

Emergence of Token Layers on Bitcoin:

Overview of Client-Side Validation, RGB and Taro





Diamond Hands

Bitcoin
Technology
Provider



Japan's No.1
Lightning
Community



Diamond Hands

Services

- Research & Consulting
- Lightning Payment Processing
- System Integration
- LSP, Routing Node Operation
- Community & Education

Presented by

Authors

Kishin Kato | Trustless Services K.K. CEO
Koji Higashi | Diamond Hands co-founder & Head of Business Development
Yuya Ogawa | Diamond Hands co-founder & Head of Technology



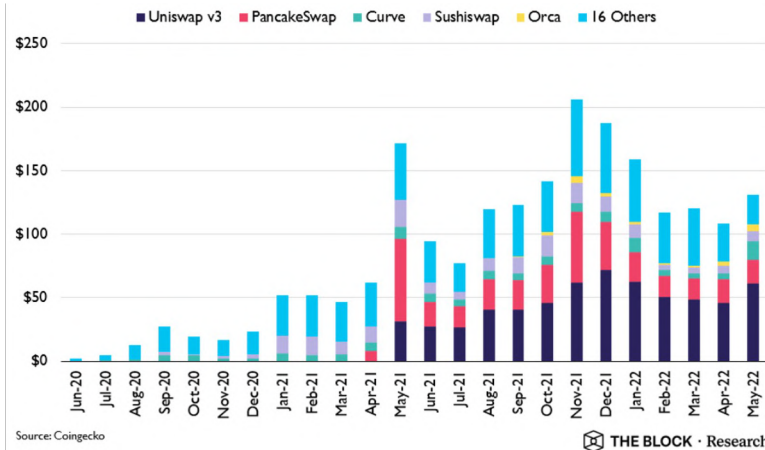
Diamond Hands

Global Consensus: How Tokens Are Used Today

Token issuance and usage is growing, with most choosing smart contract chains such as Ethereum

The market for on-chain token transfers and trades is growing

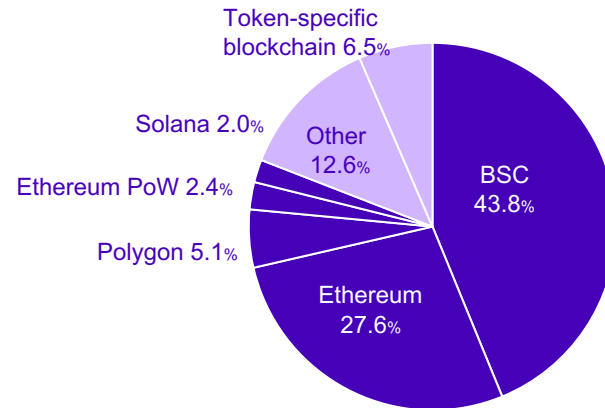
DEX Volume over time (\$bn)



Source: "Pooled Liquidity Provision in DeFi", June 2022, The Block Crypto, Inc.

Most token issuance is happening on smart contract chains

Platforms used by tokens listed on exchanges in the past 2 months



Source: CoinGecko <https://www.coingecko.com/ja/new-cryptocurrencies>

Smart contract chains use Global Consensus, a simple but inefficient approach

The Global Consensus Model:

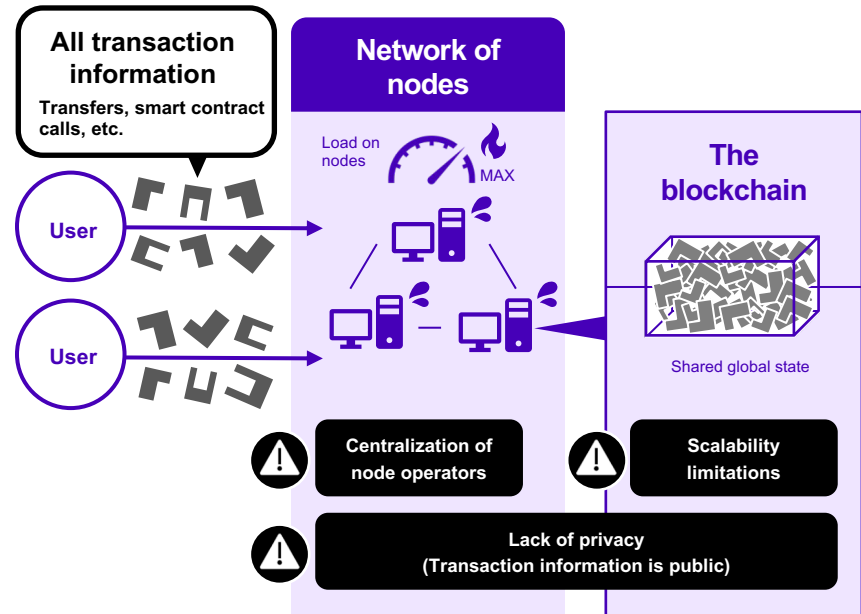
- All nodes validate all transactions
- Shared global state is conceptually simple
- Transparency enables open access

Cons



- **Scalability limitations**
Validating all contract interactions gets expensive
- **Centralization of node operators**
High costs discourage users from running nodes
- **Lack of privacy**
Transactions are public and available to third parties

How Global Consensus works





Diamond Hands

The Client-Side Validation (CSV) Model for Tokens



Transaction details can be moved off-chain without compromising on immutability

1

The fundamental purpose of a blockchain is to be an **immutable ledger of transactions**.

