RSK

ROOTSTOCK PLATFORM

BITCOIN POWERED
SMART CONTRACTS

WHITE PAPER

RSK

Bitcoin Powered Smart Contracts

White Paper
Overview

Revision: 11
Date: January 29, 2019
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, several cryptocurrencies have been launched with stateful VMs, capable of supporting Turing complete programming languages, unleashing the full power of smart contracts. Thousands of decentralized applications that interact with smart contracts, called dApps, have been developed and new use cases have emerged. However, each new platform uses a new highly speculative and volatile native token.

Since its genesis block on January 3, 2009, Bitcoin has consolidated itself as the most adopted, most robust, most secure, best store of value, and the safest protocol between all cryptocurrencies. But most dApps require more complex rules that cannot be coded into Bitcoin’s forth-like predicates. This limitation triggered the birth of RSK in 2015, and the launch of its Mainnet in January 2018. RSK is a platform that enables the execution of smart-contracts that use bitcoin as the native asset, contributing to Bitcoin’s value as the leading global cryptocurrency and expanding its reach to all potential use cases of dApps. RSK is a Bitcoin sidechain, so it has its own network, and its own blockchain, but not its own token. RSK network provides enhancement compared to Bitcoin, such as faster transactions and better scalability.

RSK is an evolution of two platforms, QixCoin and Ethereum. QixCoin was a turing-complete cryptocurrency created back in 2013 by some of the RSK founders. QixCoin introduced the concept of pay per execution, currently known as transaction “gas.” However, RSK inherits several key concepts from Ethereum, such as its account format, VM and web3 interface. Therefore, RSK is highly compatible with Ethereum compilers, tools and dApps.

Compared to Bitcoin, RSK provides an improved payment experience with near instant confirmations. And yet, RSK is also based on proof-of-work by supporting SHA-256D merged mining, the same consensus protocol and mining network that secures Bitcoin. As of January 2019, RSK has more than 40% of Bitcoin’s hashing rate, resulting in being the most secure smart-contract platform on the planet in terms of energy invested in securing the blockchain.

To enable bitcoins to flow in and out of RSK, RSK has a two-way-peg to Bitcoin. When Bitcoins are transferred into the RSK blockchain, they become “Smart Bitcoins” (ticker RBTC[1]). Smart bitcoins are equivalent to bitcoins living in the RSK blockchain, and they can be transferred back into Bitcoins at any time at no additional cost, except for standard RSK and Bitcoin transaction fees. RBTC is the native currency used on the RSK blockchain to pay miners for transaction and contract processing. There is no currency issuance: all RBTCs are created from the Bitcoins coming from the Bitcoin blockchain.

RSK currently enhances Bitcoin in the following areas:

[1] In this white paper “RSK protocol” refers to the protocol specification. “RSK reference node” refers to the reference implementation. The native RSK currency is the “Smart Bitcoin. The “ticker” or symbol of the smart bitcoin is “RBTC.” “BTC” or “bitcoin” refers to Bitcoin’s native currency. “Bitcoin” refers to the Bitcoin protocol.

- Turing-complete RSK Virtual Machine (RVM) allowing smart-contracts, highly compatible with Ethereum's VM (EVM)
- Average first confirmation of transactions in thirty seconds
- Merged mining with Bitcoin
- Two-way peg sidechain (currently a federated peg)
- Protection from Selfish-mining using the DECOR+ protocol

Also, the RSK community is strongly unified to follow the original vision to add in future network upgrades, the following features:

- Storage rent
- Block propagation optimizations
- Parallel transaction processing
- A transaction compression protocol (LTCP) for higher scalability
- Support for an additional, more performant VM based on Java byte-code or WAsm
- Hybrid Federation/Drivechain-based peg

The future features are described as RSK Improvement Proposals (RSKIPs) described in the following repository https://github.com/rsksmart/RSKIPs, along with PoC code.

RSK is a community-driven project. RSK Labs is a company founded in 2015 to develop the reference implementation of the RSK protocol, and since 2015 has paid salaries to some of the most prominent RSK Core developers. Also, RSK Labs provides platform information on the www.rsk.co website and hosts several informational services.

