TRAFFICFLOW COIN

TrafficFlow Coin Whitepaper Draft V0.1 by TrafficFLOW Team

TrafficFLOW Whitepaper Draft V0.1

INTRODUCTION

TrafficFLOW is a planned privacy blockchain with a focus on traffic management, traffic observation and scalability. TafficFLOW shal be hosted on the Ethereum network, prior to the TrafficFLOW main net deployment. The goal of TrafficFLOW is to create an anonymous coin that shall provide minimalistic feedback on traffic management, current road conditions and near instantaneous updates on other road users which shall be a break through on the Blockchain technology. TrafficFLOW chain verification and consensus will be achieved via Proof Of Audit miners, Masternodes, and Proof Of Stake nodes. This shall be done be selecting certain test protocols and utilising these features together will enable a fully autonomous Blockchain network. A main goal for TrafficFLOW shall be to anonymise assets and provide data instaneously to be used in a real live scenario for traffic management systems.

Why TrafficFLOW?

TrafficFLOW aims to improve road conditions and flows of traffic. Currently data is provided by users using supported applications, TrafficFLOW aims to bridge that gap and provide data to clients using blockchain technology via a much increased speed whilst decreasing overall data feedback. This information shall be used to alert users earlier than is currently possible of a change in road conditions and manage their routes/options as necessary. Further down the line, the aim shall be to use this data to allow traffic management systems, I.e. councils/controllers to update traffic flow systems (traffic lights etc) on the fly to correctly manage traffic and potentially avoid the unnecessary build ups that occur on a daily basis. Current system are mostly based on time management, and not near live data. TrafficFLOW shall work against this and allow a number of scenarios to be instigated dependent on the conditions and feedback the system provides.

Our aim is to use this worldwide and work in a number of markets early in the life cycle to assist with the adoption of TrafficFLOW.

Privacy and Security

Privacy currencies are not fully private. In theory, in a completely anonymous chain, no matter the protocol, node owners can collude off-chain to run their nodes maliciously. This can be disastrous in many ways for any network and represents a built-in security risk to current iterations of private blockchains. If nodes were to collude, generate infinite coins for themselves in secret, and spend them, the world would be unable to discover this as the transactions and balances will be hidden from public view.

As you cannot "roll back" these exploits without causing a chain split, it is critical to be able to detect attacks or off-chain collusion as they happen. How do you verify the status of the network, when the people telling you the status have incentive to be dishonest?

Most teams avoid the idea of private blockchains due to inherent exploitability. This exploitability is caused by the inability to track the network status and emissions by a neutral third party. The most prominent example of this critical weakness is constant exploitation of 'Zerocoin minting' and CryptoNote networks.

What is the trust issue?

To be trustless an objective third party must be able to verify the coin supply, check coin emissions, and make sure nodes are not being used maliciously. We do not believe trusting the honesty of node owners should be the only backstop against malicious actions.

For Masternode-based privacy blockchains, a degree of trust must be given to these "Masternodes" as a central governance of the coin supply, inflation and various specifications. For non-Masternode privacy networks using ZK-snarks, the network requires a complicated deployment ceremony, where a network-controlling piece of information is exposed to a certain small group of members. If these members do not completely delete this data (and do not memorize it) then the network can be entirely controlled by them.

This is the "Trust Issue". You must TRUST nodes or a group of "administrators" and central figures who can control the entire network at a whim. Current iterations of Masternodes and fully private blockchains (Zk-snarks, RingCT with full obfuscation) diverge from the "trustless" status of public blockchains.

Many non-private coins also completely ignore these governance structures and trustless network setups, declaring themselves a fully centralized central-authority dominated network.

We believe these networks are dangerous to blockchain as a whole and violate the principles of Satoshi's vision. No man-made written constitution, agreement, or arrangements can ever be as secure as the fundamentals of a third-party-secured blockchain ledger.

Proof-Of-Audit will introduce Trust-less-ness to the Trust-based system of other privacy coins. This will enable deployment of fully private blockchains using currently available tools and can expand to many existing networks.

Proof-Of-Audit can also be used in other non-privacy protocols, to enable a trustless status of their network. Proof-Of-Audit also has the added effect of causing a Proof-Of-Stake/Masternode system to be much more secure, while avoiding the issues of traditional Proof-Of-Work.

The Proof-Of-Audit idea and TrafficFLOW Protocol implementation is called the HARPOCRATES Protocol and will set out to be a new industry standard.

