PRODUCTS

MAY - OCTOBER, 2025

Citrea

Citrea

https://citrea.xyz/

- Bridge: Clementine
  - v1: BitVM2 bridge: the amount of Peg-In is fixed (10 BTC?)
  - v2: Garbled circuits and TOOP (under development)
- L2
  - zkEVM (Type 2.5) utilizing RISC Zero
  - Both zkSNARK and zkSTARK are utilized.
- DA layer
  - Utilizes Bitcoin L1
  - Inscription like
- Note:
  - Blocks are generated in approximately 2 seconds on L2.
  - It appears that they post to L1 on an hourly basis.



- RISCzero
- revvm/reth
- Succinct
- BitVM

Bitlayer

Bitlayer Version 2

Bitlayer

https://www.bitlayer.org/

- Bridge
  - BitVM2 bridge
- L2
  - Multi-VM concept enabling the management of multiple VMs on a single machine.
    - Currently, only EVM is available.
- DA layer
  - Fraud Proof with BitVM2
- Note:
  - As of June 2025, the PoS sidechain (v1)
  - To Rollup in Q1 and Q2 of 2025
  - Enhancement of TPS and related aspects in Q4 2025



- geth-based

B^2 Network

B² Network

B² NETWORK

https://www.bsquared.network/

- Bridge
  - Custom bridge
- L2
  - EVM compatible (Customized Polygon zkEVM)
- Note:
  - A fraud-proof method in which a zk-proof is written into Bitcoin L1 and accepted if no fraudulent claims are made.
  - Has a separate DA layer



- Polygon zkEVM

Starknet

Starknet

Starknet is currently running on Ethereum mainnet. The roadmap for a Bitcoin version is unclear.

STARKNET

https://www.starknet.io/

- Bridge
  - L2 verifiable with Bitcoin scripts(OP_CAT, etc...)
  - As a temporary solution, they are also developing multi-signature methods and BitVM.
- L2
  - CairoVM (language: Cairo)
  - Ensure compatibility with both Ethereum and Bitcoin.
  - zkSTARK
- Note:
  - OP_CAT Proof of Concept on Signet (November 2024)

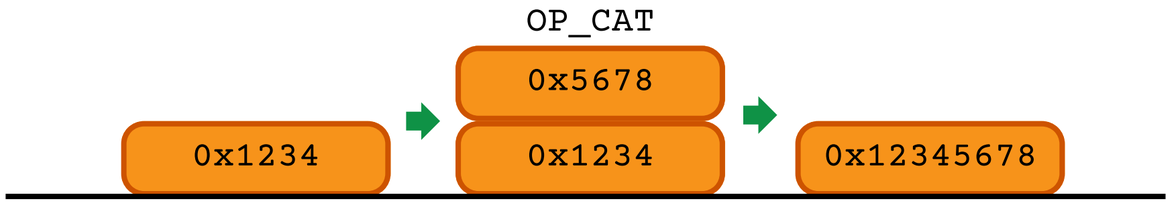
- MultiSig?
- BitVM bridge.
- OP_CAT?



- CairoVM
- STWO

OP_CAT

- It is an abbreviation for concatenate.
- This command concatenates two pieces of data stored on the Bitcoin stack.
- It was introduced in the initial versions of Bitcoin Core but was discontinued in 2010 due to security concerns.
- The proposed BIP-347 restricts the total size to 520 bytes and generates an error if this limit is surpassed.



Word	Opcode	Hex	Input	Output	Description
OP_CAT	126	0x7e	x1 x2	out	Concatenates two strings. *disabled*.
OP_SUBSTR	127	0x7f	in begin size	out	Returns a section of a string. *disabled*.
OP_LEFT	128	0x80	in size	out	Keeps only characters left of the specified point in a string. *disabled*.
OP_RIGHT	129	0x81	in size	out	Keeps only characters right of the specified point in a string. *disabled*.
OP_SIZE	130	0x82	in	in size	Pushes the string length of the top element of the stack (without popping it).