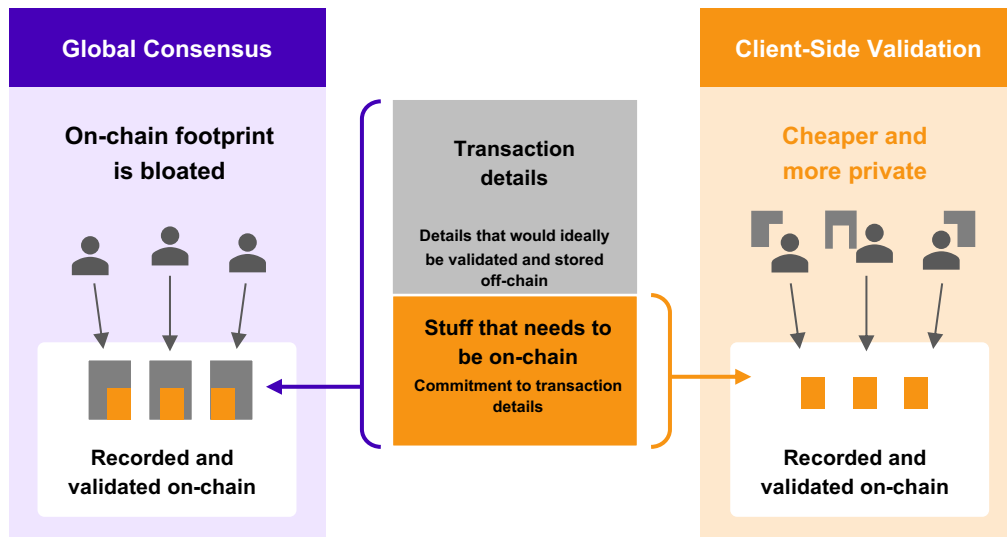
2

Transaction details can be validated privately; witnesses are only required for proving it occurred at a point in time.

3

Users store the details and results privately, committing to them in simple, nondescript on-chain transactions.

Commit only the bare minimum of information on-chain and keep details privately validated and stored off-chain



Client-Side Validation(CSV) improves scalability and privacy by moving validation off-chain

The Client-Side Validation Model:

- Store only transaction commitments on-chain
- Detailed transaction information is off-chain, and validated solely client-side
- Validate only the transactions you must

Pros



■ Scalability

- Lower costs and less computational load

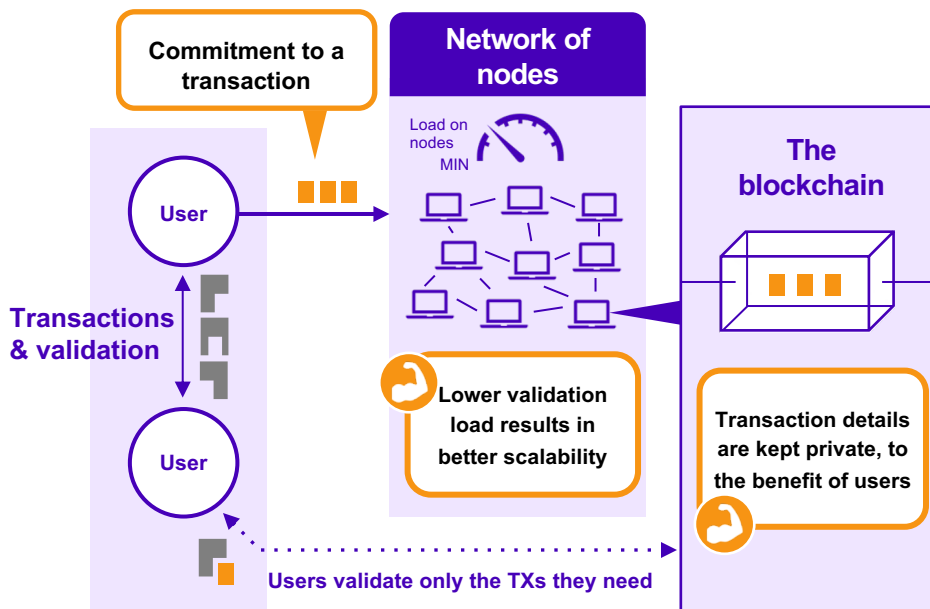
■ Privacy

- Transactions unintelligible to third parties

■ Usable on Bitcoin

- No need for complex on-chain transactions; usable today on Bitcoin

How Client-Side Validation works



Comparing Client-Side Validation and Global Consensus for token issuance

Client-Side Validation (e.g. RGB, Taro)

Global Consensus (e.g. ERC20)

On-chain token transfer fees	Contract execution and native token transfers have the same, constant fee	Token transfers are more expensive than native token transfers, and the cost of contract calls scales with contract execution complexity
Privacy	Third parties cannot observe token distribution, balances, or transfers	Third parties can easily observe token holder activity; no privacy
Third party utilization	Lack of a public global state necessitates cooperation from individual token/asset holders. Snapshots impossible	Public global state allows easy creation of snapshots and validation of token ownership at a point in time without user interaction
Dev ecosystem	Developer ecosystem still in infancy	Large developer base and good tooling thanks to years of popularity
Data availability problem	Storage of off-chain data is required to use tokens in the future	Private key is sufficient to store tokens
Onlineness requirement	Users must either be online when receiving payments, or use a service that will receive, validate and store off-chain data on their behalf	Users can receive payments offline by simply providing an address



Diamond Hands

The Benefits of CSV Tokens on Bitcoin

Tokens on Bitcoin using CSV have stability, scalability advantages

Benefits of issuing tokens on Bitcoin:



The most stable blockchain infrastructure

Bitcoin is the most decentralized and most secure blockchain today. With minimal reliance on any corporation or individual, Bitcoin is least likely to face sudden failure.



Interoperability with Bitcoin

Issued tokens will be highly interoperable with the most popular and owned crypto asset in the world. Transact with trustless financial contracts built on Bitcoin.



Connect to the Lightning Network

Cheap, fast, and stable payments on Lightning can also benefit tokens issued on Bitcoin.

Lightning Network infrastructure can be applied to transact with tokens on Bitcoin

Connecting token-specific payment channels to the Lightning Network may bring benefits to the entire ecosystem of users, developers, and Lightning node operators



Users

Make **fast and cheap payments & swaps** over Lightning.



