
RSK
ROOTSTOCK PLATFORM
BITCOIN POWERED
SMART CONTRACTS
WHITE PAPER

RSK

ビットコイン対応スマート・コントラクト

ホワイトペーパー
概要

改訂：11
日付：2019 年 1 月 29 日
著者：Sergio Demian Lerner

はじめに
開始にあたっての有用なリソース
RSK が Bitcoin Ecosystem にとって重要な理由とは?
Bitcoin ステークホルダーと価値の保護の一致
Bitcoin マイナー投資の保護
担保（Collateralized）Bitcoin による安定した価値のアセット発行
Bitcoin サイドチェーン技術の最前線にある RSK
低コストの Bitcoin 決済ネットワークとしての RSK
RSK が Ethereum ユーザーや開発者にとって重要である理由とは?
DApp ユーザー基盤の増大
EVM/Web3 標準化の推進
持続的なチェーン・フォークのリスクの低減
最初の日から、Ethereum セキュリティ脆弱性の R&D 投資の保護
DApps を RSK にポートすることによるトランザクション・スループットの増大
DApps を RSK にポートすることによるトランザクション・コストの低減
コイン・ステークと価値の保存の価値引き下げリスクの縮減
RSK 使用事例
テクノロジー概要
チューリング完全仮想マシン
サイドチェーン
マージ・マイニング
迅速な支払と低待ち時間のネットワーク
トランザクションプライバシー
スケーラビリティ
RSK 特長比較
RSK Labs の役割
RSK の未来
まとめ

はじめに

2008 年、サトシ・ナカモトなる人がビットコインを作り出して決済に革命をもたらしました。Bitcoin には、Nick Szabo 氏が 1993 年に紹介したコンセプト、いわゆる「スマート・コントラクト」のかなり限定された実装が含まれます。

以来、ステートフル VM にていくつかの仮想通貨が誕生し、チューリング（Turing）完全プログラミング言語に対応し、スマート・コントラクトの潜在能力をフルに発揮してきました。そして、dApps と呼ばれる、スマート・コントラクトと相関する何千もの分散型アプリケーションが開発され、新たな用途例が誕生してきました。しかし、新しい各プラットフォームは新規の高度に投機的で不安定なネイティブ・トークンを採用しています。

2009 年 1 月 3 日のジェネシス・ブロック以来、Bitcoin は数ある仮想通貨の中で最も採用され、堅固で安全で、最良の価値保存を有する、最も安心のおけるプロトコルとして評判を高めてきました。しかし、大半の dApps は、Bitcoin 等の述語にコード化することのできないいっそう複雑な規則が必要です。こうした制約が 2015 年に RSK の誕生、そして 2018 年 1 月の Mainnet の導入を加速化させたのです。RSK はネイティブ・アセットとして Bitcoin を使用するスマート・コントラクトの実装を可能にするプラットフォームで、グローバル屈指の仮想通貨としての Bitcoin の価値に寄与し、dApps のあらゆる潜在的な使用事例への拡張を実現します。RSK は Bitcoin のサイドチェーンであるため、独自のネットワークとブロックチェーンを有しますが、トークンは持ちません。RSK ネットワークはより迅速なトランザクションやスケーラビリティなど、Bitcoin に比べてより高度な機能を備えています。

RSK は 2 つのプラットフォーム、QixCoin と Ethereum が進化したものです。QixCoin は 2013 年、RSK 創始者の一部によって生まれたチューリング完全仮想通貨です。QixCoin はトランザクション「ガス」と呼ばれている実装ごとの決済という概念をもたらしました。ただし、RSK はアカウントのフォーマット、VM、web3 インターフェースなど、Ethereum のいくつかの重要な概念を承継しています。従って、RSK は Ethereum のコンパイラ、ツール、dApps と非常高い互換性があります。

Bitcoin と比べ、RSK はほぼ瞬間的な（near instant）確認による改善型の決済体験を提供します。同時に、RSK は SHA-256D マージ・マイニング、同じコンセンサス・プロトコル、Bitcoin を安全にするマイニング・ネットワークをサポートすることで、プルーフ・オブ・ワーク（proof-of-work）にも基づきます。2019 年 1 月現在、RSK は Bitocoin の採掘速度の 40% 以上で、ブロックチェーンの安全化に投資されるエネルギーの点で、最も安心なスマート・コントラクトのプラットフォームとなっています。

BItcoin が RSK に/から流出入できるよう、RSK は対 Bitcoin で two-way-peg（双方向の移動と取引が可能であること）となっています。Bitcoins が RSK ブロックチェーンに移管されると、「Smart Bitcoins」となります（ティッカーRBTC[1]）。Smart Bitcoins は RSK ブロックチェーンに生存する Bitcoins に相当し、標準 RSK および Bitcoin トランザクション手

[1]このホワイトペーパーでは、「RSK プロトコル」とはプロトコル仕様を指します。「RSK 参照ノード」とは参照実装を指します。ネイティブ RSK 通貨とは「Smart Bitcoin」のことです。Smart Bitcoin の「ティッカー」またはシンボルは「RBTC」です。「BTC」または「bitcoin」とは Bitcoin のネイティブ通貨を指します。「Bitcoin」とは Bitcoin プロトコルのことです。

数料を除き、いつでも、追加費用なしで Bitcoin に変換可能です。RBTC はトランザクションとコントラクト処理についてマイナーに支払われる、RSK ブロックチェーン上で使用されているネイティブ通貨です。通貨発行は伴いません：RBTCs は全て、Bitcoin ブロックチェーンに起因する Bitcoins より生成されます。

RSK は現在、次の領域で Bitcoin を包含しています：

- スマート・コントラクトを可能にし、Ethereum の VM（EVM）と非常に互換性の高いチューリング完全 RSK 仮想マシン（RVM）
- 30 秒以内というトランザクション平均初期確認。
- Bitcoin とのマージ・マイニング。
- Two-way peg サイドチェーン（現状、federated peg）
- DECOR+ プロトコルを用いるセルフィッシュ・マイニングからの保護

さらに、RSK コミュニティは、今後のネットワーク・アップデートに、以下の特長を組み込む本来のビジョンを踏襲すべく堅固に一体化されています：

- ストレージの使用料
- Block propagation 最適化
- 同時トランザクション処理
- より高度なスケーラビリティのトランザクション圧縮プロトコル（LTCP）
- Java バイトコードまたは WAsm を基盤とする付加的でより高性能の VM のサポート。
- ハイブリッド Federation/Drivechain ベースのペグ

