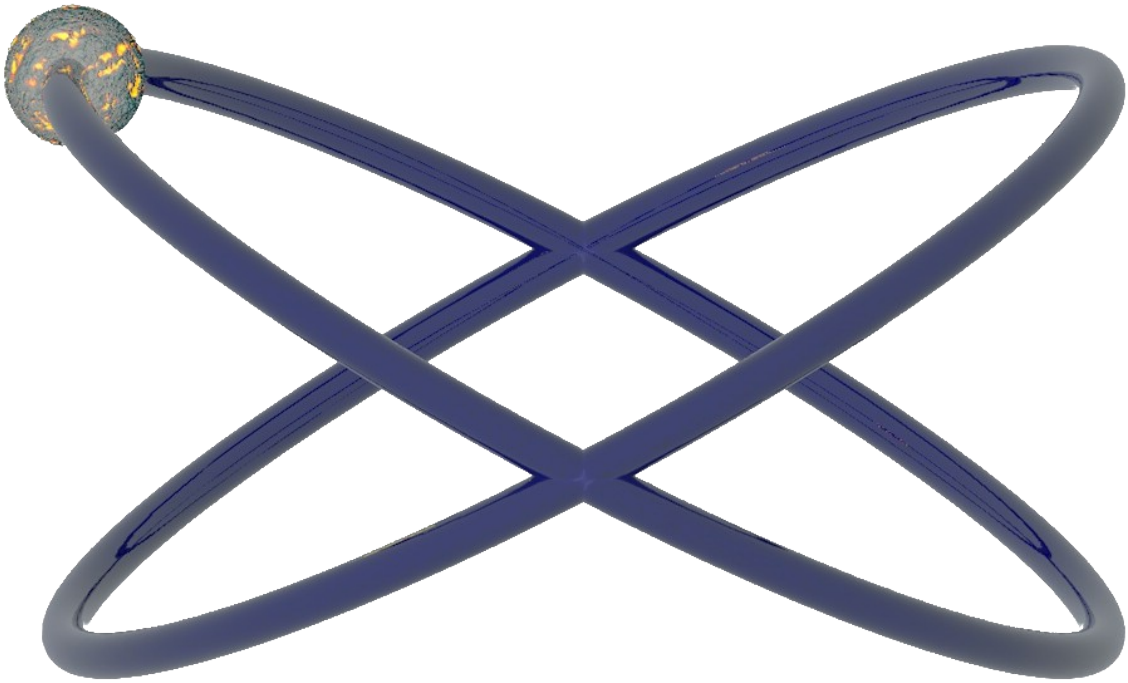
Runebase(RUNES)



0.0.2

Table of Contents

1. **Legal notice**

2. **Introduction**

3. **Reward System**
   2.1 Type: Proof of Stake
   2.2 BlockTime: ~2 min
   2.3 BlockReward: 100 RUNES
   2.4 Transaction Fees
   2.5 Max Coins

4. **Consensus**
   4.1 The Problem: Proof-of-Work
   4.2 The Solution: Proof-of-Stake

5. **Economic model**

6. **Contracts & EVM integration**
   6.1 EVM Integration
   6.2 Account Abstaction Layer
   6.3 Gas model

7. **Future directions**
   7.1 Adoption
   7.2 Development
   7.3 Partners

8. **Opportunities**

Abstract. Runebase is a smart contract platform that uses proof-of-stake to validate transactions, proof-of-stake has significant performance advantages compared to proof-of-work solutions.

Runebase is a combination of Bitcoin Core, Proof of stake and the Ethereum Virtual Machine (EVM). Runebase Core, allows smart contracts to execute on a Proof-of-Stake consensus model. The ecosystem provides familiar enviroment for smart contract and Decentralized Application Developers.

The Runebase Foundation's goal is to make sure expenses and funding for future development are covered. Another RUNES goal is to maintain compatibility with existing processes from Bitcoin and Ethereum, to be secure as possible, to be easily used by individuals, businesses and developers.