Useful Resources to Get Started

RSK Labs Website: https://www.rsk.co/
RSK Stats: https://stats.rsk.co
RSK Explorer: https://explorer.rsk.co/
RSK Faucet: https://faucet.rsk.co/
RSK Network Status: https://twitter.com/RskSmartNetwork
RSK Fee Comparison: http://rskgasstation.info/

RSK-Compatible Software Wallets:

MyCrypto: https://mycrypto.com
Jaxx: https://jaxx.io/ https:/
iBitcome: /www.ibitcome.com/
Metamask: https://metamask.io/

RSK-Compatible Hardware Wallets:

Ledger: https://www.ledger.com/
Trezor: https://trezor.io/
D'CENT: https://idcent.io/

Why RSK is Important for the Bitcoin Ecosystem

In the following sections we list several reasons why RSK is important for the Bitcoin ecosystem.

Alignment of Bitcoin Stakeholders and Protection of Value

One of RSK's goals is to provide a smart-contract platform that benefits the main stakeholders of the Bitcoin ecosystem and its community. This philosophy is directly reflected in its core architecture where Bitcoin miners provide the hashing power required to secure RSK and industry leading companies integrate the Federation that holds the keys that protect the funds locked in the two-way peg system. RSK governance model aims to represent all actors of the community, RBTC stakeholders, miners, federation members, as well as dApp developers and end-users. In the long term, the community plan is to enable objective but non-binding signaling mechanisms embedded in transactions and blocks so users can signal with their stake, wallet applications and senders can signal by tagging transactions, miners can signal by tagging blocks, and receivers can signal by tagging accounts for an even more decentralized and democratic governance.

Protection of Bitcoin Miners Investment

In May 2020, Bitcoin mining profitability will fall due to the decreasing block reward from 12.5 BTC to 6.25 BTC. The profitability reduction may imply the end for many mining enterprises and individuals, and vast amounts of mining hardware that secured Bitcoin to be unplugged. RSK, thanks to its merged mining capabilities, gives these miners the opportunity to keep their business going longer. 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 RSK mining compensates the profitability gap.

Also, by merge-mining today, miners will be supporting new unforeseen applications, which in the future may provide whole new business opportunity.

Stable Value Asset Issuing by Collateralized Bitcoins

RSK enables asset issuing with prices pegged to that of a fiat currency or other stable commodity by locking bitcoin as collateral. Stable assets achieve lower volatility while keeping Bitcoin as a reserve currency increases overall Bitcoin value. The lock of high amounts of Bitcoin reduces liquidity and therefore contributes to the rise of Bitcoin's value. However, most importantly, these Bitcoin-baked stable tokens on RSK will enable stable-coin micro-payments which allow billions of inhabitants currently underserved by the legacy financial system to participate in the global digital economy.

RSK at the Forefront of Bitcoin Sidechain Technology

RSK Labs is exploring, researching and implementing key concepts vital to any other future sidechain for Bitcoin. The success of RSK will encourage other sidechain developers to follow and to benefit from the efficient merge-mining infrastructure created, the drivechain opcodes proposed, and the technology developed for the secure creation of multi-sig federations by RSK Labs. By open-sourcing software, firmware and hardware designs, RSK Labs is advancing science and improving the functionality and security of the cryptocurrency ecosystem as a whole.

RSK as a Low-Cost Bitcoin Payment Network

Currently a Bitcoin transactions costs 24 ¢ on average[2], while RSK cost is 0.46 ¢ [3], which is 50 times lower. This is a radical improvement. But also, Bitcoin fees usually rise or fall based on block space demand, and we foresee a growing demand for on-chain transactions. After several unsuccessful attempts to increase Bitcoin's block size though hard-forks, and after the one-time Segwit space upgrade, there is no plan in the Bitcoin community to increase the block size. We can expect Bitcoin transaction fees will become prohibitively high for most applications involving personal daily transactions. RSK blocks can hold many more transactions than Bitcoin blocks due to the reduced size of its transactions, therefore RSK will naturally offer much lower fees, with the same transaction volume. In the following table we briefly compare Bitcoin against RSK.

