# RSK

Bitcoin powered Smart Contracts

## White paper
## Overview

Revision: 9
Date: November 19th, 2015
By Sergio Demian Lerner

## Introduction

In 2008 Satoshi Nakamoto revolutionized payments by creating Bitcoin. Bitcoin included a very limited implementation of the so-called "smart contracts", a concept introduced back in 1993 by Nick Szabo.

Since then, a lot of research has been dedicated to the creation of new cryptocurrencies that support full Turing complete distributed programs. Now there is a widespread confidence that useful, secure and deterministic virtual machines can be built to achieve this goal.

We believe that new use cases are necessary in order for Bitcoin to become the leading global cryptocurrency, and that adding smart-contract capabilities is key to secure that future. With that in mind we created Rootstock (RSK), a smart-contract platform that incorporates a Turing Complete Virtual Machine to Bitcoin. It also provides other enhancement to the network such as faster transactions and better scalability, features that we also believe will enable new usage scenarios.

RSK is an evolution of QixCoin, a turing-complete cryptocurrency created back in 2013 by the same development team. RSK provides an improved payment experience with near instant confirmations. It achieves currently 300 tps and confirms most payments in less than 20 seconds. And yet, is still based on the same security guarantees Bitcoin has, supporting SHA-256D merged mining.

RSK works as a Bitcoin Sidechain. When Bitcoins are transferred into the Rootstock blockchain, they become "Rootcoins" (RTC). Rootcoins are equivalent to bitcoins living in the Rootstock blockchain, and they can be transferred back to Bitcoins at any time at no additional cost (except for standard Rootstock transaction fees). RTC is the base currency used on the RSK sidechain to pay miners for transaction and contract processing. There is no currency issuance: all RTC are created from Bitcoins coming from the Bitcoin blockchain.

Rootstock enhances Bitcoin in the following areas:

- Turing-complete Rootstock Virtual Machine (RVM) allowing smart-contracts
- Average first confirmation of transactions in 10 seconds
- Safe merged mining combining PoW with threshold-signature based federation
- Embedded low-delay fast relay backbone into peer-to-peer gossip network.
- Two-way pegging using sidechains (currently a federated peg, fully automatic peg subject to Bitcoin improvements)

Acronyms: "RSK" refers to the Rootstock (the platform), related terms are "RSK protocol" (the specification) and "RSK reference node" (the reference implementation), the native RSK currency is the "Rootcoin", and "RTC" is the symbol of the Rootcoin currency, "BTC"

refers to the Bitcoin currency and “Bitcoin” refers to the Bitcoin protocol.

## Why Rootstock is important for the Bitcoin Ecosystem?

### Alignment of Bitcoin Stakeholders and protection of value

Rootstock governance's primary goal is to align the main stakeholders of Bitcoin by creating rewards that are fully aligned with their current activities.

This philosophy is directly reflected in its core architecture where Bitcoin miners provide the hashing power required for the proof-of-work block validations, industry leaders (Exchanges, Wallets and Payment Processors) integrate the Federation that creates validation checkpoints and sign the redeem transactions of the 2-way peg.

On top of that Rootstock decides improvements to its platform based on a voting system where Miners, Industry Leaders, Bitcoin / Rootstock holders and core developers take the final decision.

In the following paragraphs we describe how this incentives play along.

### Governance model

Each player in the community has the know-how to serve best the community: exchanges and web-wallets know how to protect Bitcoin savings, miners know how to realize large scale mining operations to secure user’s transactions, Blockhain companies innovate in new use cases and makes dreams come true, core developers have the technical expertise to known how to tackle the technical challenges to come, node maintainers provide the infrastructure and network connectivity, and users are the heart of the system, providing trust and liquidity.

Rootstock governance model aims to represent all actors of the community, by providing a board of governance consisting in 5 seats. Miners will be able to vote with hashing power (1 vote), Bitcoin and Rootstock users will vote with proof-of-stake (1 vote), Exchanges and web-wallets will vote though the Federation (1 vote), Rootstock and Bitcoin Core developers will have a special threshold voting system (1 vote), and the last vote will be offered to a non-profit established Bitcoin institution, such as the Bitcoin Foundation, that can represent the broader ecosystem. Also an institutional vote could be offered to the Ethereum Foundation, if it is representative of the Ethereum community.

### Protection of Bitcoin Miner's Investment

In August 2016 Bitcoin mining profitability margin will fall to less than 50% due to the decreasing block reward from 25 BTC to 12.5 BTC. Hundreds of millions of mining hardware will become instantaneously obsolete. This probably includes all mining machines in the market today, since two generations of chips (faster and with lower power consumption) will be developed and sold before 2017. Almost all current miners that have not replaced their hardware will see the end of their mining business. Rootstock, thanks to its merged mining capabilities, brings the opportunity to these miners to keep on business

at least four more years. Since Bitcoin merge-miners can mine both coins with zero marginal cost, miners will still be able to mine Bitcoin as long as the additional income provided by Rootstock mining compensates the profitability gap.