今度の特長は、PoC コードとともに、以下のレポジトリにて、RSK 改善提案（RSKIP）として明示されています：https://github.com/rsksmart/RSKIPs

RSK はコミュニティ起動型のプロジェクトです。RSK Labs は 2015 年に設立され、RSK プロトコルの参照実装を開発することを目的としていて、2015 年以来、最も顕著に寄与してきた RSK Core 開発者たちに給与を支払ってきました。さらに、RSK Labs は www.rsk.co ウェブサイト上にプラットフォーム情報を掲示し、いくつかの情報サービスをホストしています。

開始にあたっての有用なリソース

RSK Labs ウェブサイト：https://www.rsk.co/
RSK Stats：https://stats.rsk.co
RSK Explorer：https://explorer.rsk.co/
RSK Faucet：https://faucet.rsk.co/
RSK Network ステータス：https://twitter.com/RskSmartNetwork
RSK 手数料比較：http://rskgasstation.info/

RSK 対応ソフトウェアのウォレット：

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

RSKRSK 対応ハードウェアのウォレット：

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

RSK が Bitcoin Ecosystem にとって重要な理由とは?

以降のセクションでは、RSK が Bitcoin Ecosystem にとって重要な理由をいくつか挙げます。

Bitcoin ステークホルダーと価値の保護の一致

RSK の目標の 1 つは Bitcoin Ecosystem の主要ステークホルダーとそのコミュニティに恩恵をもたらすスマート・コントラクトのプラットフォームを提供することです.この哲学は、Bitcoin マイナーが RSK を安全にするのに必要なハッシュパワーを提供し、業界有数の会社が 2-way peg システム内にロックされている資金を保護するキーを保有する Federation を統合するコア・アーキテクチャに直接反映されています。RSK ガバナンス・モデルはコミュニティの全てのアクター、RBTC ステークホルダー、マイナー、federation メンバー、dApp 開発者、エンドユーザーを代表することを目指しています。長期的には、コミュニティ計画はトランザクションやブロックに組み込まれている客観的ながらも拘束力のないシグナリング・メカニズムを有効化し、ユーザーが自身の出資をシグナルし、ウォレット・アプリケーションや送付者がトランザクションのタグ付けでシグナルを発し、マイナーがブロックをタグ付けしてシグナルして受領者がいっそう分散的で民主的なガバナンスのアカウントをタグして示唆できるようにすることを目指します。

Bitcoin マイナー投資の保護

2020 年 5 月、Bitcoin マイニング収益性は 12.5 BTC から 6.25 BTC へのブロック・リワードの分散化により、下落するでしょう。収益性の縮減は数多くのエンタープライズと個人、ならびに Bitcoin をアンプラグ化から保護する膨大な数のマイニング・ハードウェアにとって終わりを示唆するかもしれません.RSK は、マージ・マイニング能力のおかげで、こういったマイナーに対し、より長期にビジネスを維持する機会をもたらします。Bitcoin のマージマイナーたちがゼロという限界費用で両方のコインを採掘できることから、マイナーたちは RSK マイニングによる付加的収入が収益性ギャップに悪影響を及ぼさない限り、Bitcoin を採掘することができます.

また、マイナーたちは、現在のマージ・マイニングを通じ、新規の予知不能なアプリケーションを支援することとなり、将来的には、完全に新しいビジネス機会を提供します。

担保（Collateralized）Bitcoin による安定した価値のアセット発行

RSK は担保として Bitcoin をロックすることで不換通貨またはその他の安定コモディティにペグされた価格でのアセット発行を可能にします。安定アセットはより低いボラティリティを達成し、リザーブ通貨として bitcoin を維持することで、Bitcoin の価格の全体的上昇を実現します。高額の Bitcoin のロックが流動性を縮減するため、Bitcoin 価格上昇につ

ながります。しかし、最も重要なのは、RSK のこうした Bitcoin 生成の安定したトークンが、現時点で古くからある金融システムによる十分なサービスを受けていない何十億もの人々によるグローバルのデジタル経済に参加するのを可能にする安定通貨マイクロ決済を有効にすることです。

Bitcoin サイドチェーン技術の最前線にある RSK

RSK Labs は Bitcoin の他のあらゆる将来のサイドチェーンに不可欠の重要な概念の模索、研究、実施に従事しています。RSK の成功は他のサイドチェーンの開発者が構築済みの効率的なマージ・マイニングのインフラ、提案されたドライブチェーン・オペコード（drivechain opcode）、RSK Labs による multi-sig federations の安全な創造に向けて開発された技術を踏襲し、これらの恩恵を享受するのを奨励します。オープンソースのソフトウェア、ファームウェア、ハードウェアのデザインにより、RSK Labs はサイエンスを進化させ、全体としての仮想通貨エコシステムの機能性と安全性を改善します。

低コストの Bitcoin 決済ネットワークとしての RSK

現在、Bitcoin トランザクションのコストは平均 24 ¢ で[2]、RSK が 0.46 ¢ [3]と、1/50 という低いコストとなっています。これこそラジカルな改善なのです。同時に、Bitcoin の手数料は、通常、ブロックスペースの需要に応じて変動しますが、当社はオンチェーン・トランザクションに対する需要が高まるのを予期しています。ハードフォークによる Bitcoin のブロック規模増大を狙った何度かの未遂、そして、1 回の Segwit スペースのアップグレードに伴い、Bitcoin コミュニティ内にはブロックのサイズを拡張する計画は現時点ではありません。当社は、Bitcoin トランザクション手数料が個人の日常トランザクションを伴う大半のアプリケーションを対象に法外に高くなると予想しています。RSK ブロックはトランザクションの縮減規模を理由に、Bitcoin ブロックをはるかに凌駕するトランザクションを保有しているため、RSK がトランザクション規模で極めて低い手数料を提示するのは当然と言えます。以下の表は Bitcoin と RSK の比較です。

パラメータ	Bitcoin	RSK
平均ブロック確認時間	10 分	30 秒（マイナーは 15 秒に縮減可能）
指摘される交換確認時間	30 分（3 ブロック）	60 分（120 ブロック）+ 現行のマージ・マイニング・ハッシュレート（40%）。
最大トランザクション/ 秒	3.3 tps （平均サイズ tx の仮定）	10 tps（外部トランザクション、2019 年 1 月時点） 20 tps（内部トランザクション）
現行の平均トランザクション・コスト	24 ¢	0.46 ¢