Parameter	Bitcoin	RSK
Average block confirmation time	10 minutes	30 seconds (miners can lower it to 15 seconds)
Suggested confirmation time for exchanges	30 minutes (3 blocks)	60 minutes (120 blocks) with current merge-mining hash rate (40%).
Max. transactions per second	3.3 tps (assuming an average size tx)	10 tps (external transactions, as of January 2019) 20 tps (internal transactions)
Current average transaction cost	24 ¢	0.46 ¢

The cost of Bitcoin transactions is directly related to the value of the block reward. Adding a transaction to a block delays its propagation. Every millisecond spent in propagation is paid proportionally to the block reward because it decreases the likelihood the block is chosen by the network. Set-reconciliation techniques (such as Bose-Chaudhuri-Hocquenghem codes provided by the Minisketch library) could, if implemented into Bitcoin, reduce this dependence. Currently, if Bitcoin price increases then transaction fees will increase as well. It is believed that Bitcoin will become a sort of inter-banking clearing system, but not a payment network. Also, is important to note that off-chain payment systems, such as the Lightning Network are emerging, but these networks will probably increase the need for on-chain transactions for channel settlement and top-up, also pushing the transaction cost up. As this cost rises, users will switch to platforms with lower transaction costs. RSK provides an excellent opportunity to transact in Bitcoin at a much lower cost.

Why RSK is important for Ethereum Users and Developers?

Increase Your DApp User Base

RSK has a unique user base initially comprised by Bitcoiners in Latin America. Now RSK is growing strong in both Latin America and Asia. By seamlessly deploying compatible DApps in both Ethereum and RSK, developers and companies can reach a wider user base

[2] https://bitcoinfees.info/

[3] http://rskgasstation.info/

while reducing their dependency to any particular blockchain. Also, currently there are several federated solutions to bridge Ethereum and RSK and transfer tokens from one blockchain to another, so the same token can live in both blockchains.

Foster the Standardization of EVM/Web3

The Ethereum community created the smart-contract virtual machine (EVM) and the interphase for decentralized applications to interact with it (Web3). By adopting these standards, RSK facilitates the process for developers to migrate their applications to RSK and to re-use most of the infrastructure software developed for Ethereum. But it also helps with standardization, by providing unifying learning material and reducing the need to learn yet another execution architecture and programming language. At the same time, all tools developed by the RSK ecosystem will also become available to the ETH users.

Reduce Persistent Chain Fork Risks

Ethereum periodically undergoes network upgrades. One of the oldest announced and yet still debated Ethereum hard forks is the migration from Proof-of-Work consensus to Proof-of-Stake. This is a radical technological and economic change, which is expected to be confronted by Ethereum miners. A new chain split will force developers to choose between the original PoW chain and the new PoS chain. Also, there are still uncertainties regarding the security and stability of the new consensus protocol. In case of failure, all users owning ether may be economically impacted, so the change may be contested by the Ethereum community. In addition to this, the Ethereum core developers have implemented and will implement changes in the money supply and proof of work algorithm which erodes the immutability and neutrality of the platform. RSK does not possess a native speculative token, and smart Bitcoins can always be moved back to Bitcoin in case a user does not agree with a community-supported RSK network upgrade. Therefore, the RSK community shows a very low level of confrontation, which minimizes the risk of a community split. On the other side, Bitcoin has a tradition of rejecting hard forks. Therefore, RSK provides a much more stable platform in the mid- and long-term.

Protect R&D Investment from 0-Day Ethereum Security Vulnerabilities

Most blockchains undergo periodic network upgrades and frequent software updates. For most blockchain projects, the technology is still experimental, and the protocols are not yet set in stone. Ethereum and RSK are far from mature. This means that new security vulnerabilities could be found, as they have been found and exploited in Ethereum’s past. Even if RSK, which has an outstanding security track record, it’s not free from risks. Yet the existence of two compatible platforms reduces the risk that resources dedicated to the development of a DApp are lost due to a catastrophic failure of a platform. The probability of a joint failure is much lower, especially taking into account the different consensus protocols involved.

Increase Transaction Throughput by Porting DApps to RSK

RSK technically stands over other platforms because of four community proposals that can provide higher on-chain scalability. The first is parallel transaction processing, specified by RSKIP4, which enables multi-core architectures to achieve full use of processing cores for transaction processing. This in turns allows for the increase of the block gas limit, enabling higher transaction throughout. The second is LTCP, specified by RSKIP53, which enables for the compression of transactions and the aggregation of transaction signatures such that many more transactions can be processed with the same amount of space and processing resources. The third is shrinking-chain scaling, which is an extension of LTCP to reduce signature space and signature processing even more. The fourth is a new improved VM that provides JIT compilation that is being tested, and whose specification is being finalized to be proposed as an RSKIP.

