FREEDOM RESERVE

16/11/2020

Decentralised
Sovereign
Blockchain

Contents

Freedom Reserve is designed to be a high-performance secure blockchain. It has the following use cases:

- Building application-specific blockchains both public and private
- Building highly scalable decentralised applications (Dapps).
- Building arbitrary customisable digital assets (Tokens)

By design, Freedom Reserve possesses the following properties:

Massive Scalability:

Freedom Reserve is designed to be massively scalable, robust, and efficient. The consensus engine is able to support potentially hundreds of millions of internet-connected devices with low latencies and high number of transactions per second.

Secure:

Freedom Reserve is designed to achieve high security. Classical consensus protocols are designed to withstand up to a certain number of attackers, and fail completely when faced with a larger number of attackers. Nakamoto consensus provides no security during a 51% mining attack. In contrast,Freedom Reserve provides a very strong guarantee of safety when the attacker is below a certain threshold, which can be parameterized by the system designer, and it degrades gracefully when the attacker exceeds this threshold. It can uphold safety guarantees even when the attacker exceeds 51%. It is one of a few permissionless systems that provides such strong security guarantees.

Decentralised:

Freedom Reserve is designed to provide unprecedented decentralisation. This includes a commitment to multiple client implementations and no centralised control of any kind. The ecosystem is designed to avoid divisions between classes of users with different interests. Crucially, there is no distinction between stakers, developers, and users.

Governable and Democratic:

£FR is a highly inclusive platform, which enables anyone to connect to its network and participate in validation and first-hand in governance. Any token holder can have a vote in deciding key financial parameters and deciding how the system evolves.

Interoperable and Flexible:

Freedom Reserve is designed to be a universal and flexible infrastructure for blockchains/assets, where the base £FR is used for security and as a unit of account for exchange. The system is intended to support many blockchains to be built on top of it. Freedom Reserve is designed from the ground up to make it easy to port existing blockchains onto it, to import balances, to support multiple scripting languages and virtual machines.

Freedom Reserve consensus protocols - Liberty* combine the best properties of classical consensus protocols with the best of Nakamoto consensus. Based on a lightweight network sampling mechanism, the nodes achieve low latency and high throughput without needing to agree on the precise membership of the system. It scales from thousands to millions of participants with direct participation in the consensus protocol. Additionally, the protocols do not make use of PoW mining, and therefore avoid its energy expenditure and payment of mining rewards, making it lightweight, green, and less dangerous.

The Liberty* protocols operate by repeated sampling of the network. Each node polls a small, randomly chosen set of neighbors, and switches its proposal if a supermajority supports a different value. Samples are repeated until convergence is reached, which happens rapidly under normal conditions.

To choose among the different transactions and prevent the doublespend, each node randomly selects a small subset of nodes and queries which of the conflicting transactions the other nodes report as valid. If the querying node receives a majority response in favor of one transaction, the node changes its own response to that transaction. Each node repeats this procedure until the entire network comes to consensus on one of the transactions.

while the core mechanism of operation is quite simple, these protocols lead to highly advantageous system with the following properties:

Asynchronously Safe:

Liberty* protocols, unlike longest-chain protocols, do not require synchronicity to operate safely, and therefore prevent double-spends even during network partitions. Bitcoin, for example, it is possible to operate independent forks of the network for prolonged periods of time

Fast Finality:

Freedom Reserve reaches finality typically in ≤ 1 second, which is significantly lower than both longest-chain protocols and sharded blockchains, which typically take up to several minutes.

High Throughput:

Liberty* protocols, which can build a DAG, reach thousands of transactions per second (5000+ tps), while retaining full decentralisation. Higher performance results (10,000+) can be achieved through assuming higher bandwidth provisioning for each node and dedicated hardware. These numbers are at the base-layer. Layer-2 scaling would increase the performance considerably.

Architecture:

An architectural view of the platform and discussion of various implementations:

The Freedom Reserve platform cleanly separates three concerns: chains (and tokens built on top of them), execution environments, and deployment.

subchains:

A subchain is a dynamic set of validators working together to achieve consensus on the state of a set of blockchains. Each blockchain is validated by one subchain, and a subchain can validate an unlimited number of blockchains.