Bitcoin トランザクションのコストは直接、ブロック・リワードの価額に相関します。トランザクションがブロックに加わると伝搬が遅くなります。伝搬の各ミリ秒の消費はブロック・リワードに比例して支払われますが、なぜなら、ブロックがネットワークに選ばれ

[2] https://bitcoinfees.info/
[3] http://rskgasstation.info/

る可能性が低くなるからです。 セット照合（Set-reconciliation）技法（例：Bose-Chaudhuri-Hocquenghem コード（Minisketch ライブラリ提供））は、Bitcoin に実装される場合、こうした従属関係を緩和する可能性があります。現状では、Bitcoin 価格が上がると、トランザクションの手数料もアップします。Bitcoin はバンキング間の決済システムのようになりますが、決済ネットワークではありません。また、重要なこととして、Lightning Network のようなオフチェーンの決済システムが新たに登場しつつありますが、こうしたネットワークは恐らく、チャネル決済やトップアップを対象とするオンチェーンのトランザクションに対する必要性を高めると同時に、トランザクションのコストを押し上げます。このコストが上昇すると、利用者はトランザクションコストの低いプラットフォームに移行してゆくでしょう。RSK は相当に低いコストで Bitcoin で取引するという素晴らしい機会を提供します。

RSK が Ethereum ユーザーや開発者にとって重要である理由とは?

DApp ユーザー基盤の増大

RSK は LATAM の Bitcoin 所有者によって当初構成されたユニークなユーザーベースです。今、RSK は LATAM およびアジアの両方で堅調に成長を遂げつつあります。Ethereum と RSK 双方の互換性のある DApps をシームレスに展開することで、開発者や会社はより広範なユーザーベースにアクセスでき、特定のブロックチェーンへの依存を弱めることができます。また現状では、Ethereum と RSK を結合し、トークンをあるブロックチェーンから別のブロックチェーンに移行するいくつかの federated ソリューションが存在するため、同じトークンが双方のブロックチェーンに存在することが可能なのです。

EVM/Web3 標準化の推進

Ethereum コミュニティはスマート・コントラクト仮想マシン（EVM）および相関にあたっての分散型アプリケーション向けのインターフェース（Web3）を構築しました。こうした標準を採用することで、RSK は開発者たちに対し、アプリケーションの RSK への移行、ならびに Ethereum 向けに開発された大半のインフラ・ソフトウェアの再利用を促しています.しかしそれは、統一型の学習マテリアルの提供、別の実行アーキテクチャやプログラミング言語を学習する必要の低減をすることにより、標準化に寄与します。同時に、RSK エコシステムによって開発されたツールは全て ETH ユーザーが利用できます。

持続的なチェーン・フォークのリスクの低減

Ethereum は定期的にネットワークのアップグレードを実施しています。最も古くに発表され、いまだ論争の的となっている Ethereum のハードフォークの 1 つはプルーフ・オブ・ワーク（Proof-of-Work）のコンセンサスからプルーフ・オブ・ステーク（Proof-of-Stake）への移行です。これは急進的な技術および経済的な変更であり、Ethereum マイナーたちによって制御されることが期待されています。新たなチェーン・スプリット（chain split）は開発者たちに対し、本来の PoW チェーンか新規の PoS チェーンの選択を行うよう強要します。さらに、新しいコンセンサス・プロトコルの安全と安定性については依然、不透明性があります。障害が生じると、Ethereum を保有する全てのユーザーが経済的に悪影響を被る恐れがあるため、変更は Ethereum コミュニティから反対されています。加えて、Ethereum のコア開発者たちは、お金の供給、ならびにプラットフォームの不変性と中立性を損なうプルーフ・オブ・ワークのアルゴリズムを実施しており、今後実施する開発者もいるでしょう。RSK はネイティブ投機的なトークンを保有していないため、smart Bitcoins は、ユーザーがコ

ミュニティ支援の RSK ネットワークのアップグレードに合意しない場合には、Bitcoin に変換することが可能です.したがって、RSK コミュニティは対立度が極めて低く、コミュニティ分断のリスクは最小化されます。他方、Bitcoin にはハードフォークを拒絶してきた伝統があります。よって、RSK は中長期的に極めて安定したプラットフォームを提供します。

最初の日から、Ethereum セキュリティ脆弱性の R&D 投資の保護

大半のブロックチェーンは定期的なネットワークのアップグレードと頻繁なソフトウェアのアップデートを実施します。大半のブロックチェーン・プロジェクトにとって、技術はまだ実験的な性質を帯びていて、プロトコルは確定済みではありません。Ethereum と RSK は成熟しているとはとても言えません。つまり、Ethereum の過去を精査および探査すれば、新たにセキュリティ上の脆弱性が見つかル可能性があります。セキュリティ面で顕著な実績を持つ RSK でさえ、リスクとは無縁ではありません。しかし、DApp の開発に特化したリソースがプラットフォームの破滅的な障害によって喪失されるリスクを軽減する 2 つの互換性のあるプラットフォームが存在します。双方が障害をきたす可能性は、とりわけ、関与するコンセンサス・プロトコルが異なることを勘案すれば、相当に低いと言えます。

DApps を RSK にポートすることによるトランザクション・スループットの増大

RSK は技術的に、より高いオンチェーンのスケーラビリティを提供できるという 4 つのコミュニティの提案を理由に、その他のプラットフォームを凌駕しています。1 つ目は、RSKIP4 指定の同時トランザクション処理で、これは、マルチコアのアーキテクチャがトランザクション処理の処理コアをフル利用するのを可能にします。結果、ブロック・ガス上限の引き上げが実現され、トランザクションのスループット増加につながります。2 つ目は RSKIP53 指定の LTCP で、トランザクションの圧縮を可能にし、さらに多くのトランザクションなどのトランザクションのシグネチャの集成が同じ規模のスペースと処理リソースとともに処理可能です。3 つ目は縮小チェーンのスケーリングで、シグネチャ・スペースとシグネチャ処理をよりいっそう縮減する LTCP の拡張機能です。4 つ目は新たに改善された VM で、試験段階にあり、仕様が RSKIP として提案される最終段階にある JIT コンピレーションを提供します。

こうした改善を駆使することで、RSK はトランザクション規模の拡大とトランザクション・コストの低減を支援します。

DApps を RSK にポートすることによるトランザクション・コストの低減

トランザクション・コストは多くの DApps にとっての制約です。RSK は上述のスケーリング提案にてオンチェーンの処理能力の向上を実施する準備を整え、トランザクション手数料の低下が見込まれています。このことは、Ethereum での法外な経費 に直面してきた使用事例の解消を実現します。