By making use of these improvements, RSK can support higher transaction volume, and/or lower transaction cost.

Reduce Transaction Cost by Porting DApps to RSK

Transaction cost is a limitation to many DApps. As RSK is preparing to grow the on-chain processing capabilities with the scaling proposals described above, a decrease in transaction fees is expected. This will enable use cases which have become prohibitively expensive on Ethereum.

Reduce Devaluation Risk for Coin Stakes and Stores of Value

Many DApps require staking cryptocurrency. Stakes are security deposits aimed to provide priority for being chosen to provide a service. Also, some DApps require security deposits as insurance against malicious behavior. Yet other DApps, such as DAOs and crowdfunds, require funds to be locked for long periods of time for vesting. In all these situations, the volatility of the native cryptocurrency reduces the incentive to lock coins. Bitcoin has shown greater resilience as a platform and lower variance as a store of value, qualities inherited by the Smart Bitcoin. Therefore, RSK is better positioned to serve these applications.

RSK Use Cases

The RSK platform provides “Turing-complete”[4] smart contracts as proposed by Nick Szabo in 1993. At the same time, RSK’s VM is backward compatible with Ethereum VM, hence RSK gives the opportunity to developers working on Ethereum to benefit from the robustness of the Bitcoin currency and the security of the RSK blockchain. Below we present a list of potential smart contracts and use cases that can be developed over RSK.

Micropayment Channels

Micropayment channels allow two parties to perform secure, frequent and generally low-valued payments without paying on-chain transaction fees for each payment, but rather by paying a one-time fee when the channel is closed. These applications will be key building blocks for a fair and inclusive new financial system which will provide alternatives to the billions of users underserved by the current system.

2nd Layer Off-Chain Payments Networks and State Channel Networks

Micropayment channels provide the basis for second layer off-chain payment networks. Second layer networks are capable of routing payments from any participant to any other, provided there is enough channel capacity, and with low third-party trust.

Second layer networks can be either instantiated by random graphs of nodes or become hub-and-spoke networks, where a low number of heavily interconnected hubs channel most inter-user payments. State Channel networks enable a set of participants to execute multi-party protocols created on-the-fly, such as games, which could result in on-chain state changes, such as token transfers, but delaying all on-chain effects to the moment the channels are closed, providing no party attempts to cheat. RSK’s rich programming language enables all these kinds of second layer networks to be implemented directly with minimal hassle.

Decentralized Exchanges (DEXs)

Decentralized Exchanges enable the creation of decentralized token and cryptocurrency markets without third-party trust. RSK supports Decentralized Exchanges in all their variants, with online or off-chain order books, with succinct proofs for order matching, from the simplest TierNolan's protocol to the more complex protocols based on zk-SNARKs.

Retail Payment Systems

RSK allows BTC to be adopted globally for every-day retail transactions. One of Bitcoin’s main limitations for retail use is its confirmation time (from ten minutes to one hour to ensure irreversibility). RSK allows consumers to benefit from Bitcoin security with payment confirmation in just a minute. Merchants will be able to accept payments

[4] Although the contracts may be Turing-complete, since they are written for a Turing-complete instruction-set, using general-purpose languages, the resources available to the VM are limited.

almost instantaneously without requiring third party gateways. RSK also provides a higher amount of transaction per second (tps), required to succeed in the retail market. The RSK network uses the DÉCOR+ consensus protocol to prevent mining centralization when transaction volume increases.

Escrow Services

RSK allows the creation of smart escrow services where oracles can sign a transaction defining whether the escrow should be released without the oracle having custody of the funds under escrow.

Crypto-Assets Creation

RSK allows the creation of crypto-assets (tokens, altcoins, etc.) secured by the Bitcoin network. These assets can be loyalty points, utility tokens, or security tokens. Also, the tokens can be fiat-denominated and backed up fiat currency. Eventually they could be created by governments or Central Banks as a way to provide low-cost programmable money to all their citizens.