Developers

Use **existing infrastructure** such as Lightning node implementations and wallets.



Lightning Nodes

Token transactions and swaps bring more **business models and routing fees**.

The development of CSV tokens will expand Bitcoin's capabilities & grow its ecosystem

The effects of tokens on Bitcoin

1 Bitcoin as a one-stop shop

As Bitcoin gains various capabilities through the use of CSV, developers will be able to build solutions entirely on Bitcoin.

2 Assisting Bitcoin adoption

During the transition to mass adoption, stablecoins on Bitcoin will provide much-needed convenience for fiat-denominated transactions. In turn, tokens on Bitcoin may drive the adoption of bitcoin the asset itself.

3 More developers and corporate participation

When token issuance and complex financial contracts become readily available on Bitcoin, we expect more developers to build on Bitcoin, enabling more corporations to utilize the asset and network in their products and services.

*Token issuance on Bitcoin is not unanimously accepted as positive; some oppose the concept with valid concerns and criticisms. See appendix for alternative approaches.



Diamond Hands

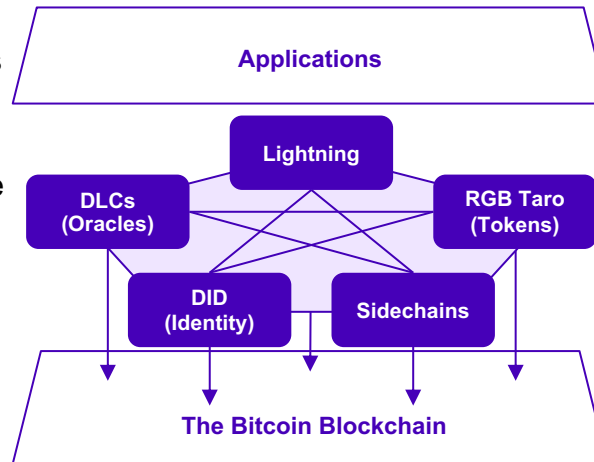
The Future and Challenges of Tokens on Bitcoin

Taking complex validation off-chain enables the development of a scalable financial layer on Bitcoin

As opposed to the Global Consensus model seen in smart contracting blockchains, we expect Client-Side Contracts and other off-chain protocols to form the foundation for sophisticated financial functions on Bitcoin.

What are Client-Side Contracts?

- Contracts shared only by the relevant parties
- Non-custodial and private
- More scalable than smart contracts using the Global Consensus model
- Extremely censorship resistant

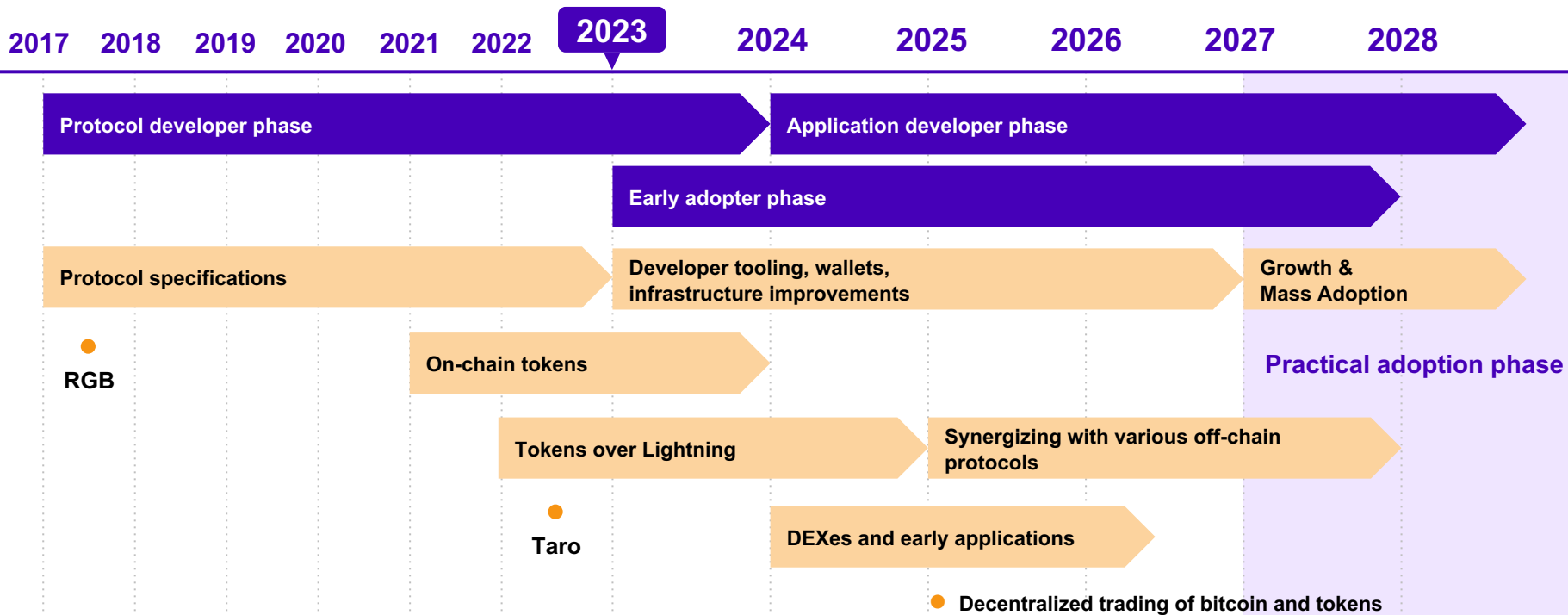


- Non-custodial, private applications
- Scalable financial applications

- Off-chain P2P contracts
- Off-chain data compatibility
- Minimizing on-chain usage

- Anchoring off-chain data
- Security and immutability from PoW

CSV tokens on Bitcoin are a work in progress; Mass adoption is likely still several years out



The CSV model does not obsolete all use cases for the Global Consensus model

Client-Side Validation advantages

Scalability, Privacy, Censorship Resistance

Example 1 : **Stablecoins**

In addition to the privacy benefits CSV provides, Lightning compatibility enables fast, cheap payments.