Additionally the reduction in mining profitability by the Halving will create additional concentration in the low cost miners which will increase Bitcoin's network vulnerability. Hence, RSK could also play a key role in promoting a broad base of profitable miners increasing the security and value of Bitcoin.

Also by starting today at a minimum cost, and creating applications for Rootstocks, Bitcoin miners may not only protect their investment, but develop a whole new business opportunity.

**Securing the Bitcoin / Rootstock 2-way peg**

Leading Bitcoin companies will integrate a Federation that will play the fundamental role of securing the transfer of funds between the Bitcoin and Rootstock blockchains. In exchange for that they will profit from the fees generated by the settlement between the inflow and outflow of funds.

**Lower Bitcoin transactions fees and stable value asset issuing**

Current Bitcoin holders and prospective users have seen their usage of the monetary system confined to certain use cases (i.e: investment, global payment network) mainly due to bitcoin price volatility but this constraint might worsen in the future due to a potential increase in transaction fees on the next Bitcoin halving.

Rootstock brings a solution to this by offering almost instant transaction validation (20 seconds) and asset issuing with prices pegged to that of a fiat currency or other stable commodity. Lowering volatility exposure in transactions while keeping bitcoin as a reserve currency increases overall bitcoin value.

**Bitcoin Security hardening**

On the next Bitcoin reward halving, hundreds of millions on dollars in obsolete mining hardware will be sold cheaply privately or online. This will open a window of vulnerability giving an attacker the possibility to buy a huge amount of hashing power for very little money and execute a 51% attack. Also the decrease in security may affect the perceived value of the coin. By increasing the profitability of Bitcoin mining with Rootstock merged mining, the Bitcoin network may prevent the hash rate to plummet.

## Rootstock as a low-cost BTC payment network

If Bitcoin block size is not increased via a hard-fork, when the next Bitcoin reward halves, Bitcoin transaction fees may become prohibitively high for certain applications. As RSK blocks can hold many more transactions than Bitcoin blocks, Rootstock will naturally offer lower fees. See next section for an analysis of future scenarios regarding transaction fees.

The future of Bitcoin and its transactions fees is unclear: currently, contentious proposals on changes in the maximum block size will have a high impact in future transaction fees. In the following table we attempt to predict future scenarios and compare RSK and Bitcoin under reasonable assumptions on growth and forks.

| Parameter | Bitcoin | Rootstock |
|---|---|---|
| Confirmation time with comparable security under Satoshi equivalence | 10 minutes | 10 seconds |
| Minimum confirmation time for a reversal probability of 0.1% | 20 minutes (2 blocks) | 30 seconds (3 blocks) |
| Max. Transactions per second | 3.3 tps<br>(assuming an average size tx) | 300 tps at launch<br>Scalable to 1000 tps |
| Current average cost for users for a standard transaction | 6 cents<br>Assuming:<br>- 1.5 tps | Market price not available |
| Current cost for miners to include a standard transaction | 1 cent<br>Assuming:<br>- Using the fast relay network<br>- UTXO in memory<br>- 1 ms processing time per tx.<br>- 25.2 BTC average block reward<br><br>5 cent<br>Assuming:<br>- Using standard relay network | <1 cent (estimated)<br>Assuming:<br>- No RSK specific hardware switching.<br>- Almost no Rootstock transactions<br><br>1 cent (estimated)<br>- Interrupting a miner to load new header loses 10 ms of processing time |
| Transaction fees by end of 2016 | 1.6 USD<br>Assuming:<br>- block size is not increased<br>- BTC/USD rate unchanged<br>- Same level of security<br>- 3 tps | 1 cent (estimated)<br>Assuming:<br>- 3 tps |

Is important to note from the above chart that transaction fees estimations are based on the unproven fact that the BTC price will remain at approximately 240 BTC/USD during 2016. If the price increases ten-fold during this period, then also will the transaction fees, rendering Bitcoin Blockchain viable as an inter-banking clearing system, but not a payment network. Also is important to note that off-chain payment systems can emerge, providing cheaper payments, but at the same time centralizing the network, and changing

its decentralized nature.

The following table shows possible future scenarios by the end of 2016, assuming that network hashing difficulty increases at the same ratio as BTC price:

| Scenario | Bitcoin cost of tx to miners | Rootstock cost of tx to miners |
|---|---|---|
| Bitcoin price increases 10x | 16 USD | 2 cents |
| TPS increases 10x via hard-fork | 11 cents | 0.2 cents |
| BTC price and TPS increase 10x | 1.1 USD | 2 cents |

As the cost of including a Bitcoin transaction increases, users will switch to platforms with lower transaction costs, such as Rootstock.