Bitcoin-Backed Token Offerings (BTOs)

BTOs are a special case of crypto-asset creation when Bitcoins are exchanged to newly minted tokens. This tool has been widely used for blockchain crowdfunding, such as Ethereum crowdfund.
In the particular case of RSK, BTOs allow startups to receive the funding directly in Bitcoin, which is the most secure and stable crypto-currency that exists, while creating the tokens on the RSK blockchain secured by the Bitcoin hash rate merge-mining RSK. The whole process of token issuance can be made trustless using the services of RSK bridge.

Asset Securitization

RSK enables the creation of digital tokens backed by real assets. This can be used 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 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. RSK enables fiat-denominated tokens and leveraging the existing infrastructure of exchanges and cash-out options so crypto-assets can provide remittances at significantly lower costs.

IP Protection/Registry

RSK enables the development of contracts that provide Proof-of-Existence (PoE). PoE enables individuals and companies alike to prove 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 ID and land registration mechanisms.

Voting Systems

RSK enables the creation of digital votes that could enable extremely secure and transparent elections at minimal cost. Also, it could be used to secure a transparent voting process for company boards or decentralized organizations.

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 enables the development of scalable, digital and programmable micro-lending contracts that could provide access to credit to the three billion poorest inhabitants in the world.

Supply Chain Traceability

RSK enables 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 international trade as well as the retail, food and healthcare industries among others. As with 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 enables the creation of digital global registries as secure as the Bitcoin Blockchain at an 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 have become major risks and user concerns. Also, the game companies may face legal and security hurdles by having users’ virtual money in consignment. As the world globalizes, so will virtual games, and players will feel uncomfortable with the fact 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 Smart Bitcoins or RBTC) for their in-game payments, or create a private digital asset that is protected by RSK. RSK payments provided by second layer off-chain networks 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 a URL or scanning a QR code, trading can be triggered using the standard player's external e-wallet software, as well as paying commissions to the gaming company.

Internet-Gambling and Prediction Markets

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

Fair-Gaming

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.

Non-Fungible Tokens (NFTs)

NFTs are unique tokens which can be linked to a specific property, license, product or service. NFTs can be easily created on RSK allowing use cases in multiple industries ranging from sports collectibles to gaming player features or “skins.”

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 exchange) based on a Federation secured with custom HSM-modules. Once the drivechain protocol becomes implemented on Bitcoin, the original plan is to move to a hybrid-drivechain mechanism
- A selfish-mining resistant merge-mining-based consensus protocol
- A low-latency block-propagation network (for fast payments)

Turing-Complete Virtual Machine

RSK virtual machine (RVM) is the core of the Smart-contract platform. Smart-contracts are executed by all network full 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 contract-persistent memory. The RVM is compatible with EVM at the op-code level, allowing Ethereum contracts to run flawlessly on RSK. Currently, the VM is executed by interpretation. In a future network upgrade, the RSK community is aiming to improve the VM performance substantially. One proposal is to emulate the 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 may bring RSK code execution to a performance close to native code.

Main features:

- Independent VM, but highly compatible with EVM at the opcode level
- Run Ethereum DApps with the security of the Bitcoin network
- Performance improvement pipeline documented in numerous RSKIPs (RSK improvement proposals) created by the RSK community

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 Smart Bitcoin (RBTC) is two-way pegged to the BTC.

In practice, when BTC are exchanged for RBTC, no currency is “transferred” between blockchains in a single transaction. When a transfer occurs, some BTCs are locked in Bitcoin and the same amount of RBTC is unlocked in RSK. When RBTC needs to be converted back into BTC, the RBTC get locked again in RSK and the same amount of BTC are unlocked in Bitcoin.

Fully trust-minimized and third-party-free two-way pegs can be created if two platforms have Turing-complete smart-contracts. But since Bitcoin does not currently support smart-contracts nor native opcodes to validate external SPV proofs, part of the two-way peg system in RSK requires trust on a set of a semi-trusted third-party (STTP), that we collectively call the Federation. No single STTP can control the locked BTCs, but only a majority of them has the ability to release BTC funds. Each STTP has a key to protect the BTC that are locked, and upcon receiving commands from the RSK blockchain, it unlocks the BTC that need to be transferred back into Bitcoin. Note that if a user transfers BTC into RBTC and back, they will normally not receive bitcoins that are directly connected by UTXOs with the original BTC sent. Therefore, do not lock RBTC for specific users, but for the whole RSK network.