コイン・ステークと価値の保存の価値引き下げリスクの縮減

多くの DApps が仮想通貨の出資を求めています。ステークはサービス提供にあたって選択されるうえでのプライオリティを供与することを目的とするセキュリティ・デポジットです。また、一部の DApps は悪意ある行動から守る保険としてセキュリティ・デポジットを要求します。そうは言えど、その他の DApps である DAOs やクラウドファンドなどは、受給目的から、長期にわたって資金をロックしておくことを要求します。こうした状況下では、ネイティブ仮想通貨のボラティリティがコインのロックにあたってのインセンティブを低減します。Bitcoin は、プラットフォームとしてより優れた弾力性、価値の保存としての変動の低さを実

証してきましたが、これらは Smart Bitcoin から受け継がれた特性なのです。従って、RSK はこうしたアプリケーションに対応するうえでより優位な立場にあります。

RSK 使用事例

RSK プラットフォームは 1993 年に Nick Szabo によって提唱された、「チューリング完全」[4]スマート・コントラクトを提供します。同時に、RSK の VM は Ethereum VM と後方互換することから、RSK は Ethereum に従事する開発者たちに対し、Bitcoin 通貨の頑強性および RSK ブロックチェーンの安全性の恩恵を享受する機会を供与します。以下には、RSK の範囲を超えて開発可能な潜在的なスマート・コントラクトと使用事例が一覧化されています。

マイクロ決済チャネル

マイクロ決済チャネルは二人の当事者が、オンチェーンのトランザクション手数料を毎回の支払いで払うのでなく、チャネルのクローズ時に 1 回支払うだけで、回数に関係なく一般的な低額の支払いを安全に実行するのを可能にします。こうしたアプリケーションは、現行制度で十分なサービスを受けていない何十億という人々に代替手段を提供する公正で包括的な新しい金融制度にとって重大な要素となるでしょう。

2 層のオフチェーン決済ネットワークとステート・チャネル・ネットワーク

マイクロ決済チャネルは 2 層のレイヤー・オフチェーン決済ネットワークの基盤を提供します。2 層ネットワークは参加者からサードパーティの信頼の低い他者への決済をルーティングすることができますが、十分なチャネル容量があることが不可欠です。

2 層ネットワークは、無作為のノードのグラフでインスタンス作成、あるいは緊密に相関する少数ハブがユーザー間決済の大半を媒介するハブ& Spoke ネットワーク化する、のいずれかが可能です。 ステート・チャネル・ネットワークは、参加者群が、ゲーム等のマルチパーティ・プロトコル生成のオンザフライ（on-the-fly）を実行するのを可能にし、結果、トークン転送などのオンチェーンのステート変更につながりますが、チャネルのクローズ時に全てのオンチェーンの効果を遅延させ、当事者による詐欺行為の企図をシャットアウトします。RSK の豊かなプログラミング言語は、こうした種類のあらゆる 2 層ネットワークが最小の手間で直接実施されるのを可能にします。

分散化交換（DEXs）

分散化交換はサードパーティの信頼を伴うことなく、分散化トークンや仮想通貨市場の生成と創造を可能にします。RSK はオンラインまたはオフラインのオーダー・ブック、オーダー・マッチングにあたっての簡潔なプルーフにて、最もシンプルな TierNolan のプロトコルからより複雑な zk-SNARKs 基盤のプロトコルに至るまで、あらゆるバリエーションの分散化交換を支援します。

[4]全般用途の言語を用いてチューリング完全指示書向けに記述されていることから、コントラクトはチューリング完全であると考えられるものの、VM が利用可能なリソースは限られています。

小売決済システム

RSK は BTC が日常の小売決済目的からグローバルに採用されるのを可能にします。Bitcoin の小売用途の主な制約の 1 つが確認時間です（不可逆性の確証まで 10 分〜1 時間）。RSK は消費者がわずか数分の確認時間で Bitcoin セキュリティの恩恵を享受するのを可能にします。マーチャントはサードパーティのゲートウェイを必要とすることなく、ほぼ瞬時に決済を受諾できるようになります。また、RSK は小売市場での成功に必要とされる、秒あたりのトランザクション(tps)規模の拡張を実現します。RSK ネットワークは DÉCOR+ コンセンサス・プロトコルを駆使してトランザクション規模の増大時の採掘の集中化の回避を図っています。

エスクロー・サービス

RSK は、Oracle がエスクロー下の資金の保管を行うことなくエスクローのリリースをすべきかどうかを規定するトランザクションにサインするようなスマート・エスクロー・サービスの生成を可能にします。

仮想アセット生成

RSK は Bitcoin ネットワークが保障する仮想アセット（トークン、アルトコイン等）の生成を可能にします。こうしたアセットとして、ロイヤルティ・ポイント、ユーティリティ・トークン、セキュリティ・トークンなどが挙げられます。さらに、トークンは法定不換紙幣建て、ならびに法定不換紙幣のバックアップが可能です。つまるところ、全国民に低コストのプログラム可能なお金を提供する手段として、政府や中央政府が創造することが可能です。

Bitcoin 支援のトークン・オファー（BTOs）

BTOs は Bitcoin が採掘されたばかりの新たなトークンと交換される際の、仮想アセット生成の特殊事例です。このツールは Ethereum クラウドファンドなど、ブロックチェーンのクラウドファンディング向けに広く採用されてきました。
RSK に限ると、BTOs はスタートアップが、現存する最も安全で安定した仮想通貨である Bitcoin で直接資金を受領するのを可能にし、Bitcoin Hashrate マージ・マイニング RSK によって保障される RSK ブロックチェーン上にトークンを生成するのを可能にします。トークン発行の全プロセスは、RSK Bridge のサービスを使用すると、管理者による承認不要で実施可能です。

資産の流動化

RSK は実資産が後押しするデジタル・トークンの生成を可能にします。これは REIT、株式、債券またはその他の資産（あるいは先物の利益）のデジタル商品化に用いることが可能です。この特定の使用事例は、従来の金融市場が成長にあたっての運転資本または資本に対する需要を満たしている開発途上国の小規模ビジネスに独自のソリューションを供与します。