Runebase is secured by Proof-of-Stake 3 consensus protocol and is integrated with a smart contract platform. Smart contracts are executed as a part of a Unspent Transaction Output, which is part of the bitcoin transaction model. Thus, the following advantages are maintained:

1) Compatibility with existing bitcoin workflows
2) Privacy aspect of the Bitcoin UTXO model
3) Bitcoin's UTXO model is scalable for the long term
4) Integration with existing models
5) A implementation which has been proven to be secure for over a decade

1. Legal notice

This paper is intended for informational purposes only. It is not intended to be investment advice, solicitation of any kind nor an endorsement. Any decisions or actions taken on the basis of information presented in this whitepaper, Runebase websites or other content is done at your own risk and discretion.

2. Introduction

Runebase is a community-driven cryptocurrency, we define being community-driven as putting people first. By educating, increasing people's awareness about cryptocurrency and reaching out to new community members we can rally up support for future goals.

3. Reward system

2.1 Type: Proof of Stake

Runebase is secured by Proof-of-Stake 3.0 (POS3). To be eligible for staking, the funds of your account require 500 confirmations since the last transaction of the funds. Active stakes will be locked out for 500 blocks, thus you won't be able to spend the funds that are staked during this period. The locked funds are returned after the 500 block lockout period.

2.2 BlockTime: ~2 min

The network aims to produce 1 block approximatly every 2 minutes

2.3 BlockReward: 100 RUNES

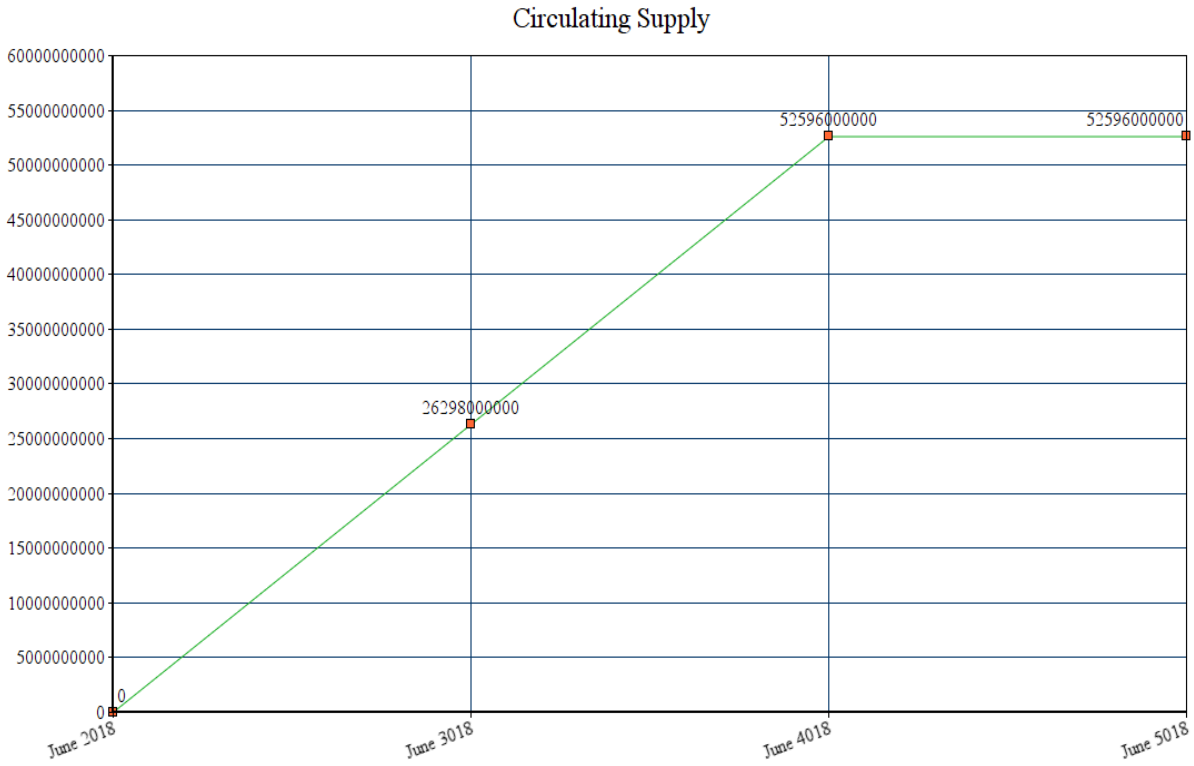
Runebase has chosen for a simpler reward structur approach. Where there is no halving of the blockrewards. Each block contains 100 RUNES + transaction fees. Staking rewards are send to the block producer in chunks of 10 RUNES each after 500 confirmations. The blockchain will keep producing coins until block 525960000 is reached.