The locking and unlocking of funds is done by the Federation without any human intervention. A requirement for being part of the Federation is the ability to audit the proper behavior of the software that powers the node, especially regarding the correctness of the component that decides on releasing BTC funds. RSK Labs developed a firmware for a Hardware Security Module (HSM) that STTPs can use, in order to provide maximum security for their private keys and, in the future, to be able to enforce a transaction validation protocol to further improve security.

As of January 2019, the RSK Federation comprises 15 well-known, and highly-secure notaries. Leading Blockchain companies currently integrate the RSK Federation and participate in an autonomous protocol to securely lock Bitcoins. In exchange for their work, Federation members are awarded 1% of the transaction fees generated on RSK, in order to cover the hardware and maintenance costs. There is an automated process to modify the composition of the federation. Each federation member can either accept or reject a composition change. The process, which is infrequent, is commanded by a smart-contract, so it’s open to the public. The protocol has a consensus enforced delay of one week until the change is activated. This allows users to transfer the Bitcoins back to the Bitcoin network in case they do not trust the new Federation composition.

If Bitcoin adds special opcodes or extensibility to validate SPV proofs as a hard-fork, and once the new system is proven to be secure and trust-free, the Federation role as STTPs will no longer be necessary, and the RSK community may implement the changes to adapt RSK to the trust-free system. The RSK community have also proposed a drivechain BIP, which enables miners to participate in the securing of the Bitcoins in the peg, and decreases the trust required on the STTPs even more.

Merged Mining

Satoshi consensus, based on proof-of-work, is the only consensus system that prevents the rewrite of blockchain history at a low cost. The academic community is advancing the knowledge and study of proof-of-stake as an alternative, but currently PoW provides the highest proven security. Merge mining is a technique that allows Bitcoin miners to mine other cryptocurrencies simultaneously with nearly zero marginal cost. The same mining infrastructure and setup they use to mine Bitcoins is reused to mine RSK simultaneously. This means that, as RSK rewards the miners with additional transaction fees, the incentive for merged mining becomes high.

We have identified three phases for RSK merge-mining growth:

- bootstrapping phase: merge-mining is below 30% of Bitcoin hashrate.
- Stable phase: merge-mining is between 30% and 60% of Bitcoin hashrate.
- Mature phase: merge-mining is higher than 60% of Bitcoin hashrate.

RSK has left behind its bootstrapping phase, when rogue merge-miners could revert RSK blockchain at a low cost. As of January 2019, more than 40% of Bitcoin miners are engaged in RSK merge-mining. But as RSK fees remain low compared to Bitcoin block reward, the cost to attack RSK by a double-spent is lower than Bitcoin's.
RSK has some properties to reduce the risk of double-spend attacks, such as long miner rewards maturity. Still RSK Lab research team has developed several protections to prevent attacks during the stable and mature phases of the project:

- **Signed notifications**: RSK clients can make use of signed notifications by notaries. Nodes can use these notifications to detect Sybil attacks and inform the user.
- **Transparent double-spend trails**: this is a method where all RSK merge-mining tags are augmented with additional information that can be used to detect selfish RSK forks that are public in the Bitcoin blockchain. Selfish-fork proofs are automatically constructed and these proofs are presented to the RSK nodes, which spread them over the network. The proofs force nodes to enter a "safe mode" where no transaction is advertised as confirmed. The safe mode prevents merchants and exchanges from accepting payments that could be double-spent. Once the proven selfish-fork is outpaced by the RSK mainchain in accumulated PoW, the network reverts to its normal state. This method is a deterrent for any RSK double-spent attempt (where the malicious miner still tries to collect Bitcoin rewards when mining the selfish fork).

Once the platform enters the maturity phase, we estimate the security of RSK will be enough to support the economy of worldwide financial inclusion.

Main features:

- DECOR+ consensus protocol
- one-day maturity for mining reward
- No loss of efficiency in Bitcoin mining expected from merge mining (for late mid-state switching)

Fast Payments and Low Latency Networks

RSK already enables second layer off-chain payment networks, but still RSK aims to provide a much better on-chain payment network compared to Bitcoin. To achieve this, RSK adopts the DECOR+ and FastBlock5 protocols, which allow reaching a fifteen second average block rate that does not create incentives for mining centralization and selfish-mining.