## Rootstock Use Cases

The Rootstock platform provides Turing-complete smart contracts as proposed by Nick Szabo in 1993. At the same time, RSK's VM is backward compatible with Ethereum VM, hence Rootstock gives the opportunity to developers working on Ethereum to benefit from the robustness of the Bitcoin Blockchain. Below we present a list of potential smart contracts and use cases that can be developed over RSK.

### Micropayment channels and Hub-and-Spoke networks

Micropayment channels allow two parties to make secure regular low valued payments without paying fees for each payment, but only one time when the channel is closed.

Hub-and-Spoke networks allow mutually untrusted users to make low-cost one time payments indirectly using payment channels to and from a third party with minimal trust. The RSK allows Hub-and-spoke networks to be implemented directly with minimal hassle and interfacing natively with standard e-wallets.

### Peer-to-peer distributed exchange

Using TierNolan's protocol RSK supports contracts that act as peer-to-peer exchanges. Automatic matching in an order book can also be easily created. This allows distributed markets over independent block-chains, exchanging crypto-assets without third parties.

### Retail Payment Systems

RSK allows BTC to be adopted globally for every-day retail transactions. One of Bitcoin main limitations for retail use is its confirmation time (from 10 minutes to 1 hour to ensure irreversibility). RSK allows consumers to benefit from Bitcoin security with confirmations in just a few seconds. Merchants will be able to accept payments instantaneously without requiring third party gateways. Another key element that any platform should have to succeed in the retail market is to be able to support a large amount of transaction per second (tps). The RSK network, using the DÉCOR+ protocol, allows to process over the Bitcoin Blockchain up to 300 tps (twice as much as Paypal)

### Escrow Services

RSK allows the creation of smart escrow services where oracles sign (or not) a transactions defining whether it should be executed (or not) without having any contact with the funds under escrow.

### Crypto-assets Creation

RSK allows the creation of crypto-assets (or altcoins) secured by the Bitcoin network. Given RSK's flexibility to price the contract's fuel these application (as all others) could be used from students to banks and corporations.

### Asset Securitization

RSK also allows the creation of digital tokens backed by real assets. This could be use to digitally commercialize REITs, shares, issue debt or any other asset (or future proceed). This particular use case will provide a unique solution to those small businesses in the developing countries where the traditional financial markets do now fulfill the demand for working capital or capital to grow.

### Decentralized remittances

This particular use case is especially important in developing economies where the unbanked/undocumented population has to pay usury fees to send money to their families for food and shelter.

### IP Protection / Registry

RSK allows the development of contracts that can replicate what is known as Proof-of-Existence which allows individuals and companies alike to proof the existence of a certain document (or property right) at any given point in time with the security of the Bitcoin Blockchain. This use case could be particularly important in societies in Latin America, Africa and Asia with unreliable land registration mechanisms.

### Voting System

As a particular case of crypto-asset, RSK allows the creation of digital votes that allow extremely secure and transparent elections at a minimum cost.

### Micro-lending

Over 50% of the global population does not have access to the traditional financial system. This lack of access to credit is a direct cause to the economic inequality that our global society faces nowadays. RSK allows the development of scalable digital micro-lending contracts that could provide access to credit to the 3 billion poorest inhabitants of the world.

### Supply Chain Traceability

RSK also allows the creation of digital wallets to track and trace (digitally) the physical location of a certain product or batch. This type of contract could be particularly useful in the retail, food and healthcare industries among others. As all the other use cases, by using RSK this could be achieved with the security of the Bitcoin Blockchain at a minimum cost.

### Online Reputation & Digital Identity

One of the main problems of the developing world is the lack of documentation and IDs for the poor. This prevents the poor from voting, accessing healthcare, reporting crimes / abuses and accessing financial aid. RSK allows the creation of digital global registries as secure as the Bitcoin Blockchain at extremely low cost.

### In-game Global Currency

Many multi-player games have in-game economies, including private currencies. As these games evolve, virtual currencies become as valuable to users as fiat money, and are often traded on secondary markets. Inflation, cheating, and online theft become user concerns. Also the game company may face legal and security hurdles having users virtual money in consignment. As the world becomes global, so will virtual games, and players will feel discomfort that money earned in one game cannot be easily spent in another game. RSK can solve these problems by allowing games to accept BTC (in equivalent RSK coins) for their in-game payments, or create a private digital asset that is protected by RSK. RSK payments can be as fast as closed-loop systems for low denominations, so game engines can use RSK as the in-game purchase system, for player-to-player trading and for company-to-player virtual offerings. By just clicking on an URL or scanning a QR code, trading can be triggered using the standard player's external e-wallet software, and also paying commissions to the gaming company.