2.4 Transaction Fees

The minimum required transaction fee is 0.004 RUNES/kb
Transaction Fees are rewarded to the block producer.

2.5 Max Coins

The max amount of coins that will ever be produced is 52596000000, however to reach the maxinimum coins is a process that will take over 2000 years. Every block produces 100 coins until max supply is reached, so there is plenty of room for people to enjoy the benefits from the reward pool.



4. Consensus

4.1 The Problem: Proof-of-Work

Proof of Work calculations require high-powered computers to perform. This requirement can include specialized computer parts like graphics processing units (GPUs) and application specific integrated circuits (ASICs). The very same components that are required by researchers, computer scientists, gamers, game designers, animators, graphic designers, etc. The increasing popularity of cryptocurrency mining can create scarcity for these critical computing components. Miners are currently using this hardware to ensure network consensus is secured via proof-of-work, however these critical components could be used many other ways that would benefit society. Those who need these computer parts are forced to settle for suboptimal hardware, pay inflated prices on secondary markets, or pay exorbitant fees to rent the necessary hardware on cloud computing platforms. A large portion of the world's critical computing hardware is being used by miners to everyone else's detriment. To grasp how much computing power the Bitcoin network is eating up, the Bitcoin network is eating up more computing power then 900,000 copies of the world's most powerful super computer. The computing power of Bitcoin only continues to grow, and this problem will probably get worse, as shown by the network's exponentially ever increasing hashrate.**(2)(3)**

4.2 The Solution: Proof-of-Stake

The advantages of the Proof of Stake algorithm are energy efficiency and security. A large number of users are encouraged to run nodes because it's easy and affordable. This along with the randomization process also makes the network more decentralized, since mining pools are no longer needed to mine the blocks.

5. Economic model

The Foundation functions as an umbrella under which all expenses and funding for the development of Runebase are managed. This means full transparency towards the community on the costs and funding of the project, but also the community's participation on how we want or can fund future developments. The Foundation expects a revenue stream to maintain its sustainability and to ensure it's goals are achieved. any surplus cash flow may be used to support technology development.

6. Contracts & EVM integration

The Ethereum Virtual Machine is a stack-based virtual machine. thereum use this virtual machine for the execution of their smart-contracts. The EVM is designed for Ethereum's blockchain, and assumes that all value transfer will be done using an account-based method. Runebase is based on Bitcoin's blockchain design and uses the UTXO-based model. Runebase has an Account Abstraction Layer implemented which translates the UTXO-based model to an account-based interface for EVM to use. there is an additional Blockchain Interface so that the EVM can directly access various information about the Runebase blockchain. **(1)**

6.1 EVM Integration

Just like Bitcoin all transactions on the Runebase blockchain use Bitcoin Scripting. however, there are 3 additional opcodes.