Mechanisms

TrafficFLOW Masternodes are required to have 10,000 TrafficFLOW collateral, a dedicated IP address and to run 24 hours a day without more than a 1 hour connection loss. Masternodes get paid using the See-saw method as described in the next section. For offering their services to the network, Masternodes are paid a portion of block rewards to maintain the ecosystem. This payment will be in TrafficFLOW and it serves as a form of passive income to the Masternode owners.

The TrafficFLOW Masternode system is modelled after the PIVX Masternode system. This has many bonuses, including preventing a 51% attack unless both Proof-Of-Stake and Masternode layers are compromised simultaneously.

The SBRS (See-Saw Balance Reward System) will have a 80/20 MN/PoS reward split balancing to a maximum of 80/20 MN/PoS reward split. This will give a fair reward to holders with too little coins to partake in a Masternode, an issue in many Masternode coin networks.

Chain verification will be done using Proof-Of-Audit, Masternodes, and Proof-Of-Stake (v3). This will give the TrafficFLOW network resistances against most known attacks and ensure the chain is secure while allowing it to be publicly scrutinized.

TOR Layer

Nodes will be mandatory TOR Hidden Services with .onion addresses to prevent attacks on node operators by tracing IP or port usage.

As some areas block Tor access, OBFS4 will also be implemented so users from these areas may use the TrafficFLOW wallet safely. OBFS4 will be mandatory along with TOR Hidden services, to allow anyone to access the network from anywhere. One trade-off of this technology is slower wallet synchronisation times on launch, which is acceptable in order to achieve wholly-obfuscated and protected nodes.

Stealth and Transparency

TrafficFLOW will have a public and a private address system, with private being the default option. Users will be able to create public addresses at any time, with a dynamic stealth address allocated to the public address on time of receiving transaction. The public-address function will enable non-private functionality on our fast and secure network.

Emissions and Founders Fee

The TrafficFLOW coin emissions will be 25 TrafficFLOW per block. There will be a 5 TrafficFLOW per block fee ("Founder's fee") allocated to the TrafficFLOW Development fund, used to further development and sustain the project long-term. A low, reasonable long-term fee gives the development team a long-term structure and incentive to create value.

50 TrafficFLOW Per block will be rewarded to MasternodeS, PoS stakers, and PoA miners.

The split will be: 45 Masternodes/PoS (rebalancing from 80/20 MN/PoS to 80/20 MN/PoS) 5 PoA

This will ensure the long-term health of the network by balancing the mining and Masternode vs staking rewards, preventing runaway Masternode growth and disincentivizing mining exploits.

TrafficFLOW Coin Specs

Initial supply: 400,000

TrafficFLOW Supply (emissions) cap: 30,000,000

Consensus: Proof-Of-Audit, Proof-Of-Stake v3, Masternodes (See-saw rewards)

Block time: 30 seconds

Block reward: Up to 30 TrafficFLOW

Development allocation per block: 5 TrafficFLOW

Block reward split: 20 Masternode/PoS (see-saw), 5 PoA

Masternode collateral: 10,000 TrafficFLOW

See-saw rebalance: 60/40 MN/PoS reward split, up to maximum 40/60 MN/PoS

Confirms required to spend: 4 blocks

Stake maturation: 200 blocks

Approximate emissions: ~236,000 TrafficFLOW per year until 4.7 Million TrafficFLOW emitted

