UTXO

OCTOBER 2023

RGB

RESEARCH REPORT

PREPARED BY:

UTXO MANAGEMENT RESEARCH

CONTENTS

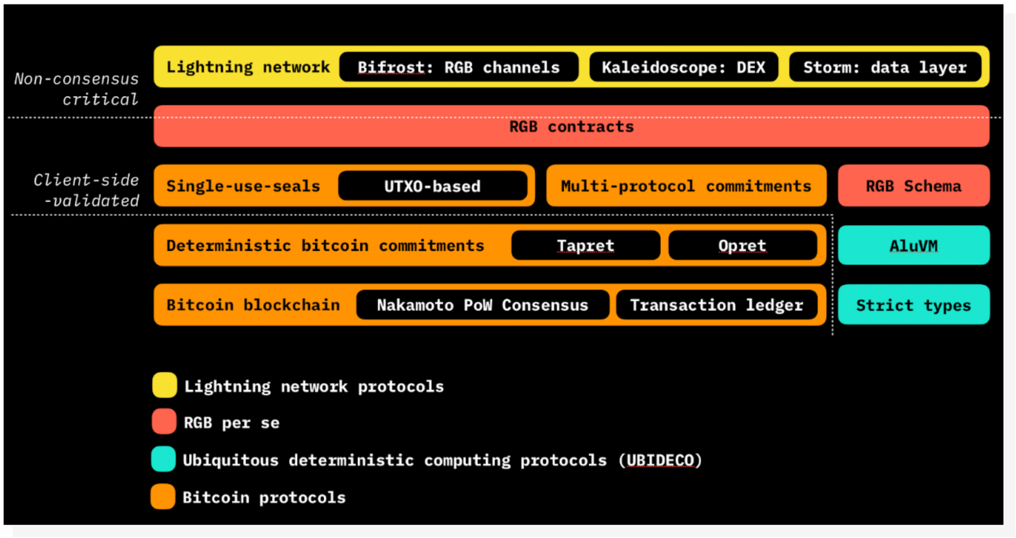
OBJECTIVE

In a landscape where Bitcoin's potential is still being fully realized, understanding emerging protocols/layers like RGB is both timely and essential. This report consolidates existing knowledge on RGB's nascent yet promising role in Bitcoin's ongoing evolution. With this streamlined overview, we aim to create a definitive resource for current industry discussions while spotlighting both existing innovations and future possibilities. Drawing upon our years of hands-on experience in the Bitcoin ecosystem, UTXO Management employs a thoughtful, research-backed approach to allocate capital across various opportunities in both public and private markets. Our accumulated knowledge guides our ongoing exploration of emerging protocols like RGB for potential future venture allocations.

The report provides an in-depth analysis of RGB, an advanced smart contract framework explicitly tailored for Bitcoin and its second-layer Lightning Network solution. Covering foundational concepts to advanced features, the report aims to offer a comprehensive understanding of RGB's current status, its security model, and the growing ecosystem around it.

KEY FINDINGS

- Technology Overview: RGB blends Bitcoin's security features with advanced smart contract functionalities, enabling use-cases like DeFi, NFTs, and DAOs.
- Security and Architecture: RGB adopts Bitcoin's anti-double-spending and censorship-resistant features, enhancing robustness through client-side validation.
- Scalability and Privacy: Features like client-side validation and the Bifrost Protocol make RGB scalable and privacy-focused.
- Applications: RGB supports a wide array of both financial and non-financial applications, including potential disruptions in DeFi and NFT markets.
- Current Status: As of April 2023, RGB's Version 0.10 is out, but adoption rates are lagging due to complexity.
- Industry Adoption: Major industry players like Fulgur Ventures, Bitfinex, and Pandora Prime are backing RGB. The ecosystem is rich with projects like Infinitas, MyCitadel, and DIBA focusing on different use-cases.



Source: RGB Blackpaper

COMPREHENSIVE ANALYSIS OF RGB

RGB is a smart contract system explicitly crafted for Bitcoin and its second-layer solution, the Lightning Network. With its roots dating back six years, RGB has been evolving, and the most recent release—Version 0.10—introduces a slew of features that make it more robust, scalable, and versatile. Developed by the LNP/BP Standards Association, it aims to introduce advanced functionalities like token launches, DeFi, DAOs, and NFT minting into the Bitcoin ecosystem. RGB is designed to allow everything possible with blockchain-based smart contracts. This comprehensive analysis unpacks RGB's unique attributes, how it operates, and how it compares with other smart contract solutions.