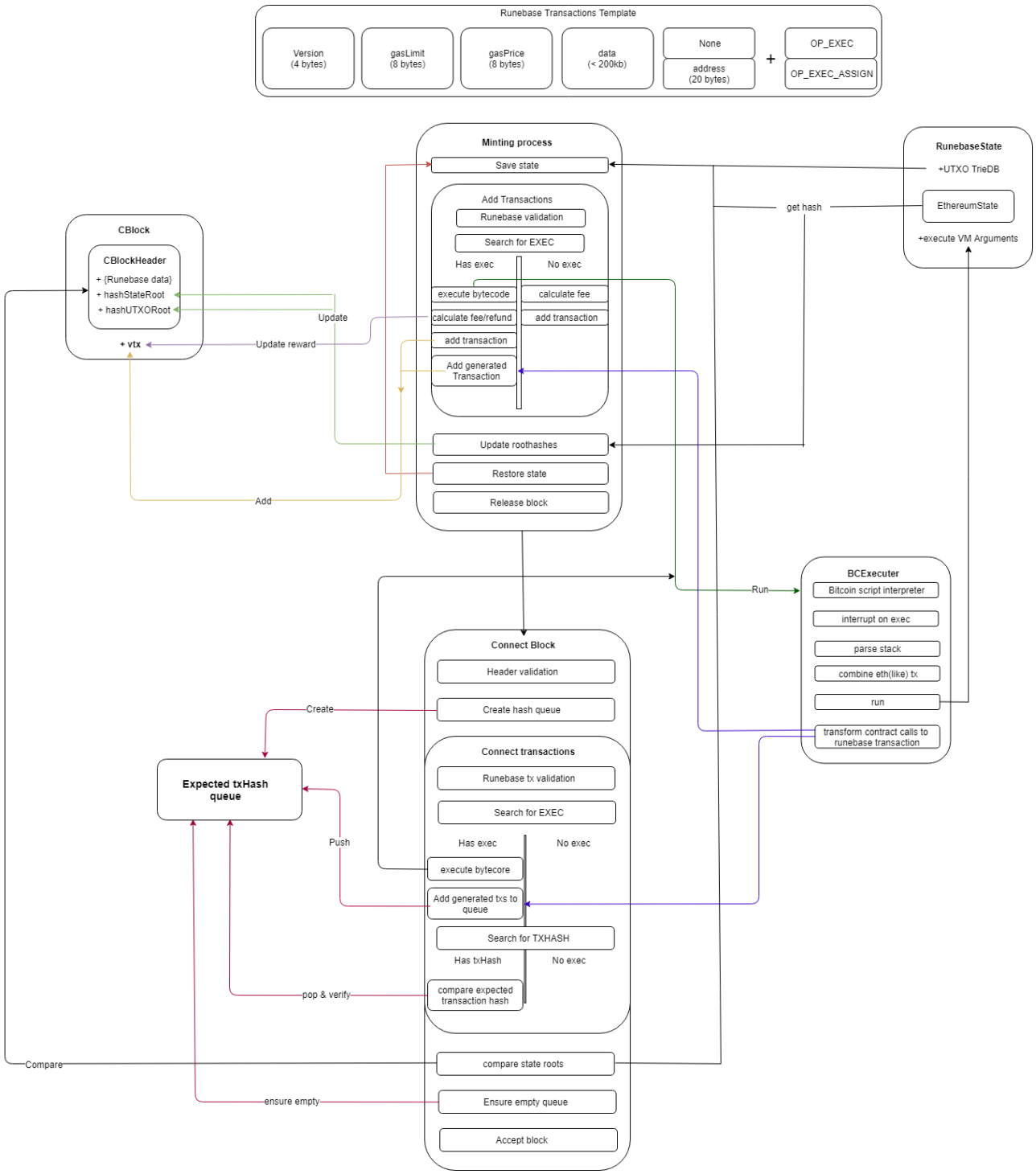
1. OP_EXEC - This opcode will trigger processing of a transaction and will execute the given EVM bytecode.

2. OP_EXEC_ASSIGN - This opcode will also trigger processing like OP_EXEC. This opcode is passes a contract address and data to the contract. It will execute the contract's bytecode while passing given data (CALLERDATA). This opcode is also used for giving funds to a smart contract.

3. OP_TXHASH - This opcode is used to reconcile an odd part of the accounting abstraction layer. It simply pushes the transaction ID hash of the current transaction being executed. **(1)**

6.2 Account Abstaction Layer

The Ethereum Virtual Machine is designed to function on an account-based blockchain. Runebase however, being based on bitcoin, uses a UTXO-based blockchain. To handle this, Runebase contains an Account Abstraction Layer which will allow the Ethereum Virtual Machine to function on the Runebase blockchain without significant modifications to the virtual machine nor existing Ethereum contracts. The EVM account model exposed to smart contract developers is fairly simple. There are operations that can check the balance of the current contract and other contracts, and there are operations which can send funds to other contracts. **(1)**