### Internet-gambling and Prediction Markets

Fast payments also means fast payouts. Bitcoin gambling sites such as SatoshiDice have managed to provide no-registration fast betting experience using 0-confirmations and chained transactions, but at a security risk for the gambling site. RSK allows betting with near instant payouts having block confirmation.

### Fair-playing

By incorporating smart-contracts, and in conjunction with well-studied cryptographic protocols such as Mental Poker, RSK is able to provide an open and fair platform for card playing without the requirement for a trusted third party taking a rake.

These are just a few examples among many others that could be developed and programmed over the RSK platform using the underlying Bitcoin technology. It is important to mention that the Bitcoin miners (via merge mining) are going to be the ones running these contracts and benefiting from the vast majority of the fuel consumed to run those contracts.

## Technology Overview

RSK platform is, at its core, the combination of:

- A Turing-complete resource-accounted deterministic virtual machine (for smart contracts)
- A two-way pegged Bitcoin sidechain (for BTC denominated trade)
- A dynamic hybrid merge-mining/federated consensus protocol (for consensus security), and a low-latency network (for fast payments).

### Turing-Complete virtual Machine

RSK virtual machine (RVM) is the core of the Smart-contract platform. Smart-contracts are executed in parallel by a high-percentage of the network nodes. The result of the execution of a smart-contract can be the processing of inter-contract messages, creating monetary transactions and changing the state of contracts persistent memory. The RVM op-code level compatible with EVM, to allow Ethereum contracts to run flawlessly on RSK. In the first release, the VM is executed by interpretation. For the next release, it is planned to emulate EVM by dynamically retargeting EVM opcodes to a subset of Java-like bytecode, and a security-hardened and memory restricted Java-like VM will become the new VM (RVM2). This will bring RSK code execution to a performance close to native code.

Main features:

- Independent VM, but compatible with EVM at the opcode level.
- Rootstock provides Ethereum users the possibility to run their projects with the security of the Bitcoin network.
- New opcodes for fast int32 arithmetic and better just-in-time compilation (planned), for greater performance.

### Sidechain

A sidechain is an independent blockchain whose native currency is pegged to the value of another blockchain currency automatically by using proofs of payment. There is a two-way peg when two currencies can be exchanged freely, automatically, and without incurring in a price negotiation. In RSK, the Rootcoin (RTC) is two-way pegged to the BTC (more precisely, a Rootoshi, the minimum unit of account in RSK, is pegged to a Satoshi, the minimum unit of account in Bitcoin).

In practice, when BTC are exchanged for RTS, no currency is “transferred” between blockchains in a single transaction because Bitcoin cannot verify the authenticity of balances on another blockchain. When a transfer occurs, some BTC are locked in Bitcoin and the same amount of RTC is unlocked in RSK. When RTC needs to be converted back into BTC, the RTC get locked again in RSK and the same amount of BTC are unlocked in

Bitcoin.

### Semi-Trust-Free Sidechains

Fully trusted and third-party-free two-way pegs can be created using smart-contracts on both platforms. But since Bitcoin does not currently support smart-contracts nor native opcodes to validate external SPV proofs, part of the two-way pegging system in RSK requires trust on a set of a semi-trusted third-parties (STTP). No single STTP can control the locked BTCs, but only a majority of them has the ability to release BTC funds. The STTPs temporarily store the BTC that are locked, and unlocks BTC to pay Bitcoin users RTC are locked in RSK to be transferred back to Bitcoin.

In RSK the STTPs that protect the locked funds are precisely the members of the Federation. This is because the Federation incentives are highly aligned with the STTPs: they must be well-respected community actors, such as universities, and they must also have the technical ability to maintain a secure network node. The locking and unlocking of funds is done by this secure network nodes without any human intervention. Therefore a requirement for being part of the Federation is the ability to audit the proper behaviour of the software that powers the node, specially regarding the correctness of the component that decides on releasing BTC funds. We plan to create tamper proof hardware that will enforce the Federated validation algorithm to further improve security.

Once Bitcoin adds special opcodes or extensibility to validate SPV proofs as a hard-fork, and once the new system is proved secure and trust-free, the Federation role as STTPs will no longer be necessary, and the RSK team will implement the changes to adapt RSK to the trust-free system.

### Dynamic Hybrid Merged mining/Federation

We believe that PoW is the only consensus system that prevents the re-write of blockchain history at low cost. All other consensus systems that do not consume a valuable resource for mining have this drawback, and rely on reputation, and prevent anonymous participation in mining. All other consensus systems require new users to trust in a set of parties to find an authenticated checkpoint of the ledger.