分散化送金

この特定の使用事例は、銀行未利用/ 未実証の人々が食糧や住居目的で家族に送金するのに高額の手数料を支払っている開発途上国においてとりわけ重要です。RSK は法定通貨建てのトークンや既存の交換インフラ利用を可能にし、仮想通貨試算のキャッシュアウトのオプションにより、極めて低いコストで送金を実行できます。

IP 保護 / レジストリ

RSK は存在証明（PoE）を提供するコントラクト開発を実現します。 PoE は個人や会社が、Bitcoin ブロックチェーンの安全性ついていつでも、特定の文書（あるいは財産権）の存在を証明するのを可能にします。この使用事例は ID や登録のメカニズムの信頼性が低い中南米、アフリカ、アジアの社会ではとりわけ重要です。

投票制度

RSK は最小コストで、極めて安全で透明性の高い選挙を実現するデジタル投票の創造を可能にします。同時に、会社役員会や分散型組織の公正な投票プロセスを確保するのに使用される可能性もあります。

マイクロレンディング（少額融資）

グローバル人口の 50% 超が従来型の金融制度にアクセスできていません。こうした信用アクセスの欠如は現在のグローバル社会が直面する経済格差の原因となっています。RSK は世界の 30 億という最貧困層に信用アクセスを提供可能にする拡張可能なデジタルおよびプログラム対応の貸借契約の開発を可能にします。

サプライチェーンのトレーサビリティ

RSK はデジタル・ウォレットが特定の製品やバッチの物理的ロケーションの（デジタル的な）追跡や追尾を行うのを可能にします。こうした種類のコントラクトは国際通商、ならびに小売、食品、ヘルスケア産業においてとりわけ有益と考えられます。その他の全ての使用事例においても、RSK を用いることで、最小コストにて、Bitcoin のブロックチェーンを安全のうちに実現可能です。

オンラインの評判 & デジタル・アイデンティティ

開発途上国の主要な問題の 1 つとは、貧困層にとって文書化や ID が不十分であることです。結果、貧困層による投票、医療へのアクセス、犯罪/ 虐待や酷使の報告、金融支援の活用が妨げられています。RSK は極めて低いコストで、Bitcoin ブロックチェーンと同程度に安全なグローバルのデジタル・レジストリの創造を実現します。

インゲームのグローバル通貨

多くのマルチプレーヤー・ゲームがプライベート通貨などのインゲーム・エコノミーを採用しています。こうしたゲームの進化に伴い、利用者にとって仮想通貨が法定通貨と同じ程度にまで有用となり、二次市場ではしばしば取引されています。インフレ、詐欺、オン

ライン窃盗は大きなリスクであり、利用者の懸念となってきました。また、ゲーム会社は利用者の仮想通貨を委託することで法定およびセキュリティ上のハードルに直面することもあります。グローバル化が進むにつれ、バーチャルゲームも同様であり、プレーヤーは、1 つのゲームで獲得したお金を他のゲームで簡単に消費できないという不便を感じるようになるでしょう。RSK はインゲーム決済として（ Smart Bitcoins や RBTC に相当する）BTC をゲームが受諾する、あるいは PSK によって保護されているプライベート・デジタル・アセットの創造を可能にすることで、こうした問題を解消することができます。2 層オフチェーン・ネットワークによって提供される RSK 決済は低額のクローズドループ・システム（closed-loop systems）同様にスピーディとなり得ることから、ゲームエンジンはプレーヤー同士の取引や会社とプレーヤー間のバーチャル・オファー目的でインゲームの購買システムとして RSK を採用することができます。URL のクリックまたは QR コードのスキャンにより、取引が標準プレーヤーの外部電子ウォレット・ソフトウェアを使うことで起動可能で、また、ゲーミング会社への委託料の支払にも対応します。

インターネット・ゲーミングおよび予測市場

迅速な決済とは迅速な払い出しも意味します。Bitcoin のゲーミング・サイト（例：SatoshiDice）は 0 確認やチェーンド・トランザクションを使って登録不要の瞬時の賭博体験を提供しようとしていますが、ゲーミング・サイトにとってはセキュリティ面のリスクが伴います。RSK は非ゼロ・ブロック確認を伴うほぼ瞬時の払い出しの賭博を可能にします。

公正なゲーミング

スマート・コントラクトの導入により、ならびに Mental Poker 等のよく研究された暗号プロトコルと連動して、RSK は上前をはねる、信頼の置けるサードパーティの要件を伴うことなく、カードゲームのオープンで公正なプラットフォームを提供することができます。

代替不可能トークン（NFTs）

NFTs は特定の財産、ライセンス、製品、サービスとリンク可能な一意のトークンです。NFTs は、スポーツのコレクション品からゲームプレーヤーの特長や「皮膚」に至る、多様な産業での使用事例を可能にし、RSK 上で容易に創造できます。

テクノロジー概要

RSK プラットフォームは、根本的には、以下の組み合わせです：

- チューリング完全リソース説明決定論的仮想マシン（スマート・コントラクト向け）
- カスタム HSM モジュールによって保障された Federation ベースの two-way pegged Bitcoin サイドチェーン（BTC 建ての交換）。Drivechain プロトコルが Bitcoin に実装されると、本来の計画はハイブリッドのドライブチェーン・メカニズムへの移動となります。
- セルフィッシュの採掘禁止マージ・マイニングベースのコンセンサス・プロトコル
- 低待ち時間ブロック増殖ネットワーク（迅速な決済向け）

チューリング完全仮想マシン

RSK 仮想マシン（RVM）はスマート・コントラクトのプラットフォームの基幹です。スマート・コントラクトはあらゆるネットワーク・フル・ノードによって実施されています。スマート・コントラクトの実施に伴い、コントラクト間メッセージが処理され、金銭トランザクションの生成、ならびにコントラクト持続メモリの状態の変更につながる可能性があります。RVM はオプコード（op-code）レベルで EVM と互換し、Ethereum コントラクトが RSK 上で円滑に実行されるのを可能にします。現状において、VM は解釈によって実施されています。今後のネットワークのアップグレードにおいて、RSK コミュニティは VM パフォーマンスを持続可能なものに向上させること目指します。1 つの提案として、EVM オプコードを Java のようなバイトコードのサブセットにダイナミックに再標的化することで EVM をエミュレートすることが挙げられ、セキュリティ硬化およびメモリ制約の Java のような VM は新たな VM（RVM2）になります。 結果、RSK コード実行がネイティブ・コードに近似するパフォーマンスにすることがあります。