Example 2 : **Peer-to-Peer token exchanges**

CSV enables users to trade tokens and bitcoin in a private, self-sovereign, and scalable way.

Example 3 : **Bitcoin-native finance**

Building on Bitcoin enables financial integration without the need for centralized and risky products such as Wrapped BTC.

Global Consensus advantages

Transparency, Liquidity Pools, Contract-to-Contract Interactions

Example 1 : **NFTs**

Third parties are easily able to identify ownership information and transactions because the global state is public.

Example 2 : **AMM (Automated Market Makers)**

Multiple users can simply deposit their liquidity into a shared state which is updated when trades occur, such as with Uniswap.

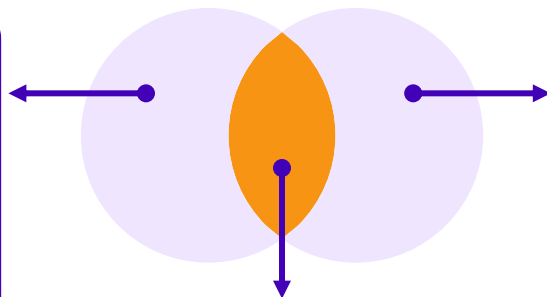
Example 3 : **Composable Financial Products, Aggregators**

Contract state being public enables a high level of composability, where contracts can make calls to other contracts.

The token ecosystem on Bitcoin is behind, and specific challenges such as data storage exist

Challenges specific to Client-Side Validation

- **Limits to off-chain validation**
Significant use will eventually increase validation costs for popular CSV tokens.
- **More data must be stored**
Losing the off-chain data used to validate a transaction prevents the user from ever spending it: holding requires storing more than keys.



Ecosystem is still in its infancy

The ecosystem is still in its early days. Developer tooling and user onboarding could take several years.

Challenges specific to token issuance on Bitcoin

- **On-chain throughput is limited**
Bitcoin has limited transaction throughput compared to other blockchains.
- **Incentives may misalign**
Tokens on Bitcoin may introduce external influences that interfere with the incentives that make Bitcoin work (e.g. during contentious forks).



Diamond Hands

Overview of Topical CSV protocols

- ▶ **RGB**
- ▶ **TARO**



RGB



- 1 RGB is a smart contract platform on Bitcoin
- 2 An MVP implementation was released in 2019
- 3 Non-profit LNP/BP Association leads protocol development along with other external entities
- 4 The first contracts available are token contracts

RGB aims to enable more scalable and private smart contracts on Bitcoin

RGB is a Client-Side Validated smart contract platform

Single-Use Seals are used to associate off-chain contract state with a Bitcoin UTXO, which is eventually spent (closed) in a way that commits to an off-chain RGB transaction that executes the next state transition.

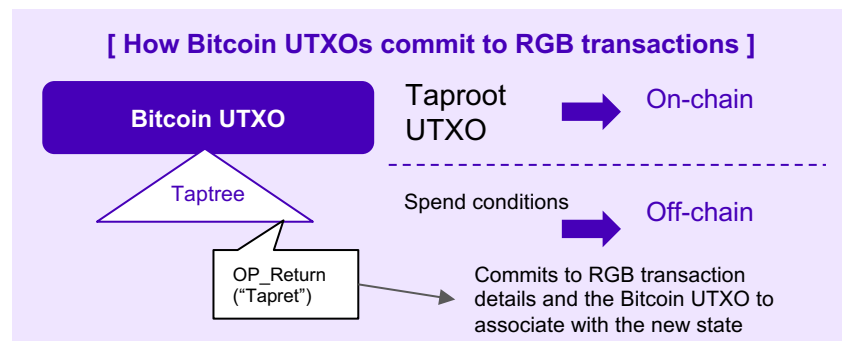
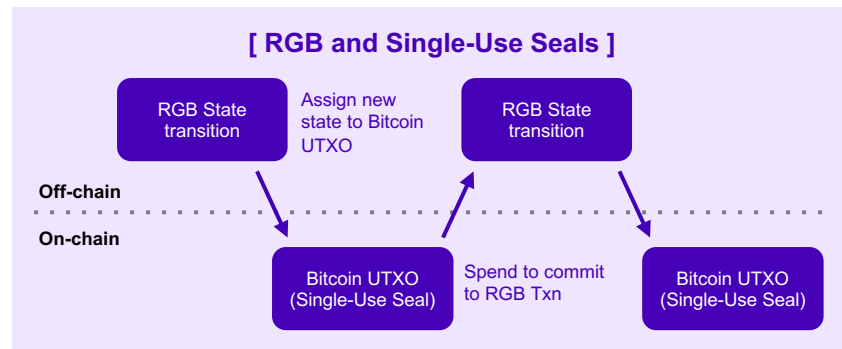
RGB strengths:

1. Privacy

Third parties do not see RGB transactions nor their associated Single-Use Seals. Even the issuer is unable to detect transactions as the set of current holders and their UTXOs is unknowable.