High rate PoW consensus based on periodic blocks with low orphan waste requires miners to stop their hardware miners and restart them to mine on new header mid-states each time a new block is solved by the network. This result in mining time gaps, or greater network latencies for mid-state switching, on average. These gaps reduce the efficiency of Bitcoin mining even if they consume a few milliseconds. Therefore RSK uses the DECOR+ block reward sharing scheme to reduce competition and allow miners late switch to the RSK best block. If miners switch their hardware each time a RSK block is found, they compete for a full RSK block reward. If they late switch, and keep mining past block tips, they create uncles and and earn a share of the block reward. In none of these cases they are fully orphaned, as DECOR+ pays a reward to uncles and the GHOST rule counts uncles as normal blocks and secures the best chain. The efficiency of BTC mining is therefore maximized.

As we expect a period where RSK hashing power will be below 50% of the total BTC

hashing power. This would leave the network vulnerable to a 51% attack where the remaining hashing power outperforms the existing RSK hashing power to double-spend. To prevent such situation RSK includes federated checkpoints for PoW mined blocks. Federated checkpoints are signed by the Federation members and clients can use the the majority of the signatures to better decide which is the best chain. Also Rootstock has a last-resort protocol where if mining power goes below 5% of Bitcoin hashing power, the Federation is able to create signed blocks. By default, clients stop using federated checkpoints when if Roostock hashing power is over 66% of the maximum BTC hashing difficulty observed in the best chain and the fees paid in a block is higher or equal to the average reward of a bitcoin block.

The RSK platform will be launched with a federation of well-known and community respected members. Each member is identified by a public key for the checkpoint signature scheme. The federation is be able to add or remove members using and embedding voting system, although these actions would require a high percentage of the member votes.

The aim of RSK founders is that the RSK network will incentivize merge-mining. However RSK is robust to merge-mining shortage as the Federation is automatically brought to secure the network in the shortage case.

Main features:

- 1-day maturity for mining reward.
- Federated members checkpoints
- Code embedded checkpoints during bootstrapping period.
- No loss of efficiency in Bitcoin mining expected from merge mining (less than 0.1% for immediate mid-state switching and 0% for late switching)

**Fast payments and low-latency-network**

RSK aims to be a better payment network. To achieve fast payments, several solutions have been developed:

- Use of competition-free block selection (e.g. Hyperledger, Ripple, closed-loop systems)
- Use of hub-and-spoke networks (e.g. Bitcoin lightning network)
- Use of high PoW block rates

Hub-and-spoke networks add new centralization nodes, and require a complete adaptation of client wallets to a new, completely different payment model. Although so this alternative can be easily implemented on RSK, is not the native system for fast payments. RSK adopts the DECOR+ and FastBlock5 protocols, which allow reaching a 10 seconds average block rate that does not create incentives for mining centralization, is selfish-mining free and incentive compatible.

Main features:

- 10 seconds block interval
- Two stage block propagation (2SBP) protocol

- Push Missing Transactions (PMT) protocol
- Full network propagation of last competing blocks to prevent selfish mining and reduce stale block rate.
- Delayed Transaction Inclusion heuristic (DTI). Transactions are delayed 5 seconds on each miner's block transaction queue to allow the fastest possible block verification, because transactions are already present in the pools of every node of the network.
- New network command to spread block headers with time critical priority.
- New network command to spread block transactions hash list immediately after block header propagates.
- Mining on Unverified Blocks Heuristic (MUB). Mining over block headers with unverified transactions with a 5 seconds fallback.
- Block headers are flagged when they have no transactions (except for coinbase)
- Two Prioritized Streams for each Connection protocol (2PSC). New message transport layer with message-slicing allowing two parallel sessions with distinct priority. This allows block headers to be sent over the high priority session and interrupt whatever message was being transmitted over the low priority session.
- Local Route Optimization Protocol (LRO). Local optimal block routing based on peer priorities. Local optimal transaction routing based on peer priorities
- DECOR+ protocol for reward sharing between competing blocks.
- GHOST protocol for chain weighting.