主要な特長：

- 独立した VM、ただし、オプコード・レベルで EVM との非常に高い互換性。
- Ethereum DApps を Bitcoin ネットワークの安全性で実行する。
- RSK コミュニティ作成の無数の PSKIPs（RSK 改良提案書）にて立証済みのパフォーマンス向上パイプライン。

サイドチェーン

サイドチェーンは、そのネイティブ通貨が決済証明を使用することで、現状では自動で別のブロックチェーン通貨の価値にペグされている独立したブロックチェーンです。2 つの通貨で自由に、自動で、価格交渉において負担を伴わずに、交換可能な時に two-way peg が存在します。RSK においては、Smart Bitcoin（RBTC）が BTC に two-way ペグされています。

実際、BTC を RBTC と交換する場合には、ブロックチェーン間で「変換」される通貨はありません。変換が生じる際、一部の BTC は Bitocoin にロックされ、同量の RBTC が RSK から解除されます。RBTC を BTC に戻す必要がある場合、RBTC を RSK に再度ロックし、同量の BTC が Bitcoin から解除されます。

完全な信頼最小化およびサードパーティ・フリーの two-way pegs は、2 つのプラットフォームにチューリング完全スマート・コントラクトがある場合、創造可能です。しかし、Bitcoin が現状ではスマート・コントラクトに対応せず、外部 SPV プルーフの認証にあたってネイティブ・オプコードにも対応しないことから、RSK の two-way peg システムの一部は半信頼サードパーティ（STTP）群を必要とし、結果、総体的に Federation に要請を行います。No シングル STTP はロックされた BTCs を制御できるものの、その大半が BTC 資金をリリースする能力を有しています。各 STTP にはロックされている BTC を保護するキーがあり、RSK ブロックチェーンからコマンドを受領すると、Bitcoin に変換する必要のある BTC を解除します。利用者は、BTC を RBTC に転送して戻す場合、通常、当初送付された BTC を伴う UTXOs と直接結合されている Bitcoins を受領しません。従って、特定の利用者ではなく、RSK ネットワーク全体のために RBTC がロックされます。

資金のロックと解除は人的介入を伴わず、Federation によって実施されます。Federation の一員になるには、特に BTC ファンドの解除を決定する要素の正当性に関して、ノードに動力を供給するソフトウェアの適切な挙動を検証する能力が必要です。RSK Labs はプライベート・キーの最大の安全性を供与し、将来的に、セキュリティ向上を図るようトランザクション認証プロトコルに命じることのできるような、STTPs が利用できるハードウェア・セキュリティ・モジュール（HSM）のファームウェアを開発しています。

2019 年 1 月時点、RSK Federation は 15 の著名で確固とした安全性を誇る公証人から構成されています。有数の Blockchain 企業は、現在、RSK Federation を統合し、匿名のプロトコルに加入して Bitcoin を安全にロックしています。作業の対価として、Federation のメンバーには、ハードウェアおよび保守管理コストを補填する目的上、トランザクション手数料の 1% 相当が付与されます。Federation の構成を変更するうえで自動化プロセスがあります。federation の各メンバーは構成の変更の受諾あるいは却下を行うことができます。不定期に発生するこのプロセスはスマート・コントラクトによって制御されているため、公開となっています。プロトコルは、変更が実施されるまで、1 週間の遅延が合意されています。結果、利用者は新規の Federation 構成を信用できない場合、Bitcoin ネットワークに Bitcoin を戻すことができます。

Bitcoin がハードフォークとして SPV プルーフ認証にあたっての特殊オプコードまたは拡張性を付加する場合で、新規システムが安全で管理者による承認不要であることが証明されたら、STTPs としての Federation の役割はもはや不要と化し、RSK コミュニティは変更を実施して RSK を管理者による承認不要のシステムに適応させる場合があります。また、RSK コミュニティは Drivechain BIP を提案していますが、これは、マイナーがペグ内の Bitcoin の安全化に関与するのを可能にし、STTPs にて必要な承認の程度を大幅に縮減します。

マージ・マイニング

サトシのコンセンサスは、プルーフ・オブ・ワーク（Proof-of-Work）を基盤とし、低コストでブロックチェーンの歴史の上書きを防ぐ唯一のコンセンサス・システムです。アカデミック・コミュニティは代替として、プルーフ・オブ・ステーク（Proof-of-Stake）の知識と研究を推進していますが、現在、PoW が高度に証明されたセキュリティを提供します。マージ・マイニングという技法は、Bitcoin のマイナーたちが同時に、ほぼゼロの限界費用で他の仮想通貨を採掘するのを可能にします。Bitcoin の採掘に用いられる同じ採掘インフラとセットアップが同時に RSK を採掘するのに再利用されます。すなわち、RSK がマイナーに付加的なトランザクション手数料を付与するにあたり、マージ・マイニングのインセンティブが高くなるのです。

当社は、RSK マージ・マイニングの成長の 3 つの段階を特定しています：

- ブートストラップ・フェーズ：マージ・マイニングは Bitcoin のハッシュレートの 30% 未満です。
- 安定フェーズ：マージ・マイニングは Bitcoin のハッシュレートの 30%～60% です。
- 成熟フェーズ：マージ・マイニングは Bitcoin のハッシュレートの 60% 超です。

RSK は、不正なマージマイナーが低コストで RSK を戻すような際、ブートストラップ・フェーズを放置した状態にしておきます。2019 年 1 月時点、Bitcoin マイナーの 40% 以上が RSK マージ・マイニングに従事しています。しかし、RSK 手数料が依然、Bitcoin ブロックのリワードと比べ低いままであることから、二重支出による RSK 攻撃の対価は Bitcoin の場合より低く済みます。
RSK はより長いマイナーリワードの満期など、二重支出のリスクを低減する一部特性を備えています。そうは言えど、RSK Lab 研究チームはプロジェクトの安定および成熟フェーズ中の攻撃を防ぐいくつかの特性を開発してきました：

- **署名入り通知：**RSK クライアントは公証人による署名入り通知を活用できます。ノードは Sybil 攻撃の検出と利用者への周知にあたってこうした通知を利用できます。
- **透明性のある二重支出トレイル：**この手法では、全ての RSK マージ・マイニングのタグが Bitcoin ブロックチェーンにおいて公開されているセルフィッシュの RSK フォークの検出に利用可能な付加的情報で増補されます。セルフィッシュのフォーク・プルーフは自動的に構築され、こうしたプルーフは RSK ノードに提示され、ネットワーク全体に拡散されます。プルーフはノードに対し、一切のトランザクションが確認済みと発表されていない「安全モード」に入るよう強要します。安全モードはマーチャントや交換が２重支出と考えられる支払を受諾するのを防ぎます。実証済みのセルフィッシュのフォークが堆積 PoW の RSK メインチェーンによって追い撃ちを掛けられると、ネットワークは通常状態に回帰します。この手法は RSK 二重支出に対する抑止力です（セルフィッシュのフォークの採掘時に、悪意あるマイナーが依然、Bitcoin リワードを収集しようとする場合）。