Runebase Transactions Template
Version (4 bytes)
gasLimit (8 bytes)
gasPrice (8 bytes)
data (< 200kb)
None
address (20 bytes)
+
OP_EXEC
OP_EXEC_ASSIGN
Minting process
Save state
Add Transactions
Runebase validation
Search for EXEC
Has exec
No exec
execute bytecode
calculate fee
calculate fee/refund
add transaction
add transaction
Add generated Transaction
Update roothashes
Restore state
Release block
RunebaseState
+UTXO TrieDB
EthereumState
+execute VM Arguments
get hash
CBlock
CBlockHeader
+ {Runebase data}
+ hashStateRoot
+ hashUTXORoot
+ vtx
Update
Update reward
Add
BCExecuter
Bitcoin script interpreter
interrupt on exec
parse stack
combine eth(like) tx
run
transform contract calls to runebase transaction
Run
Connect Block
Header validation
Create hash queue
Create
Expected txHash queue
Connect transactions
Runebase tx validation
Search for EXEC
Has exec
No exec
execute bytecore
Add generated txs to queue
Search for TXHASH
Has txHash
No exec
compare expected transaction hash
Push
pop & verify
Compare
compare state roots
Ensure empty queue
ensure empty
Accept block

(1)

5.3 Gas model

The gas concept can be summarized by saying that each EVM opcode executed has a price, and each transaction has an amount of gas which can be spent. Whatever amount of gas remains after the transaction is complete will be refunded back to the sender. Also if the amount of gas required to execute a contract exceeds the amount of gas available to a transaction, then the transaction's actions and state changes are reverted. This means any permanent storage that has been modified will be reverted to its original state, and any spending of contract funds will be reverted so that they are not spent. all of the gas consumed by transactions is given to the miner processing it. Although Runebase uses the gas model from Ethereum, it is expected that the gas schedule (gas price for opcode execution) will be different from the Ethereum blockchain. This is because some operations on the Runebase blockchain are more expensive or cheaper than on the Ethereum blockchain. When creating a contract funding or deployment transaction, the user specifies two specific items for gas. The first is the GasLimit (How much gas can be consumed) by the exection of the contract. The other is the GasPrice, which is the price of each unit of gas in RUNES. The maximum RUNES expenditure of a contract execution can thus be easily calculated by multiplying GasLimit with GasPrice. If this maximum expenditure exceeds the transaction fee provided by the transaction, then the transaction will be invalidated and will not be processed. **(1)**

7. Future directions

Below we set out goals. We have not set any dates for when we anticipate these to be completed at this time. We are constantly evolving and try to adjust to any given climate.

7.1 Adoption

The trustless nature of the blockchain is incredibly powerful, but we believe a bridge of social trust is still needed for us to achieve adoption. The adoption process plays a big part in our ability to grow and to expand our reach by listing on additional exchanges.

7.2 Development

Runebase will stay compatible with bitcoin, the latest bitcoin core software updates will be integrated into the the runebase core software. We will release a iphone wallet once the barriers are lifted which restrict us from doing so. The foundation will direct and fund the development that give partners the ability to build, grow, and create value for one another. As part of this process, All code produced by the Runebase foundation is made available as an open source project that can be leveraged to power new communities and add capabilities to existing ones. Our motto is underpromise and overdeliver.

7.3 Partners

Partnerships with complementary businesses can give access to new userbases. Partnerships often benefit both parties. Even though partnerships are often only for a specific goal, it can create long-lasting business relationships.

8. Opportunities

Runebase operates on a relatively young and growing market. Because the blockchain is still a fairly new and developing technology, whose countless possibilities have not been tried so far, there is a chance that the market and its capitalization will grow. This may also result in an increase in RUNES price. One of the aspects affecting cryptocurrency development is directly linked to FIAT currencies, FIAT currencies weakening value, their lack of support in gold, growing inflation, as well as relatively small profits from deposits and bonds. These factors may cause investors to transfer their funds from traditional forms of investment to blockchain projects, including cryptocurrencies.

References

(1) https://whitepaperdatabase.com/qtum-whitepaper/

(2) S.A.R.L. Hash rate,2017 https://blockchain.info/charts/hash-rate?timespan=all

(3) https://www.savebitcoin.io/whitepaper