## Rootstock Feature comparison

We attempt to compare RSK with other blockchains, and we show that essentially RSK present better technical choices without eroding decentralization, where decentralization is measured as the inverse of the cost of running a full-node instance.

| Item | Bitcoin | Ethereum | Factom | Counterparty | Rootstock |
|---|---|---|---|---|---|
| Average Confirmation Time | 10 min. | 12 sec (GHOST) | 1 min. (Federated servers ) | 10 min. | 10 sec. (DECOR+GHOST) |
| Security threshold (due to selfish mining) | ~30% | between 30% and 50% | ~30% | ~30% | 50% (DECOR+GHOST) |
| Turing complete Smart-Contracts | No | Yes | Yes | Planned | Yes |
| Adds value to Bitcoin | - | No | No | No | Yes (merge-mined) |
| Integration with Bitcoin | - | No | Overlay protocol | Overlay protocol | Sidechain |
| Scalability via Probabilistic Verification and fraud proofs | No | No | No | No | Yes |
| SPV clients | Yes | Yes | No | No | Yes |
| Block relay backbone | Yes | No | Yes | Yes | Yes |
| Native support for user-defined access structures | Yes | No | Yes | No | Yes |
| Native support for user-defined signature schemes | No | No | No | No | Yes |
| Easy Hardware wallet Integration | No | Yes | No | No | Yes |
| Security guarantee | SHA256D miners | Ethash miners | SHA256D miners + federation | SHA256D miners | SHA256D merge-miners + federation |
| Confidential Transactions | No | Via contract | Via external program | No | Native support Planned using AppeCoin protocol |
| Unique transaction ID | No (malleab.) | Yes | No | No | Yes |
| Scalability [tps] | 3 to 24 | unbounded | unbounded | 3 to 24 | 300 at launch |
| Native token | BTC | ETH | FACTOID | XCP | BTC via two-way peg |

## Instant Payments Technology preview

Since the creation of Bitcoin there has been a race towards lower intervals for PoW block-chain based cryptocurrencies. First there was Bitcoin with a 10 minute interval, then was LiteCoin using a 2.5 interval, then was DogeCoin with 1 minute, QuarkCoin with 30 seconds, and Ethereum with 12 seconds. Every new cryptocurrency lowers it a little bit, but very few designers actually know what the implications of doing so are. To understand how the block interval impacts the stability and capability of the cryptocurrency network, several factors must be taken into account. First of all, the most important factor that affects the viability of short confirmation intervals is the number of stale blocks generated. Two other factors mainly affect the stale block rate: the block propagation protocol and the block propagation time from the top miners to the top miners. For Rootstock we've carefully analyzed these factors and run simulations in order to verify the performance, usability and security of the network. In this section we'll review the new protocols Rootstock use to reduce the stale block rate.

### DECOR+ Protocol

In Bitcoin, when two or more miners have solved blocks at equal height, there is a clear conflict of interests. Each competing miner wants his block to be selected by the remaining miners as the best-chain tip, while the remaining miners generally would not mind which one is chosen. However, all the remaining honest miners and users would prefer that all of them choose the same block tip, because this reduces the natural reversal probability. The ideal solution would incentivize the miners in conflict to choose the same parent also, and DECOR+ sets the right economic incentives for a convergent choice, without requiring further interaction between miners. DECOR+, a is reward sharing strategy that incentivizes economically resolving the conflict such that:

1. The conflict is resolved deterministically when all parties have access to the same block-chain state information.
2. The chosen resolution is the one that maximizes all miners revenue, both for miners in conflict and for the rest.
3. Resolving the conflict takes negligible time.

### The block propagation protocol

Bitcoin and Ethereum forward each block by packing the block header with all the transactions contained in the block. This strategy, while being the most easy to analyze, is known to perform badly both regarding block propagation latency and bandwidth usage, which is doubled. Bitcoin miners partially solved this problem using the Fast Relay Network: this is a centralized backbone that relays blocks in a compressed form, and it is maintained by a single user. Rootstock was born with a Fast Relay Network embedded into the network protocol, and the low latency properties emerge from the network topology and do not require centralization.

### Two Stage Block Propagation (2SBP)

RSK blocks are sent in two stages: in the first stage only the block header is sent. In the second stage the list of hashes of transactions included in the block is sent. Using 2SBP the channel capacity is doubled, allowing more transactions to be stored in each block. After each node has received the block header and the transaction hash list associated with the block header, the node attempts to reconstruct the block in order to fully verify it.

### Push Missing Transactions protocol (PMT)

Since each node stores the hashes of the transactions advertised by its peers, the miner also sends immediately the transactions included in the block that he knows are missing in each peer's pool. This eliminates completely the need of a second interaction to request additional transactions. Sending the missing transactions before they are asked by a peer is a third phase of the 2SBP protocol.

### Delayed Transaction Inclusion heuristic (DTI)

Miners only include transactions that have been received before a few of seconds back. This assures with high probability that does transactions will have already been received by peers before the block is mined. Note that delaying transactions is a miner best interest since it reduces the block verification time and so decreases the chances of competing blocks. This optimization is not required when Mining on Unverified Blocks Heuristic (MUB) is in effect in the network.

### Immediate Block Header Propagation (IBHP)

When a block header of an up-to-date block is received, nodes will forward the block header before checking the transactions or the validity of the block, and only checking the block PoW and height at forward time. This allows the header to spread over the network in less than a second.