Architectural Framework and Key Components

- **Base Layer:** RGB contracts are intrinsically linked to Bitcoin's Unspent Transaction Output (UTXO) model. This foundational layer holds cryptographic commitments, making RGB inherently secure by leveraging Bitcoin's proven security features.
- **Client-Side Validation Layer:** Built atop the Bitcoin layer, this part includes protocols for deterministic Bitcoin commitments, single-use seals, and multi-protocol commitments.
- **AluVM Virtual Machine:** AluVM is a specialized virtual machine designed to handle computing tasks in a consistent and secure way, particularly for smart contracts and systems where multiple computers need to agree on outcomes. Unlike other virtual machines, it has a simpler, more secure structure that makes it harder for errors to occur. This makes it ideal for running complex agreements or contracts in a way that everyone can trust, without requiring a central authority. It also has built-in flexibility to adapt to different computing needs and ensures a high level of security.

Core Technologies

- **Client-Side Validation:** RGB diverges from traditional smart contract platforms like Ethereum by implementing a client-side validation model. Unlike network-wide execution systems, RGB's localized approach only tasks immediate participants in a contract with its validation and execution. This significantly reduces the computational load on the broader network, thus dramatically improving scalability. To fortify this model, RGB employs deterministic Bitcoin commitments and multi-protocol commitments, which allow for harmonious functionality with any future protocols that adopt similar client-side validation methods. A crucial aspect of this architecture is the use of single-use seals defined over Bitcoin's Unspent Transaction Outputs (UTXOs), serving as cryptographic markers that affirm the contract's unique state. The localized validation process is guided by RGB's schema, a set of deterministic rules that facilitate the contract's evolution through a Directed Acyclic Graph (DAG) of state transitions. This structured approach not only enhances scalability but also adds layers of security and privacy by keeping all transaction data off-chain.
- **Single-Use Seals:** Originating from a concept proposed by Peter Todd in 2016, single-use seals in RGB serve as a cryptographic commitment mechanism designed to prevent double-spending and ensure transactional integrity. Unlike traditional commitments, they allow for a two-level future commitment for a unique message. Seals manifest as transaction output-based single-use seals (TxO seals) that remain hidden in the transaction graph yet can be verified. Defined seals, consisting of transaction identifiers and output numbers, become "closed" once a related spending transaction is known, forming a cornerstone for RGB's decentralized and secure smart contracting.
- **Schema:** A predefined set of rules, or schema, governs the evolution and validation of each smart contract within RGB. This standardization ensures uniformity and eases the process of contract verification and auditing.

Scalability and Privacy

- **Scalability Advantages:** RGB utilizes off-chain data storage and allows for transaction batching. These features let multiple transfers be committed in a single Bitcoin transaction, considerably enhancing scalability.
- **Bifrost Protocol:** Bifrost is a secondary protocol for the Lightning Network that facilitates various advanced functionalities, including client-side validated data transmission and decentralized exchanges, specifically tailored for mobile RGB wallets. Though not technically part of RGB, it functions as an enhanced, more versatile version of the existing Watchtower concept in the Lightning Network. Bifrost offers public key-value storage for securely holding encrypted, client-validated data and has the flexibility for future integration into the LN. It also adds the benefit of holding information for users when they are offline, making the network more accessible and user-friendly.

Types of Commitments

- **Tapret Commitments:** Implemented as OP_RETURN-based scripts that reside within a specific location in a Taproot script tree. These commitments are not directly exposed in the blockchain data, maintaining privacy. Special procedures ensure their unique and deterministic placement within the Taproot script tree, including a nonce for hash "mining" and a uniqueness proof to verify the absence of alternative commitments. This secure and efficient approach aligns with BIP-341 standards and facilitates client-side validation through off-chain data.
- **OP_RETURN Commitments:** Compatible with older systems but less efficient and private.

Security Model

RGB leverages Bitcoin's Proof-of-Work consensus for security. Using client-side validation, it keeps all data off-chain, enhancing scalability and privacy. Security is fortified through Bitcoin script and single-use seals tied to unspent Bitcoin transaction outputs.