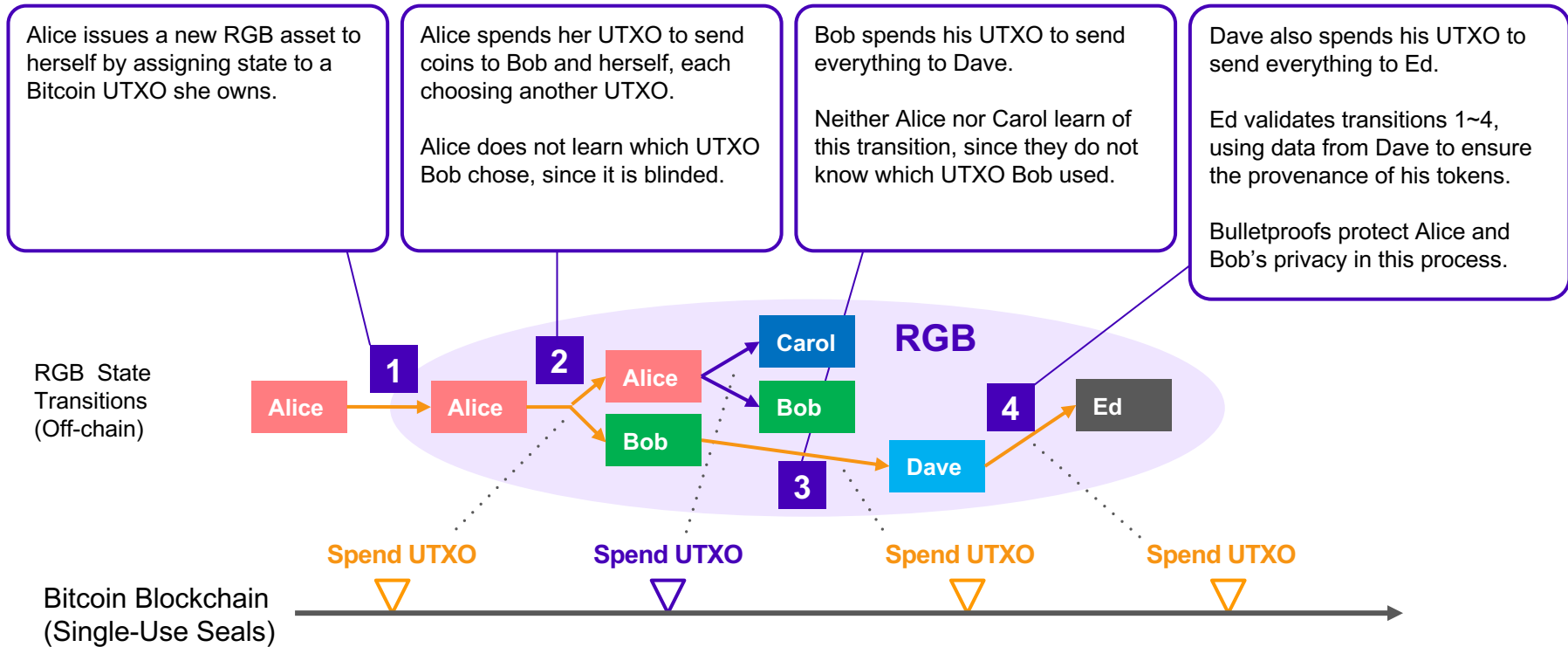
2. Smart contracting capabilities

Client-Side executed smart contracts are more private and will be more flexible than bitcoin script contracts executed on-chain.





RGB state transitions are validated off-chain by consuming UTXOs on the blockchain

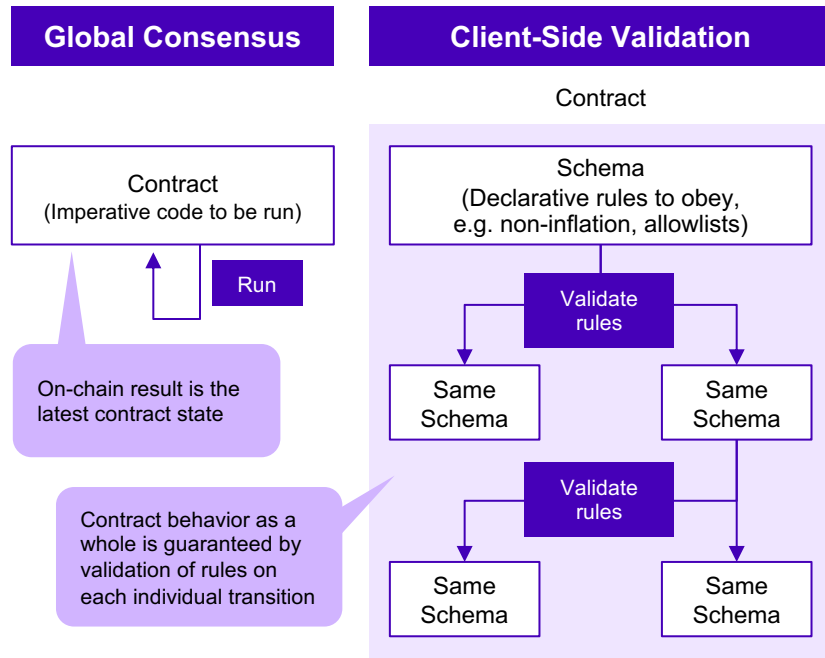


RGB contracts limit individual state transitions to guarantee an unobservable global property

RGB contracts are a collection of “local rules”

As with token transfers, RGB contract state is distributed among many users. Smart contracts on RGB declaratively describe the rules each state transition must follow as a *Schema*, ensuring that the contract as a whole, though unobservable, follows the intended emergent property.

User conditions (“who”) can be handled on-chain by UTXO ownership, whereas spending conditions (“how”) are written as RGB contracts. In the future, the AluVM virtual machine will be used to validate schemas, but common schemas are preinstalled and can be validated natively (e.g. RGB20).



RGB is highly capable and full of potential, but its complexity and scope pose a challenge

Challenges faced by RGB:

1. Steep learning curve

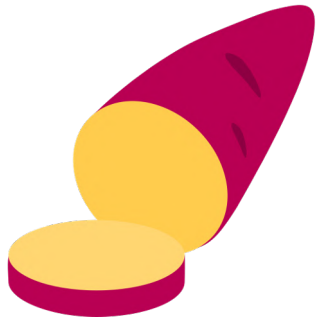
In addition to Bitcoin transactions used for Single-Use Seals, developers must learn to handle new concepts such as RGB state transitions and contracts, which have a steep learning curve that may slow bottom-up adoption.