OP_CAT

OP_CAT allows us to do things that were previously impossible.

- Covenants: Limitations on recipients and the amounts of remittances
  - Recursive covenants facilitate pseudo-states, among other possibilities.
- Constructing and validating a Merkle tree
- Tree Signatures
- Lamport, the originator of the quantum-resistant signature
- Non-cheating agreements: Sanction for duplicate expenditure
- STARK Validation
- etc...

Covenants in OP_CAT

Bitcoin scripts are unable to access the amount being transmitted or the destination address, thus it is typically not feasible to incorporate these conditions into the script.

However, by leveraging the Schnorr signature calculation method and incorporating conditions into the private key, it becomes feasible to compute the hash value of a transaction.
Direct specification of the amount to send or the destination address is not feasible; however, it can be indicated through the transaction hash.

Consequently, the script retains the hash value of the remittance amount and the remittance destination address, while additional data is supplied through the stack. These elements are subsequently concatenated to generate a transaction hash value, which is then compared to enforce constraints.



Rootstock

Rootstock



https://rootstock.io/

A well-established sidechain system, previously referred to as RSK Network, also functioned on the mainnet.

- L2
  - EVM compatible(Rootstock VM)
- Mining
  - Merged Mining is a technique that enables Bitcoin miners to also function as Rootstock miners.
    - Auxiliary Proof-of-Work

Liquid Network

Liquid Network

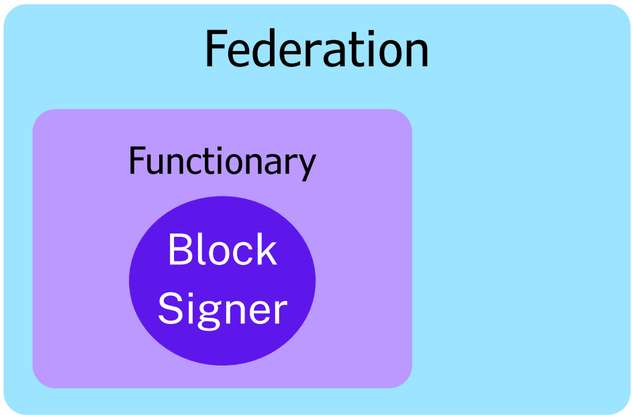


https://liquid.net/

- Sidechain developed by Blockstream
- The native token : L-BTC
  - Tokens can be issued with the permission of the Federation。
- Blocks are generated every minute
- The consensus algorithm is referred to as Strong Federation.
  - Currently, 11-of-15 multisig.
- Confidential Transactions can be established to obscure amounts and assets.
  - Hidden yet verifiable

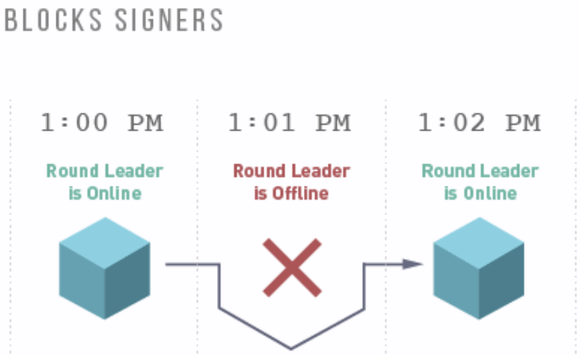
Functionary

- Liquid Federation comprises 81 members.
  - Members can operate the bridge.
- Among them, the individuals who directly manage the nodes are referred to as ”Functionary”.
  - Dedicated server equipped with HSM(Hardware Security Module)
  - Peg-In/Peg-Out etc.
- 15 of the Functionary companies are Block Signers.
  - Proposing and signing blocks
  - Selection considering geographical and geopolitical diversity
  - Members may be substituted without disrupting chain operations.