Main features:

- fifteen to thirty second block intervals (depending on the miner's state switching efficiency)
- Full network propagation of last competing blocks to prevent selfish mining and

reduce stale block rate

- New network command to spread block headers with time critical priority
- DECOR+ protocol for reward sharing between competing blocks
- GHOST protocol for chain weighting

Since the creation of Bitcoin there has been a race towards lower intervals for PoW blockchain based cryptocurrencies. But low block interval may impact the stability and capability of the cryptocurrency network, so several design factors must be considered. First of all, the most important factor that affects the viability of short confirmation intervals is the number of stale blocks generated. The main factor that affects the stale block rate is the block propagation protocol. For RSK we've carefully analyzed this protocol and we've run simulations in order to verify the performance, usability and security of the network.

In Bitcoin, when two or more miners have solved blocks at equal height, there is a clear conflict of interest. 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 care which one is chosen from the two. However, all the remaining honest miners and users have a rational preference that the same block tip is chosen, because this reduces the reversal probability. The DECOR+ consensus protocol sets the right economic incentives for a convergent choice, without requiring further interaction between miners. The DECOR+ protocol is a reward sharing strategy that incentivizes resolving the conflict economically such that:

1. The conflict is resolved deterministically when all parties have access to the same blockchain state information
2. The chosen resolution maximizes all miners’ revenue (collectively) and for both the miners in conflict in case block rewards differ by a high margin
3. The chosen resolution maximizes censorship-resistance if competing blocks have approximately similar rewards
4. Resolving the conflict takes negligible time

Transaction Privacy

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

Scalability

RSK can scale far beyond Bitcoin in its current state. An RSK payment requires a fifth of the size of a standard Bitcoin payment. Using the proposed LTCP protocol, transaction size can be reduced to 1/50th of a Bitcoin transaction size. This immediately leads to a substantial increase in transaction volume capability. Besides, there are community proposals (RSKIPs) to enable user-selectable signature schemes: ECDSA, Schnorr and Ed25519. Because Ed25519 is more performant than Bitcoin ECDSA curve, using this scheme may lead to even more capacity.

RSK Feature Comparison

The following table is an attempt to compare RSK's main features with the features of other alternatives, including the Liquid sidechain (Blockstream), and the WBTC token (BitGo). Both Liquid and WBTC are pegged to BTC. We show that essentially RSK presents better technical solutions with a low impact on decentralization.

Item	**Bitcoin**	**Ethereum**	**Ethereum**	**Liquid**	**RSK**
	BTC	**ETH**	**WBTC**	**LBTC**	**RBTC**
Average confirmation time	10 min.	15 sec (GHOST)	Same as Ethereum	60 sec	15 sec to 30 sec (DECOR+GHOST)
Security threshold (due to selfish mining or collusion)	~30%	Lower than 30%	Same as Ethereum	50%	50% (DECOR+GHOST)
Turing complete smart-contracts	No	Yes	Yes	No	Yes
Adds value to Bitcoin	-	No	Yes	Yes	Yes (merge-mined)
Integration with Bitcoin	-	No	No	Sidechain	Sidechain
SPV clients	Yes	Yes	Yes	Yes	Yes
Hardware wallet integration	Yes	Yes	Partial	No	Yes
Transaction finality guarantee	Nakamoto consensus. SHA256D	Ethereum consensus. Ethash	Same as Ethereum	Federation	DECOR+GHOST. SHA256D PoW
Confidential transactions	No	Via contract	No	Yes	Via contract. Native support planned
Scalability [tps]	3 (6 with segwit)	Unbounded, currently 15	Same as Ethereum	3 (6 with segwit)	Unbounded, currently 10
Blockchain size	200 GB	> 1.5 TB	> 1.5 TB	~300 MB	~2 GB
Token peg security	--	--	Single Company	Federation	Federation
Token	BTC	ETH	WBTC	LBTC	RBTC

The Role of RSK Labs

RSK Labs has established itself as a strong community player by creating the reference implementation of the RSK node. Nowadays RSK Labs continues performing both technical and community activities such as:

- Pushing the development of the RSK reference platform through periodic updates
- Establishing collaboration with academia
- Maintaining community discussion channels, forums and FAQs
- Coordinating conferences and local meetups
- Promoting the use of the RSK blockchain
- Requesting and publishing periodic external security audits
- Participating in discussions of community proposed network upgrades
- Security auditing the RSK codebase
- Advising governments, startups, entrepreneurs and companies of the best ways to benefit from the RSK network

RSK Labs continuous commitment on RSK is rewarded by the RSK platform: 20% of the platform transaction fees are paid to an account controlled by RSK Labs.