### Two Prioritized Streams for each Connection protocol (2PSC)

Each network connection comprises two logical bidirectional streams with two different priorities. The high priority stream is used to send the block header immediately even if a lower priority message is being send on the low-priority stream.

### Mining on Unverified Blocks Heuristic (MUB)

Nodes can then start mining an empty block on top of the header even if the transactions are still missing, during a fixed interval. After that interval, they resume mining in whatever block they were mining before. These empty blocks reduce the effective

bandwidth and block-chain storage usage, but simulations show that if DBI is used, the number of empty blocks generated, and the space required for storing the empty blocks and the reduction in TPS is low.

### Local Route Optimization Protocol (LRO)

To reduce the number of stale blocks is important to reduce the inter-miner transfer latency. Rootstock network is dynamically optimized to reduce the inter-miner latency and to prioritize traffic between miners. In other words, Rootstock embeds a fast relay network in the peer network, enhancing the gossip protocol with geolocation and optimal local routes. The inter-miner block forwarding path is a critical path for block propagation and so is of extreme importance to the peer network. The existence of non-miner network nodes in the peer network in the critical path tend to increase the rate of stale blocks. Non miner-nodes (such as end-users or monitoring nodes) in the critical path can only serve the miners only as weak anonymization hops. To create the critical paths from only local node decisions, a prioritization of nodes is done using the LRO protocol. This protocol creates a dynamic embedding of a directed acyclic graph (DAC) into the random topology of the Rootstock network, where this DAC optimally connect the miners.

### Re-using the Bitcoin Mining Network

A concentrated mining network, having large mining pools, tend to generate much less state blocks than a complete distributed mining topology. Therefore, regarding fast payments, cryptocoins based on SHA-256D PoW have an advantage over non ASIC-friendly PoW based cryptocoins.

### The real topology of the network

Bitcoin design assumes the network is similar to a random graph, having a certain average out-degree and in-degree. While this is far from true in reality, network nodes take local decisions to avoid forming geographical clusters (at least for the out-bound connections). This is not the best topology to help block propagation. The best topology for block propagation is one that serves the top miners better, by encouraging direct connections between them or by routing blocks faster between them. Also a direct miner-to-miner backbone can help to decrease notably the number of stale blocks. This has been proposed for Bitcoin to increase resilience from attacks. Rootstock uses the LRO heuristics to establish a dynamic miner's backbone, without incurring in the cost of miner-to-miner authentication, miner's privacy, disclosure of IP addresses and possibly associated DoS attacks.

### The PoW function Verification Time

SHA-256 is very fast to evaluate and so the Bitcoin PoW verification time is negligible. A scrypt PoW, on the contrary, may take from 3 to 30 milliseconds to evaluate depending on the parameters chosen (GPU or ASIC “resistance”). To protect the network from spamming and DoS attacks, each node needs to verify the block PoW before forwarding the block

header again, so the verification delay gets multiplied by the number of hops in the block critical path between miners.

### Client Networking Stack

Once a node receives a block header the best it can do to reduce the creation of stale blocks in the network is to forward it as soon as possible. This means that all other node activity should be paused or stopped. Rootstock design allows low-priority operations to be immediately canceled and accept re-tries. To allow immediate forwarding, the client networking stack does not block the client in transaction verification procedures or other housekeeping activities, such as chain re-organizations. This is achieved by a Rootstock client that is allows multi-threading and dynamically assign thread priorities to boost the thread that has received the block header.

### The Block Overhead

Block headers in most cryptocurrencies are small (~100 bytes) so the header size (compared to the whole block size) does not pose a significant overhead. The Rootstock header is larger, but the block header overhead does have a noticeable negative impact on the propagation time, since low-level network MTU is generally 1500 bytes, which is above the block header size.

### Simulations

We've simulated the block propagation using a discrete event simulation built specifically for this purpose. The simulator simulates the interaction between a small set of top-miners, each one in a random graph where the hop distance between them is near the average distance between nodes in the network. Even if this is not the worst case, since it is the best interest for top-miners to be well-connected, we assume miners perform not worse than the average. The simulated events are the creation of a block in one of locations and the propagation of the block to each of the other miner locations. The following results show the simulation Rootstock with a 5 block interval and 300 TPS (currently the block interval is 10 seconds). The key simulation result is that a transaction is accepted with probability 99.98% (reversal probability of 0.02%) before 20.35 seconds have elapsed. Note that this reversal probability does not take into account that the replacement fork may also contain the removed transaction, so in practice it may be much lower.