プラットフォームが成熟フェーズに突入すると、RSK のセキュリティは世界中の金融包含の経済を支援するのに十分となると推測されます。

主要な特長：

- DECOR+ コンセンサス・プロトコル
- 採掘リワードの 1 日満期。
- マージ・マイニングにて期待される Bitcoin マイニングの効率性の非喪失（遅延ミッドステート・スイッチング）

迅速な支払と低待ち時間のネットワーク

RSK はすでに 2 層オフチェーン決済ネットワークを有効にしていますが、依然、RSK は Bitcoin と比較して、より優れたオンチェーン決済ネットワークを提供することを目標としています。この実現にあたり、RSK は DECOR+ および FastBlock5 プロトコルを採用していますが、これらは採掘の集中化とセルフィッシュ採掘を対象とするインセンティブを生成しない 15 秒という平均ブロックレートの実現を可能にします。

主要な特長：

- 15～30 秒のブロック・インターバル（マイナーのステート・スイッチング効率性による）
- セルフィッシュ採掘の防止とブロックレートの低減にあたっての最終競合ブロックの完全ネットワーク増殖。
- タイムクリティカルの優先事項を伴うブロック・ヘッダー拡散にあたっての新規ネットワーク・コマンド。
- DECOR+プロトコル（競合ブロック間のリワード共有）。
- GHOST プロトコル（チェーン加重）。

Bitcoin の創造は PoW ブロックチェーン・ベースの仮想通貨を対象とするより低いインターバルに向けての競争でした。しかし、低ブロック・インターバルは仮想通貨ネットワークの安定性と能力にインパクトを及ぼす恐れがあることから、いくつかの設計上の因子を勘案する必要があります。何よりも、短い確認インターバルの実現性に影響を及ぼす最重要因子は生成される失効ブロックの数です。失効ブロックレートに影響を及ぼす主因子はブロック増殖プロトコルです。 RSK について、当社は慎重にこのプロトコルを解析し、シミュレーションを実施してネットワークのパフォーマンス、有用性、セキュリティを検証してきました。

Bitcoin においては、2 人以上のマイナーが同じ高さでブロックを解いた場合、明らかな利害相反が存在します。競合する各マイナーはベストチェーン・チップとして残りのマイナーから自身のブロックが選ばれて欲しいと考え、残りのマイナーたちは、全般に、2 つのうちのどちらを選択するかについては気に留めないでしょう。ただし、残り全ての正直なマイナーや利用者は同じブロックチップを選ぶことを希望すると考えられますが、なぜなら、逆転する可能性が低減するからです。 DECOR+ コンセンサス・プロトコルは、一点に集中した選択向けに適切な経済的誘因を設定しますが、マイナー間のさらなる相互作用の強化は必要とされません。DECOR+ プロコトルは以下に沿うように紛争を経済的に解決するリワード共有戦略です：

1. 全当事者が同じブロックチェーン・ステートの情報にアクセスする際、紛争が決定論的に解決されます。
2. 選択される解決法は全てのマイナーの収益を（集合的に）最大化し、ブロックのリワードが高いマージンで異なる場合、紛争状態にある全てのマイナーがその対象となります。
3. 選択される解決法は、競合ブロックが近似するリワードを有する場合、検閲への耐性を最大化します。
4. 紛争解決には僅かですが、時間がかかります。

トランザクションプライバシー

RSK 自体、Bitcoin より優れたトランザクション・プライバシーを提供せず、ハンドルネームに依存します。にもかかわらず、RSK の VM はチューリング完全であることから、ハンドルネーム技術（例：CoinJoin、ring Signatures、zCash）はサードパーティの認証を伴うことなく、安全に実施可能です。

スケーラビリティ

RSK は現状、Bitcoin よりはるかに拡張可能です。RSK 決済は標準 Bitcoin 決済の規模の 1/5 を必要とします。提案された LTCP プロトコルを用いることで、トランザクションの規模は Bitcoin トランザクション規模の 1/50 にまで縮小可能です。結果、瞬時に、トランザクション規模能力の実質的増大につながります。加えて、利用者が選択可能なシグネチャ・スキームを有効にする次のコミュニティ提案（RSKIPs）が存在します：ECDSA、Schnorr、Ed25519Ed25519 は Bitcoin ECDSA 曲線よりも高性能であることから、このスキームを用いると、能力のさらなる向上に寄与する場合があります。

RSK 特長比較

以下の表は RSK の主な特長を代替（Liquid sidechain（Blockstream）、WBTC トークン（BitGo）含む）と比較したものです。Liquid と WBTC の双方が BTC にペグされています。基本的に、RSK が分散化に及ぼすインパクトが少ない、より優れた技術ソリューションであることが判明しました。

項目	Bitcoin BTC	Ethereum ETH	Ethereum WBTC	Liquid LBTC	RSK RBTC
平均確認時間	10 分	15 秒（GHOST）	Ethereum と同じ	60 秒	15〜30 秒（DECOR+GHOST）
セキュリティ閾値（セルフィッシュ採掘または癒着が原因）	〜30%	30% 未満	Ethereum と同じ	50%	50%（DECOR+GHOST）
チューリング完全スマート・コントラクト	なし	あり	あり	なし	あり
Bitcoin に価値を付加する	-	なし	あり	あり	あり（マージ・マイニング）
Bitcoin と統合	-	なし	なし	サイドチェーン	サイドチェーン
SPV クライアント	あり	あり	あり	あり	あり
ハードウェア・ウォレット統合	あり	あり	部分/ 一部	なし	あり
トランザクション・ファイナリティ保証	ナカモトのコンセンサス SHA256D	Ethereum コンセンサス Ethash	Ethereum と同じ	Federation	DECOR+GHOST。SHA256D PoW
機密トランザクション	なし	コントラクト経由	なし	あり	コントラクト経由。ネイティブ・サポート計画済
スケーラビリティ[tps]	3 （ 6 + segwit）	非結合、現状 15	Ethereum と同じ	3（6 + segwit）	非結合、現状 10
ブロックチェーン規模	200 GB	> 1.5 TB	> 1.5 TB	〜300 MB	〜2 GB
トークン・ペグ・セキュリティ	--	--	単一の会社	Federation	Federation
トークン	BTC	ETH	WBTC	LBTC	RBTC