2. Ambitious scope

In order to achieve the ambitious goal of enabling various smart contracts off-chain, RGB faces a significant amount of work to build its developer ecosystem. Novel user interfaces will also be needed for market adoption.



TARO



- 1 Taro is a token protocol for Bitcoin that uses Taproot
- 2 Lightning Labs leads development
- 3 Announced at the Bitcoin 2022 conference in April 2022
- 4 Taro stands for "Taproot Asset Representation Overlay"

Taro is a token protocol that applies Taproot, focusing on Lightning compatibility

Taro is a CSV token protocol

Bitcoin Taproot UTXOs that commit to Asset Trees containing balances of Taro assets are spent in Bitcoin transactions, creating new Taproot UTXOs containing the resulting Taro asset balances.

TARO strengths:

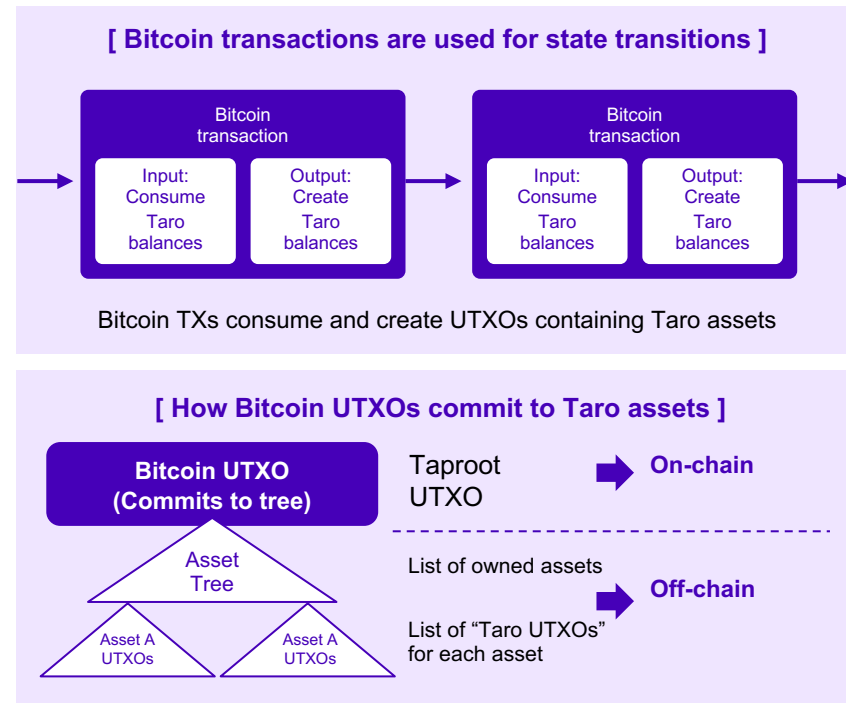
1. Lightning compatibility

Taro was designed with Lightning compatibility in mind, and the conceptual model of state transitions using Bitcoin transactions is easy for developers to understand.

2. Lightning Labs leading development

With Lightning Labs' backing, Taro is likely to make it into popular Lightning node implementation(LND) when ready, which could help it quickly gain users.

※Taproot introduced the ability for multiple scripts that unlock a UTXO to be stored in a tree data structure. The user can spend a UTXO either with the corresponding key (key-spend) or fulfilling one of these scripts (script-spend); scripts are never revealed except for the single one used in a script-spend.

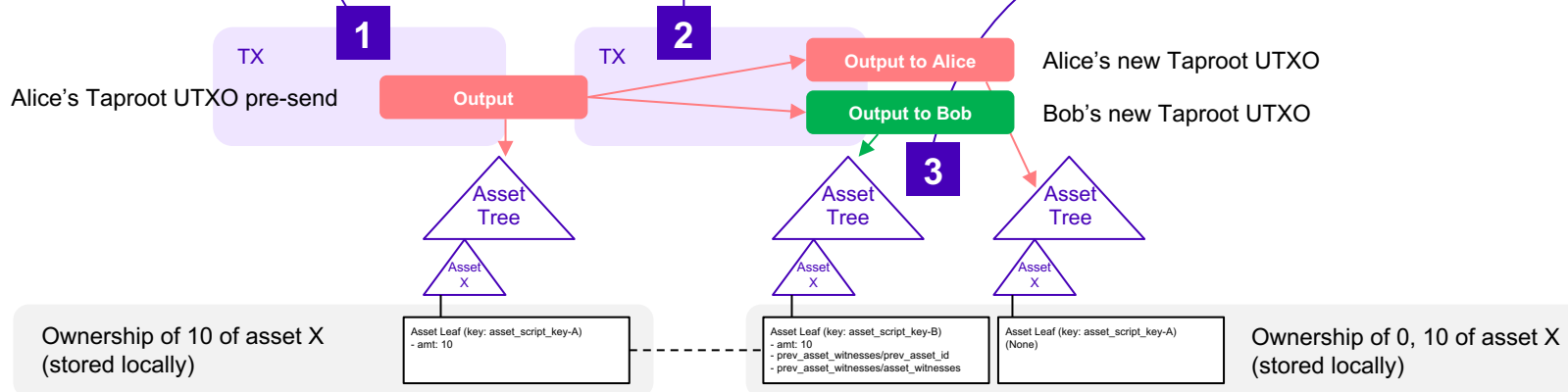


Taro transactions use Bitcoin transactions to consume old balances and create new ones

Alice issues a new Taro asset to herself by creating a new Taproot UTXO committing to the Taro asset.

Alice sends all 10 of her assets to Bob by spending her previous UTXO and sending to new UTXOs of Bob's and hers each committing to the new balances of 0 and 10.