Each contract starts with a "genesis state" and evolves via a DAG (directed acyclic graph) of client-validated state transitions linked to Bitcoin's UTXO set. This DAG setup requires each new transaction to have at least two predecessors for confirmation. RGB's schema, set at genesis, defines consistent client-side validation rules. The system allows high scalability and potential functionalities like decentralized exchanges through the Bifrost protocol. Compared to other smart contract protocols like Ethereum or other EVM chains, RGB has the potential to be more layered, scalable, and private by keeping data and evolution off-chain.

Application Possibilities

RGB can enable a plethora of both financial and non-financial applications ranging from decentralized finance protocols to identity verification, with the potential for real world asset adoption to take place in the future as development continues and adoption increases.

Current Status

As of September 6, 2023 the stable release of RGB version 0.10 was rolled out after a 5-month alpha testing period. The release marked a pivotal moment, featuring a command-line tool and runtime library designed for easy desktop and mobile integration. Independently audited by several teams, the software has shown reliable performance and is integrated into three wallets: MyCitadel for desktop, Iris for Android, and BitMask for web-based usage.

Ecosystem and Support

Companies like Fulgur Ventures, Bitfinex, and Pandora Prime have shown support for RGB. Various projects within the ecosystem like Infinitas and MyCitadel focus on exploiting RGB’s high-security and privacy features.

Comparative Analysis

- **ERC-20 Tokens and Altcoin Protocols:** Alternative cryptocurrencies such as Ethereum enable the creation of secondary assets and smart contract capabilities natively, yet face challenges in scalability and privacy, while also incorporating a token which is used to pay for network native compute. These platforms are often less decentralized and may be vulnerable to censorship due to characteristics inherited from their parent altcoins.
- **Liquid:** Operating as a Bitcoin sidechain, Liquid supports native assets and offers confidential transactions, which obscure both the payment amount and the asset ID. Despite these features, the protocol's federated model limits its decentralization and makes it less resistant to censorship.
- **OmniBOLT:** As an extension of OmniLayer compatible with the Lightning Network, OmniBOLT shares features with RGB. It retains token-related data on-chain, which impacts both its privacy and scalability. Compatibility constraints also exist; OmniBOLT requires separate nodes for its own network and the Bitcoin Lightning Network, and cannot function using only Bitcoin Core.
- **Taproot Assets (formerly Taro):** Currently in its development phase without a mainnet release candidate, Taproot Assets aims to offer features comparable to RGB for creating and transacting with assets on the Lightning Network. Although developed by Lightning Labs, leaders in the Lightning ecosystem, it is still speculative whether Taro and RGB will achieve interoperability in the future.

Future Directions

RGB aims to fully support smart contracts within the Lightning Network, focusing on compatibility in the upcoming months. The promise lies in complex applications like DeFi, NFTs, and more, making RGB a strong contender for enhancing Bitcoin's smart contract functionalities, something that has mostly been reserved for EVM protocols so far.

Notable Projects in the RGB Ecosystem

One of the major potential use cases for RGB is bringing stablecoins to Bitcoin. USD backed stablecoins on other L1s and L2s have been key to the value proposition and user demand of these other networks. Although a highly controversial topic, RGB may offer a more scalable, cheaper, decentralized and more private solution for accessing and leveraging stablecoins. Currently, the total USD backed stablecoin supply is around $133 billion with Tether making up nearly 70% of the market. 55% of all stablecoin supply lives on Ethereum. Around 33% of the $91 billion USDT in supply lives on Tron.

Paolo Ardoino, CTO of Bitfinex and Tether, recently highlighted a new vision on the future of USDT leveraging RGB:

“We firmly believe that RGB will usher in a new era for digital assets, smart contracts, and digital rights, garnering comprehensive support from major players in our industry. Once USDT on RGB goes live, the world will witness USDT on another super-powerful and scalable Bitcoin layer.”

USDT has been attempted on Bitcoin’s Omni Layer before but with a lack of adoption and overall success. RGB may be the key for market players to pursue serious stablecoin efforts on Bitcoin while diversifying away from stablecoin dominant networks like Ethereum and Tron.

RGB PROJECTS

Infinitas

Infinitas was among the first projects that ventured into developing Turing-complete smart contracts based on the Bitcoin network. It integrates both the RGB protocol and the Lightning Network to realize goals like robust privacy safeguards, high transaction speed, and low-latency processing. Since its inception in 2021, the project has focused on fortifying the notion of Turing-complete smart contracts by utilizing Bitcoin's inherent security features and consensus models. The key people behind this venture are long-time contributors to Bitcoin core code and blockchain research. Infinitas aims to offer features such as an online development environment, data browsing capabilities, and wallet integrations to boost both developer and user engagement.