The Freedom Reserve platform supports the creation of unlimited subchains. In order to create a new subchain or to join a subchain, one must pay a fee denominated in £FR.

Since subchains decide who may enter them, one can create private subchains. That is, each blockchain in the subchain is validated only by a set of trusted validators.

There is one special subchain called the Default subchain. It is validated by all validators. To validate any subchain, one must also validate the Default subchain. The

Default subchain validates a set of pre-defined blockchains which includes the blockchain where £FR lives and is traded.

Virtual Machines:

Each blockchain is an instance of a Virtual Machine. A VM is a blueprint for a blockchain. The state and behavior of a blockchain is defined by the VM that the blockchain runs. When creating a blockchain, one specifies the VM it runs, as well as the genesis state of the blockchain. A new blockchain can be created using a pre-existing VM, or a developer can code a new one.

The first step in participating in Freedom Reserve is bootstrapping. The process occurs in three stages: connection to seeds, network and state discovery, and becoming a validator.

The role of DNS seed nodes is to provide useful information about the set of active participants in the system. The same mechanism is employed in Bitcoin Core, where the src/chainparams.cpp file of the source code holds a list of hard-coded seed nodes. The difference between BTC and Freedom Reserve is that BTC requires just one correct DNS seed node, while Freedom Reserve requires a simple majority of the anchors to be correct.

Anyone can become a seed anchor, a set of seed anchors can not dictate whether a node may join the network, since nodes can discover the latest network of Freedom Reserve peers by attaching to any set of seeds.

Once connected to the seed anchors, a node asks for the latest set of transitions. We call this set of transitions the accepted frontier. For a chain, the accepted frontier is the last accepted block. For a DAG, the accepted frontier is the set of vertices that are accepted, yet have no accepted children. After collecting the accepted frontiers from the seed anchors, the state transitions that are accepted by a majority of the seed anchors is defined as accepted. The correct state is then extracted by synchronising the sampled nodes. As long as there is a majority of correct nodes among the seed anchors, then the accepted state transitions must have been marked as accepted by at least one correct node. This process is also used for network discovery. The membership set of the network is defined on the validator chain. Therefore, synchronising with the validator chain allows the node to discover the current set of validators. The validator chain will be explained in the following part.

For security and for incentive alignment, £FR chooses PoS as the core consensus mechanism. Some forms of staking are inherently centralised: PoW is inherently centralised in the hands of a few people with access to the infrastructure required for chip manufacturing. PoW mining 'leaks value' due to the large miner rewards. Disk space is mostly owned by large data centers. All sybil control mechanisms that have ongoing costs leak value out of the ecosystem and waste energy. This reduces the

operational envelope of the reward token, where adverse price moves can cause a mining crisis. We choose proof-of-stake, because it's green, accessible, and open to all. We note, however, that while £FR uses PoS, the Freedom Reserve network enables subchains to be launched with PoW and PoS.

Unlike other systems that also propose a PoS mechanism, £FR does not make usage of slashing, and therefore all stake is returned when the staking period expires. This prevents unwanted scenarios such as software or hardware failure leading to a loss of coins.

In Freedom Reserve, nodes issue stake transactions to the validator chain. Staking transactions name an amount to stake, the staking key of the participant that is staking, the duration, and the time that validation will start. Once the transaction is accepted, the funds will be locked until the end of the staking period. The minimal allowed amount is decided and enforced by the system. The stake placed by a user has implications for both the amount of influence the user has in the consensus process, as well as the reward obtained

Freedom Reserve supports standard Solidity-based smart contracts through the Ethereum virtual machine (EVM). We envision that the platform will support a richer and more powerful set of smart contract languages:

- Smart contracts with off-chain execution.
- Smart contracts with parallel execution.
- An improved Solidity, called Solidity++.