As with RGB, Bob validates transactions 1 ~ 2 to ensure the provenance of these assets. Alice must provide this data.







Taro's lower prioritization of on-chain usage may tend users toward permissioned payment aggregators

Challenges faced by Taro:

Incomplete on-chain specifications and the allure of permissioned services

Taro development seems to focus on off-chain transactions over on-chain sending. For instance, the on-chain protocol is incomplete, and may end up requiring complex coordination. Taro also offers no on-chain scalability benefits, nudging users towards Lightning and other transaction aggregators.

In Taro, anybody can operate a Pocket Universe, where one Bitcoin UTXO commits to many users' Taro assets, enabling the aggregation of many Taro transfers. While cheap and convenient, Pocket Universe operators can freeze assets, preventing them from being transferred or withdrawn.

	 User owns keys to Bitcoin UTXO	 Someone else owns keys to Bitcoin UTXO
 User owns keys to Taro UTXO	User is self custodial Taro asset	User can have their assets frozen, but not stolen (Using a Pocket Universe)
 Someone else owns keys to Taro UTXO	User is operating a Pocket Universe	User is in a traditional custodial relationship

RGB and Taro have differing characteristics and properties, and will likely serve different use cases



RGB

- Third parties cannot detect transactions, and even senders and recipients are somewhat protected from each other.
- On-chain traceability is zero.
- RGB state transitions add an abstract layer that differs greatly from Bitcoin transactions, posing a challenge to Lightning developers.
- Future plans to support sophisticated financial applications through turing complete smart contracts.
- GUI wallet supporting tokens is available.
- Lightning support and non-token schemas have yet to arrive.
- On-chain transaction size can be constant, and in fact cheaper than standard bitcoin transactions.
- Privacy-focused stablecoins and IOUs, Bitcoin Finance

Privacy

Lightning compatibility

Smart contracts

Current state of project

On-chain fees

Ideal use cases

Taro

- Third parties may detect payments in some cases, but details belong only to sender, receiver, and future recipients.
- Transfers leave an on-chain trace.
- Additional concepts are not abstract, and possibly more familiar to Lightning developers.
- Lightning Labs' support is an advantage for adoption.
- Focusing on tokens over general-purpose smart contracts for the time being.
- CLI wallet exists, but key specifications still not determined.
- Lightning support yet to be delivered.
- Same fees as bitcoin transactions; more recipients leads to higher fees.
- Stablecoins, rewards points, IOUs

Conclusions

➤ There are clear advantages to CSV tokens on Bitcoin

Client-Side Validation tokens on Bitcoin, particularly in combination with layer 2 technologies such as the Lightning Network, offer clear advantages in terms of scalability and privacy when compared to the status quo of Global Consensus blockchain tokens.

➤ The financial applications of CSV have immense potential

Off-chain protocols, including those using Client-Side Validation, will synergize to create a sophisticated financial layer atop Bitcoin. This development will, in turn, accelerate bitcoin adoption through increased utility.

➤ The technology is young, and there is a long road ahead

CSV tokens are a novel concept requiring new tooling and user interfaces; this process takes time. Furthermore, specific use cases that are a fit for CSV must be found that are able to onboard users in order to gain relevance.

➤ RGB and Taro have key differences in their priorities and tradeoffs

RGB and Taro are sometimes portrayed as competing CSV token protocols, but have key differences in their priorities and tradeoffs, which lead to diverging use cases. RGB's novel off-chain smart contracting and Taro's Lightning-oriented tokens can coexist.



Diamond Hands

Appendix



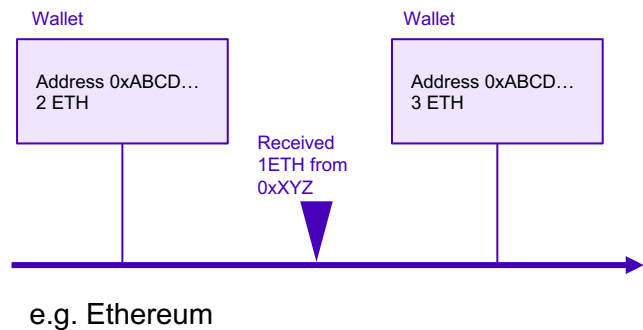
Account model vs. UTXO model

Accounts :

Each account has a balance, which is updated as a result of transactions.

Users often reuse a single address.

In other words, address == account.

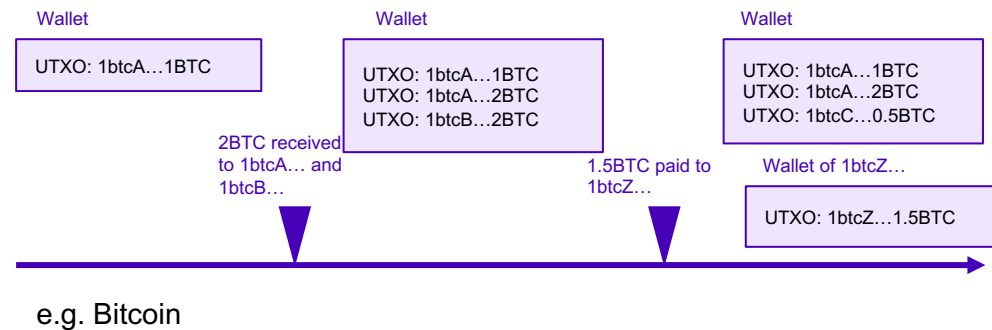


UTXOs :

Transactions create outputs to addresses, such that $\text{sum}(\text{outputs})$ does not exceed $\text{sum}(\text{inputs})$. Inputs are chosen from previously unspent outputs.

Coins are managed as outputs, even if they were sent to the same address.

Users usually have multiple addresses.



Many financial uses cases on Bitcoin do not require the use of tokens

Some point out the possible negative influence tokens on Bitcoin may bring. Indeed, developers have been working on financial solutions and techniques that just use bitcoin instead.