Profit Diagram

Phase	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
Blocks from and to	10001 - 20000	20001 - 30000	30001 - 40000	40001 - 50000	50001 - 60000	60001 - 70000	70001 - 80000	80001 - 90000	90001 - 100000	100001 - 110000	110001 - 120000	120001 - 130000	130001 - 140000	140001 - 150000	150001 - 160000	160001 - 170000	170001 - 180000	180001 - 190000
Reward for 1 Block	17.5	18	18.5	19	19.5	20	20.5	21	21.5	22	22.5	23	23.5	24	24.5	25	24.9	24.8
Masternode Reward %	80	80.5	81	81.5	82	82.5	83	83.5	84	84.5	85	85.5	86	86.5	87	87.5	88	88.5
Staking Reward %	20	19.5	19	18.5	18	17.5	17	16.5	16	15.5	15	14.5	14	13.5	13	12.5	12	11.5
MN Reward coin (1 block)	1.2	1.61	2.025	2.445	2.87	3.3	3.735	4.175	4.62	5.07	5.525	5.985	6.45	6.92	7.395	7.875	7.832	7.788
Phase	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**
Blocks from and to	190001 - 200000	200001 - 210000	210001 - 220000	220001 - 230000	230001 - 240000	240001 - 250000	250001 - 260000	260001 - 270000	270001 - 280000	280001 - 290000	290001 - 300000	300001 - 310000	310001 - 320000	320001 - 330000	330001 - 340000	340001 - 350000	350001 - 360000	360001 - 370000
Reward for 1 Block	24.7	24.6	24.5	24.4	24.3	24.2	24.1	24	23.9	23.8	23.7	23.6	23.5	23.4	23.3	23.2	23.1	23
Masternode Reward %	89	88.5	88	87.5	87	86.5	86	85.5	85	84.5	84	83.5	83	82.5	82	81.5	81	80.5
Staking Reward %	11	11.5	12	12.5	13	13.5	14	14.5	15	15.5	16	16.5	17	17.5	18	18.5	19	19.5
MN Reward coin (1 block)	7.743	7.697	7.65	7.56	7.47	7.38	7.29	7.2	7.11	7.02	6.93	6.84	6.75	6.66	6.57	6.48	6.39	6.3
Phase	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**		
Blocks from and to	370001 - 380000	380001 - 390000	390001 - 400000	400001 - 410000	410001 - 420000	420001 - 430000	430001 - 440000	440001 - 450000	450001 - 460000	460001 - 470000	470001 - 480000	480001 - 490000	490001 - 500000	500001 - 510000	510001 - 520000	520001 - 21000000		
Reward for 1 Block	22.9	22.8	22.7	22.6	22.5	22.4	22.3	22.2	22.1	22	21.9	21.8	21.7	21.6	21.5	20		
Masternode Reward %	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80	80		
Staking Reward %	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
MN Reward coin (1 block)	6.21	6.12	6.03	5.94	5.85	5.76	5.67	5.58	5.49	5.4	5.31	5.22	5.13	5.04	4.95	4.5		

Transactions

RingCT

RingCT "Confidential Transaction" Ring Signatures, allowing users to increase or decrease the level of obfuscation, with fees scaling according to the level set.

Balances

STEALTH ADDRESSES

RINGCT

- Mandatory stealth address/public address system, allowing users to optionally track certain spending.

- Ring CT will also obfuscate wallet balance

Other Features

- Static emissions, No fancy inflation models, flat emissions
- 10MB Block size, Scalable into indefinite future
- PoSV3, Energy efficient, fair – Masternodes
- On chain supply "audit" - address "trustless Trust" issue of wholly-private network - The Harpocrates keystone. This will be called "Proof-Of-Audit". As details of this are highly confidential, we will not release this information until it is produced publicly to prevent copycat protocols from emerging in other competitors.

Using the above chain features, we hope to completely obfuscate transactions, addresses, balances, and nodes/IP. With a built-in coin supply audit on-chain, the system will be trustless and avoid the "trust" issue of wholly-private coins. This unique mix of features based on a staking network will be called the Harpocrates Protocol and we believe it will change the standard for privacy coins. We believe Proof-Of-Audit can augment and enhance other contemporary protocols as well, making our project's mission beneficial to the industry as a whole.

As total Decentralization is the long-term goal, future feature pushes will include cross-chain/off-chain swaps (Atomic Swaps) to help remove the influence of exchanges on the market.

Notes

Website: TBC

Discord: TBC

Contact: trafficflow-blockchain@outlook.com

Documentation:

Bitcoin trustless

https://keepingstock.net/explaining-block-chain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

Z-cash Trust Problem:

http://weuse.cash/2016/10/28/the-untrusted-setup/

Libzerocoin Protocol

http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

Masternodes:

https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146943/Masternodes
http://dashMasternode.org/what-is-a-Masternode/

See-saw reward scheme

https://pivx.org/knowledge-base/see-saw-rewards-mechanism/

Posv3

http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version

Ring CT

https://eprint.iacr.org/2015/1098

Tor/OBFS documentation:

https://github.com/Yawning/obfs4

https://www.torproject.org/docs/onion-services

Stealth Addresses:

https://steemit.com/monero/@luigi1111/understanding-monero-cryptography-privacy-part-2-stealth-addresses