### Safe Merged mining

Merge mining is a technique that allows Bitcoin miners to mine simultaneously other cryptocurrencies with near zero marginal cost. The same mining infrastructure and setup they use to mine Bitcoins is reused to mine Rootstocks simultaneously. This means that, as RSK pays additional transaction fees, the incentive for merged mining is high. But it also means that the cost to attack the network using pump-and-dump or parallel chains is below the cost of attacking non-merged cryptocurrencies. RSK has several protections to

prevent attacks during the initial bootstrapping phase:

- Federated checkpoints: Rootstock clients expects checkpoints signed by the Federation members. The Federation will include exchanges and other highly secure parties involved in the success of the platform. Nodes use federated checkpoints to detect Sybil attacks and inform the user.

- Mined coins maturity: each miner coin has a 24 hours maturity time, slightly higher than in Bitcoin. The increase of coin maturity time reduces the incentives for pump-and-dump attacks.

- Checkpoints embedded in the source code

## Transaction Privacy

Rootstock does not provide by itself better transaction privacy than Bitcoin and relies on pseudonyms. Nevertheless, the VM of Rootstock is Turing-complete, , so anonymization technologies such as CoinJoin or AppeCoin can be implemented securely without third party trust.

## Security

Merged mining has not been widely used by alt-coins because during the initial cryptocurrency bootstrap period it allows large Bitcoin mining-pools to disrupt the new cryptocurrencies with 51% attacks. RSK implements federated checkpoints as a safe way to bootstrap the platform and notably reduce this risk. Also RSK will be launched with a minimum hashing power equivalent to 30% of the Bitcoin hashing power. The Rootstock Foundation will monitor the network health and will use its alert system to inform users and protect the network from rollback attacks.

## Scalability

RSK can scale far beyond Bitcoin in its current state. A RSK payment requires a fifth of the size of a standard Bitcoin payment, and the block payload per time interval is 8 times higher than in Bitcoin. Also RSK will provide several user-selectable signature schemes: ECDSA, Schnorr and Ed25519. The last one being in general several times more performant than Bitcoin ECDSA curve.

All things equal, RSK consumes on average 50% less bandwidth than Bitcoin, since blocks do not contain transaction data, but only references to previously known transactions. Storage and Bandwidth usage can be further reduced using probabilistic verification and fraud proofs.

### Probabilistic Verification and Fraud Proofs

The cost of owning a full node is the main factor that affects the degree of centralization of

a cryptocurrency. The higher the cost, the highest the centralization. We believe however that the maximalist position on decentralization implies that the cryptocurrency cannot become a global payment network. Both goals are in contradiction. Bitcoin already provides a highly decentralized network as the block chain size limit is sufficiently low to ensure most individual users can take part. This allows RSK sidechain to increase scalability beyond Bitcoin while having Bitcoin network as a guard against centralization of the control of the currency.

We believe that a tradeoff between third party trust, network nodes trust and self-verification is possible, and we invite users to find the ratio they are comfortable with. In RSK platform allows nodes to store and validate a subset of the full block-chain, in order to reduce the node cost. This is done by probabilistic verification and fraud proofs. Probabilistic verification is a technique where a (partial) node chooses randomly which blocks it will verify, and accepts the remaining blocks as good as long as some conditions are met: some time has elapsed, some confirmation blocks have been added, the network connectivity is adequate, there was no valid fraud proof broadcast and optionally some authoritative checkpoints have been broadcast. Fraud proofs are blocks that are flagged as "fraudulent". When a node receives a fraud proof it checks if a block with the same height has been locally accepted (but not validated) and if so it validates the block. If it is invalid, then the local best chain is reorganized accordingly. The cost to broadcast a fraudulent fraud proof is high since fraud proofs also carry proof of work. A node that receives a fraudulent fraud proof from a peer bans the cheating peer. If necessary, nodes will request an initial proof of work from peers to prevent cheap DoS using compromised IPs. Miners (both PoW and Federated) must be full-nodes, so an attacker withholding block data (but broadcasting the header) does not affect the best-chain, as miners will rapidly discard the attackers block.

## Conclusions

RootStock represents the culmination of 4 years of blockchain technology improvements and it will allow the cryptocurrency ecosystem to make use of the best features of programmable money and payments while increasing bitcoin (the currency) value.

It will allow developers around the globe to create personal and corporate decentralized solutions that run in the most secure network worldwide with low transaction cost that fit an ample range of needs.

It will allow Bitcoin miners to participate in the Smart Contract market adding significant value to the mining industry and ensuring its long term sustainability.

It will contribute to the creation of a broader base of miners strengthening Bitcoin network's security.

It will enable the development of a decentralized, instant and inexpensive financial system that will create inclusion and opportunities for three thousand million people who remain unbanked and financially impaired in our world.

**RootStock Core Team**