Financial technologies on Bitcoin that do not require tokens

DLCs(Discreet Log Contracts) :

Contract-for-difference protocol similar to payment channels that enables users to trade trustlessly based on results reported by an oblivious third-party oracle. Non-custodial, private, P2P financial transactions.

【 Products using DLCs 】

Atomic Finance, DLC.link

Stablesats :

Automated hedging of bitcoin on a derivatives exchange to stabilize the dollar value of a Lightning channel. Allows users to replace stablecoin credit risk with futures exchange counterparty risk.

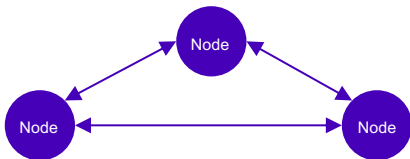
【 Products like Stablesats 】

Bitcoin Beach Wallet, Collider



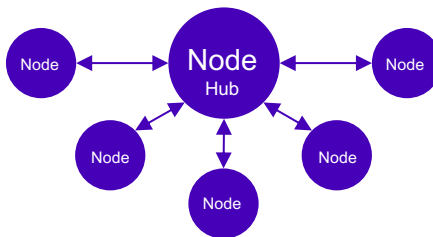
How tokens may interface with Lightning

Peer-to-Peer



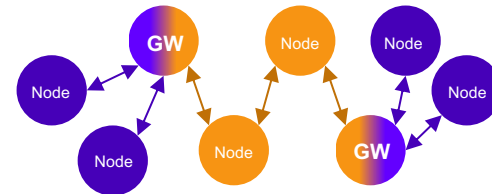
- ◎ Maximal privacy
 - ◎ Payments to direct peers are free
 - × Capital inefficient - low utilization
 - × Non-business nodes can be unreliable
- Good for assets where privacy is important, or for frequent transactions with a certain counterpart

Hub-and-Spoke



- ◎ Capital efficient - keep just 1 channel
 - × Relies on hub service
 - × Privacy from hub can be very low
- Good for assets relying on centralized operators anyway, or when cost savings are crucial but privacy is not

Gateways (GW)



- ◎ Connect to Bitcoin LN liquidity
 - ◎ Can be used to trade assets, BTC
 - × Complexity may cause unreliability
 - × Exchanging assets is expensive
 - × Gateways only for tokens with volume
- Good for using as a DEX

Taro and RGB can both be used in any way above. The most likely outcome is that most users prefer connecting to a hub, and some hubs provide services as gateways, enabling users to send or exchange tokens, even across different token protocols.

Liquid Network has smart contracts that extend Bitcoin's scripting capabilities

The Liquid Network



Consortium sidechain operated by the Liquid Federation and Blockstream.

Although it is based on Bitcoin, additional opcodes (functions) improve privacy and smart contracting, with functions such as tokens and covenants available for use.

Applications

- Liquid Network enables financial applications beyond what is possible on Bitcoin. For example, issuing, trading, and settling transferable options contract tokens on-chain.
- Some Bitcoin users also use Liquid L-BTC to rebalance their Lightning channels. Similar interoperability can be explored in various scenarios, taking advantage of high compatibility and relatively low validation costs.

Client-Side Validation similarities to Rollups on Ethereum

What is a Rollup?

An Ethereum scaling solution, Rollups let users deposit funds in a smart contract, after which the tokens can be transferred among users of the same Rollup off-chain. These transactions are aggregated and committed on-chain periodically in a verifiable manner.

Client-Side Validation	Optimistic Rollup	ZK-Rollup
Similarities	<ul style="list-style-type: none">Ethereum nodes do not validate the aggregated commitments; users do (if they care to)	<ul style="list-style-type: none">Users can validate state transitions and balances from transaction data and validity proofs
Differences	<ul style="list-style-type: none">Lack of privacyOn-chain smart contract used for permissionless exiting and for fraud proofsNodes must store potentially vast amounts of transaction data (data availability problem)	<ul style="list-style-type: none">State transitions and validated by all Ethereum nodes via an on-chain contract; this is not Client-Side ValidationValidity proofs must be submitted to the blockchainCensorship resistance is eroded if transaction data is not also stored on-chain (data availability problem)

References ①



Diamond Hands

37

Client-Side Validation

- <https://scalingbitcoin.org/transcript/milan2016/client-side-validation>
- <https://github.com/LNP-BP/presentations/blob/master/Presentation%20slides/PRISM%20-%20RGB%20computing%20model.pdf>

Single-Use Seals

- <https://petertodd.org/2016/commitments-and-single-use-seals>

Lightning Network

- <https://lightning.network>
- <https://docsend.com/view/e67t2yst5yvijt76>

RGB

- <https://rgb.info>
- <https://github.com/LNP-BP/LNPBPs>
- <https://github.com/RGB-WG>
- <https://medium.com/@FedericoTenga/understanding-rgb-protocol-7dc7819d3059>
- <https://bitcoinmagazine.com/technical/rgb-magic-client-contracts-on-bitcoin>
- <https://www.rgbfaq.com/>

Taro

- <https://github.com/lightninglabs/taro>
- <https://docs.lightning.engineering/the-lightning-network/taro>
- <https://medium.com/nayuta-inc/taro-ed6b93b09a75>
- <https://river.com/learn/what-is-taro-in-bitcoin/>
- <https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro.mediawiki>

References ②



Diamond Hands

38

DID

- <https://github.com/decentralized-identity/ion>
- <https://developer.tbd.website/projects/web5/>

Decentralized Social Social Media

- <https://nostr.com>

DLCs

- <https://bitcoinops.org/en/topics/discreet-log-contracts/>
- <https://river.com/learn/terms/d/discreet-log-contract-dlc/>

Stablesats

- <https://stablesats.com/>

Liquid

- <https://blockstream.com/liquid/>