Governance and The £FR Token

The £FR Native Token Monetary Policy:

The native token, £FR, is capped-supply, where the cap is set at 160,000,000 tokens, with 80,000,000 tokens available on mainnet launch. However, unlike other capped-supply tokens which bake the rate of minting permanently, £FR is designed to react to changing economic conditions. The objective of £FR's monetary policy is to balance the incentives of users to stake the token versus using it to interact with the services on the platform. Participants in the platform act as a decentralised reserve bank. The levers available on Freedom Reserve are staking rewards, fees, and airdrops, all of which are influenced by governable parameters. Staking rewards are set by on-chain governance, and are ruled by a function designed to never surpass the capped supply. Staking can be induced by increasing fees or increasing staking rewards. On the other hand, we can cause increased engagement with the Freedom Reserve platform services by lowering fees, and decreasing the staking reward.

Payments:

True decentralised peer-to-peer payments are largely an unrealised dream for the industry due to the current low of performance from blockchains. £FR is as powerful and easy to use for payments as using Visa, allowing thousands of transactions every second, in a decentralised manner. For merchants, £FR provides lower fees than Visa.

Atomic swaps:

Besides providing the core security of the system, the £FR token serves as the universal unit of exchange. From there, the Freedom Reserve platform will be able to support trustless atomic swaps enabling truly decentralised exchanges of any type of asset directly on Freedom Reserve.

Governance

Governance is critical to the development and adoption of any platform because Freedom Reserve will also undergo natural evolution and updates. £FR provides on-chain governance for parameters of the network where participants are able to vote on changes to the network and solve network upgrade decisions democratically - Factors such as the minimum staking amount, minting rate, as well as other economic parameters. This enables the platform to perform dynamic parameter optimisation through the crowd. Unlike some other governance platforms, Freedom Reserve does not allow unlimited changes to arbitrary aspects of the system. Instead, only a predetermined number of parameters can be modified via governance, making the system more predictable and safe. All parameters are subject to specific time bounds, making it resistant to sudden change.

State pruning:

Pruning is simple in the Liberty* family. Unlike in Bitcoin (and similar protocols), where pruning is not possible per the algorithmic requirements, in £FR nodes do not need to maintain parts of the DAG that are deep and highly committed. These nodes do not need to prove any past history to new nodes, and simply have to store active state, the current balances, and uncommitted transactions.

Client Types:

Freedom Reserve can support three different types of clients: archival, full, and light.

Sharding:

In Freedom Reserve, sharding exists through the subchains functionality. One may launch a gold subchain and another stablecoin subchain. These two subchains can exist entirely in parallel. The subchains interact only when a user wishes to buy stablecoins using their gold holdings, at which point Freedom Reserve will enable an atomic swap between the two subchains.

Virtual machines:

The Freedom Reserve network model enables any number of VMs, so it supports a quantum-resistant virtual machine with a suitable digital signature mechanism. We anticipate several types of digital signature schemes to be deployed, including quantum resistant signatures. It is straightforward to extend the system with a new virtual machine that provides quantum secure cryptography.

Realistic Adversaries:

Freedom Reserve provides very strong guarantees in the presence of a powerful and hostile adversary, known as a round-adaptive adversary in the full point-to-point model. In reality, such an adversary is purely theoretical since practical implementations are limited. In practice, we expect worst-case-scenario attacks to be difficult to deploy.

Fair minting:

Every participant in staking is rewarded proportionally based on stake. By allowing very large numbers of people to participate in staking, Freedom Reserve can accommodate 400 million people participating equally in staking. The minimum amount required to participate in the protocol will be decided by governance, but it will initially be a low value to encourage participation.

Conclusion:

Compared to other blockchains which either run classic consensus protocols and therefore are inherently non-scalable, or use Nakamoto consensus that is inefficient and imposes high operating costs, Freedom Reserve is lightweight, scalable and secure. The native token, which secures the network and pays for various infrastructural costs is simple and backwards compatible. £FR has capacity beyond other projects to achieve full decentralisation, resist attack, and scale to millions of users without any central control, and without imposing any limits to participation.