COSMINMART

COSMINMART builds upon the Lightning Network and is also compliant with RGB protocols. The COSM Wallet, one of its core offerings, is a versatile asset management tool that supports Bitcoin's mainnet, Lightning Network, and RGB assets. Additionally, the platform is working on COSM Market, aimed at facilitating trading of various Bitcoin-based derivatives. COSM Launchpad is another component, focused on identifying and supporting promising projects in the Bitcoin landscape. The company plays a pioneering role in defining Web4 and aims to integrate traditional apps deeply with the Lightning Network.

Pandora Prime

Pandora Prime combines RGB smart contracts and Lightning Network, focusing on high transaction throughput and lower KYC requirements for certain transactions.

MyCitadel

Operating under the umbrella of Pandora Prime, MyCitadel offers the first GUI wallet supporting RGB. Developed in 2021, it provides a user-friendly asset management experience and is available as a cross-platform desktop application as well as iOS/iPad applications.

RGB Explorer

RGB Explorer is another initiative by Pandora Prime and stands as the first browser designed to enable RGB asset registration and smart contract interactions. It currently supports a variety of asset types such as RGB20, RGB21, and RGB25.

DIBA

DIBA focuses on community development by helping people understand, possess, and utilize decentralized digital assets built on Bitcoin. It is notably the first marketplace to use RGB smart contracts and the Lightning Network for trading Bitcoin NFTs.

Bitmask

A product of DIBA, Bitmask is the initial NFT wallet within the RGB landscape. Designed to operate directly in web browsers, it enables user interaction with RGB contracts, much like MetaMask does for Ethereum.

IRIS Wallet

Developed by the Bitfinex team, IRIS Wallet is focused on integrating RGB and offers support for both fungible and non-fungible assets. It aims to simplify RGB asset operations, from creation to spending and receipt, in a user-friendly wallet interface.

Bitswap-BiFi

Bitswap-BiFi is an emerging project focusing on decentralized exchange (DEX) solutions for RGB assets. Currently, in the validation phase, it aims to introduce "SWAPS" into a DEX framework, although it does not yet support Automated Market Makers (AMM) or Liquidity Provider (LP) functionalities.

CONCLUSION

In summary, RGB stands as a revolutionary smart contract framework designed explicitly for Bitcoin and its Lightning Network, offering cutting-edge functionalities that range from DeFi to NFTs. Unlike traditional smart contract platforms that rely on network-wide computation, RGB employs client-side validation, enhancing both scalability and privacy. Despite the slow adoption rates attributed to its complexity, the framework garners strong support from industry leaders and boasts an increasingly robust ecosystem. Although substantial progress has been made, further work is required to realize its full potential in extending Bitcoin's capabilities, promising an exciting future in redefining what Bitcoin can achieve.

Parameter	**RGB**	**Liquid**	**Ethereum, RSK etc**	**Taproot Assets**
Native Currency	✅ BTC	⚠️ LBTC (federated peg)	🚫 ETH	✅ BTC
Requires token	✅ No	✅ No	🚫 Yes (Except RSK)	✅ No
Issues token	✅ No	✅ No	🚫 Yes	✅ No
Gas	✅ No	✅ No	🚫 Yes	✅ No
Non-token smart contracts	✅	🚫	✅	🚫
Data network for NFTs and attachments	✅ Storm on LN paid in sats	🚫	⚠️ IPFS (no incentivisation)	Unknown
Support for arbitrary structured data	✅	🚫	✅	🚫
Virtual machine	Bitcoin Script + AluVM	Bitcoin Script	EVM, sometimes EWASM	Bitcoin Script
Turing completeness	✅	🚫	✅	🚫
Separation of state from ownership	✅	🚫	🚫	✅
Client-side-validation (scalability & privacy)	✅	🚫	🚫	✅
Zero knowledge	✅ Bullet Proofs	✅ Range Proofs	⚠️ n/a, maybe STARK's	🚫
Breaks transaction graph & chainanalysis	✅	🚫	🚫	🚫
Released / used in production	✅	✅	✅	🚫

Source: **RGB Blackpaper**

UTXO

UTXO.MANAGEMENT