RSK Labs の役割

RSK Labs は RSK ノードの参照実施を生成することで強力なコミュニティ・プレーヤーとして設立されています。現在、RSK Labs は以下の技術およびコミュニティ活動の実施に従事しています：

- 定期的なアップデートを通じての RSK 参照の開発の推進
- 学術分野との連携の構築
- コミュニティ・デイスカッション・チャンネル、フォーラム、FAQ（よくある質問）の保守管理
- カンファレンスと地域の会合の実施
- RSK ブロックチェーン利用の推進
- 定期的な外部のセキュリティ監査の要請と公表
- コミュニティ提案型ネットワーク・アップグレードの協議への参加
- RSK コードベースのセキュリティ監査
- RSK ネットワークの恩恵を享受する最善の方法についての政府、スタートアップ、起業家、企業への周知

RSK Labs による継続的な RSK へのコミットメントは RSK プラットフォームによって保証されています：プラットフォーム・トランザクション手数料の 20% が RSK Labs の支配するアカウントに支払われています。

RSK の未来

RSK ロードマップは RSK コミュニティによって策定されています。RSK 開発の初年度中、RSK Labs は参照実施の構築において積極的な役割を果たしました。RSK 導入後も、RSK Labs は引き続き、コードベースの改良および RSKIP 提案レポジトリ・システムを通じての改善の提案により、コミュニティと深く関与してきました。レポジトリはコミュニティのメンバーが複数のコードベースについての協議、却下、受諾、展開を調整するのに寄与しています。改善の提案の規模は膨大です。以下は 2018 年 12 月時点の主な提案の一覧です：

分散型メモリ、ダイナミックな契約の依存関係、静的な契約の依存関係を用いた並行実行、ルーチンの契約の依存関係を用いた並行実行、シフト・オペレーションズ、ブロックサイズ上限、コードによって支払われる持続的ストレージ・レンタル、認証の少ないマイニング、交渉済みの最低ガス価格、決してブロックを無効化しないトランザクション、TXINDEX オプコード、契約スリープ、安定アセット& トークン発行のサポート、リワード・マネージャー・スマート・コントラクト（REMASC）、簡略型リワード・マネージャー・スマート・コントラクト（REMASC）、複合ステート・ツリー、より簡易の持続的ストレージ・レンタル、Trie を使った瞬時のハイバネーション・ウェイクアップ、RSK アドレス・フォーマット、存続および一時的なメモリスペース、効率的な持続的ストレージ・レンタル、Merkle ツリー・エレメント数へのコミット、オンチェーン PoUBS、新規バイナリ Trie、メモリのキャッシュ、DUPN と SWAPN オプコード、高度に効率的なス

トレージレンタル、一時的 segwit、アカウント作成コストの変更、コード・ページネーション、ハイバネーション圧縮、ダブルハッシュド・アドレス、CODEREPLACE オプコード、契約 const データ・セクション、BridgeMaster Federation メンバーの管理、トランザクション・カプセル化、単一アドレス・スマート・ウォレット、シグネチャ圧縮、マルチキー・アカウント、Bitcoin への two-way-peg 基本ブリッジ、拡張 Bitcoin ブリッジ・トランザクション、受領からのワールド midstates の除去、連続的アドレス・フォーマット、データ内の 0 バイト・ディスカウントの除去、新規イベント・ツリーと拡張ログ、ブロック採掘手数料情報メカニズム、CALLNUM オプコード、ブロックごとの平均フリー・ガスの周知、One-To-Many ハブ決済チャネル、ヘッダーpseudo-オプコードを使ったスクリプト・バージョン、メモリ・マップド構成設定登録、キャッシュ指向ストレージ・レンタル、Lumino トランザクション圧縮（LTCP）、トランザクション規模 & 目的先のプライバシー、ネイティブ確率的決済、散在的で認証の少ない採掘、ヒエラルキー決定論的ウォレットの逸脱パス、Bitcoin フォークへの対応、児童契約、Checksum アドレス・エンコーディング、キャッシュ指向ストレージ・レンタル（EOT バージョンにて収集）、ステート trie アップデート・バッチを用いた圧縮ブロック増殖（COBLO）、遅延シグネチャ集合の二重署名、既定 TX データ、ネイティブ・オフチェーン確率的決済、よりスムーズな障害調整、指示セット拡張としての DELEGATECALL、BridgeMaster Federation メンバーの管理

一部プロトコルは依然、未熟ですが、それ以外は数回のデイスカッションを経て改良されていて、将来のネットワークのアップグレードの一部となるにあたってのコミュニティ支援を恐らく得ていることでしょう。

まとめ

RSK はチューリング完全スマート・コントラクトを提供する、Ethereum 標準と互換性のある、Bitcoin のマージ・マイニングによって安全が保証されている生産中の初の Bitcoin サイドチェーンです。

RSK は 5 年に及ぶブロックチェーン技術改良の積み重ねを表し、Bitcoin エコシステムがプログラム可能なお金と決済の最良の特性を駆使するのを可能にし、bitcoin の有用性と価値を向上します。

RSK の革新的な設計はより高度なスケーラビリティとトランザクション費用の低減を実現します。

RSK は世界中の開発者たちが多様なニーズと使用事例に適合する、トランザクション費用が低い、世界で最も安全なネットワークで起動する個人および法人の分散型ソリューションを創造するのを可能にします。

RSK は Bitcoin のマイナーたちが、スマート・コントラクト市場に参加するのを可能にし、Bitcoin の採掘業界に大きな価値を付加して長期にわたる持続可能性を保証します。そして、Bitcoin マイナーたちの経済的持続性および Bitcoin ネットワークのセキュリティの成長に寄与します。

RSK は Ethereum の利用者や企業に対し、ネイティブ通貨として Bitcoin を使い、セキュリティ面で Bitcoin の採掘インフラに依存し、より広範な利用者基盤にアクセスするソリューション展開にあたっての新たな互換性のあるプラットフォームを提供します。

RSK は銀行を利用していない、ならびに金銭的に十分に恵まれていない世界中の 30 億以上の人々に機会を創造するような、分散型の安全でオープン、そして安価なブロックチェーンベースの金融制度の創造を可能にします。