Spurs Outcry by Suggesting Blockchain Rollback", https://www.bloomberg.com/news/articles/2019-05-08/crypto-savior-spurs-outcry-by-suggesting-blockchain-rollback, 8th May 2019, 18:51 BST
- [4] XianchaoXie & ZhiGeng, "Directed acyclic graph", https://pdfs.semanticscholar.org/1182/d7f8e1342348b8280975b3f6ffb3f6643289.pdf, 12th June 2019

- [5] GitHub, “chainparams.cpp#L232”, https://github.com/bitcoin/bitcoin/blob/0.18/src/chainparams.cpp#L232, 17th February 2019
- [6] Anas Baig, “How to Check If Your VPN Is Leaking Your IP Address on Your Computer or Smartphone”, https://www.globalsign.com/en/blog/is-my-vpn-leaking-my-ip-address-on-my-smartphone-or-tablet/, 9th July 2017
- [7] Simar Preet Singh & A Raman Maini, “DNS spoofing”, https://pdfs.semanticscholar.org/44a8/2b4bdbac5d7f3451628733ef1bbd021b042c.pdf, 14th June 2019