The Future of RSK

The RSK roadmap has been established by the RSK community. During the first years of RSK development, RSK Labs had an active role building the reference implementation. After RSK was launched, RSK Labs continued to be highly involved with the community by improving the codebase and proposing improvements through the RSKIP proposal repository system. The repository helps the community members to coordinate discussions, rejection, acceptance and deployment over multiple codebases. The amount of improvement proposals is vast. Here is a list of some key proposals as of December 2018:

Distributed Memory, Dynamic Contract Dependency, Parallel Execution using static contract dependencies, Parallel Execution using runtime contract dependencies, Shift Operations, Block Size Limit, Persistent Storage Rent Paid by Code, Verification-less mining, Negotiated Minimum Gas Price, Transactions never invalidate blocks, TXINDEX Opcode, Contract Sleep, Support for stable assets & token issuance, Reward Manager Smart Contract (REMASC), Simplified Reward Manager Smart Contract (REMASC), Combined State Tree, Simpler Persistent Storage Rent, Fast Hibernation Wakeup using Trie, RSK Address formats, Survive and Ephemeral Memory Spaces, Efficient Persistent Storage Rent, Commit to number of Merkle tree elements, Onchain PoUBS, New Binary Trie, Memory caches, DUPN and SWAPN opcodes, Highly Efficient Storage Rent, Ephemeral segwit, Change in Account creation cost, Code Pagination, Hibernation Compression, Double-Hashed Addresses, CODEREPLACE opcode, Contract const DATA Sections, Managing BridgeMaster Federation Members, Transaction Encapsulation, Single Address Smart Wallets, Signature Compression, Multi-key Accounts, Basic Bridge for two-way-peg to Bitcoin, Extended Bitcoin Bridge Transactions, Remove world midstates from receipts, Sequential Address format, Remove the zero-byte discount in data, New Event Tree and Extended LOG, Block Mining Fees Information Mechanism, CALLNUM opcode, Informing average free gas per block, One-To-Many hub payment channels, Script Versions using HEADER pseudo-opcode, Memory-Mapped configuration register, Cache Oriented Storage Rent, Lumino Transaction Compression (LTCP), Transaction amount & destination privacy, Native Probabilistic payments, Sporadic Verification-less mining, Derivation Path for Hierarchical Deterministic Wallets, Handling Bitcoin Forks, Child Contracts, Checksum Address Encoding, Cache Oriented Storage Rent (collect at EOT version), Compressed block propagation using state trie update batch (COBLO), Double Signing for Delayed Signature Aggregation, Default TX Data, Native Off-Chain Probabilistic payments, Smoother Difficulty adjustment, DELEGATECALL as an instruction set extension, Managing BridgeMaster Federation Members

While some proposals are still immature, others have evolved after several rounds of discussion and have probably gained community support to become part of future network upgrades.

Conclusions

RSK is the first Bitcoin sidechain in production that provides Turing-complete Smart Contracts, compatible with the Ethereum standards, and secured by Bitcoin merge-mining.

RSK represents the culmination of five years of blockchain technology improvements and it enables the Bitcoin ecosystem to make use of the best features of programmable money and payments while increasing Bitcoin utilization and value.

RSK innovative design enables higher scalability and reduced transaction costs.

RSK enables developers around the globe to create personal and corporate decentralized solutions that run in the most secure network worldwide with a low transaction cost that fits an ample range of needs and use cases.

RSK enables Bitcoin miners to participate in the Smart Contract market adding significant value to the Bitcoin mining industry and ensuring its long-term sustainability. It contributes to the economic sustainability of Bitcoin miners and the growth of Bitcoin network's security.

RSK provides Ethereum users and companies a new compatible platform to deploy their solutions using Bitcoin as the native currency, relying on the Bitcoin mining infrastructure for its security, and accessing a wider user base.

RSK enables the creation of a decentralized, secure, open and inexpensive blockchain-based financial system that will create inclusion and opportunities for more than three billion people who remain unbanked and financially impaired in our world.