Block Signer

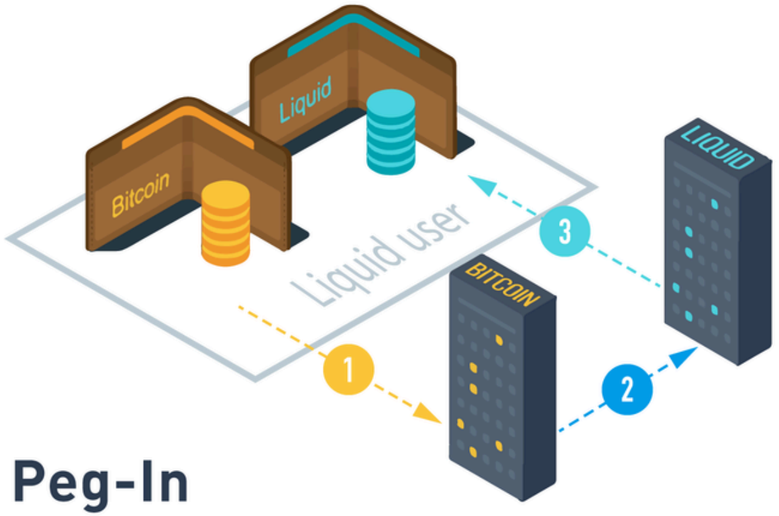
- One of the Block Signers assumes responsibility for proposing a block and gathering signatures.
  - 11 out of 15 Block Signer signatures required
    - Contingency plans are in place in case signatures are not collected.
  - The roles will be rotated in a round robin format.
  - If the round is not completed within one minute, the round is failed and the next round begins.
- Since there is a slight possibility of a reorg, finality occurs after the next block is approved.
  - This only happens when communication is unstable.
  - It does not branch beyond one block.



https://docs.liquid.net/docs/technical-overview

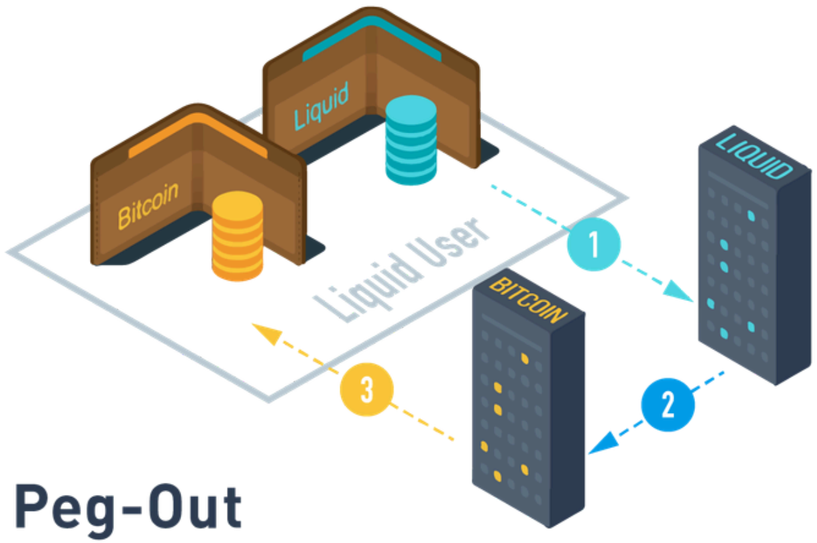
Bridge

- The Bitcoin-Liquid bridge utilizes the same key as Block Singer.



Peg-In

1. Liquid user sends BTC over the Bitcoin Network to peg-in address.
2. Liquid user waits for 102 confirmations. Functionaries in Liquid Network now accept this freezing of BTC and allow access to L-BTC.
3. Liquid user claims L-BTC and it appears in their Liquid wallet.



Peg-Out

1. Liquid User creates a peg-out transaction to request release of BTC.
2. Liquid Network releases BTC after 2 Liquid confirmations.
3. Liquid User receives BTC into Bitcoin wallet.

https://docs.liquid.net/docs/technical-overview

Confidential Transaction

- Liquid's transaction framework resembles that of Bitcoin.
- Transaction formats that conceal amounts and assets can also be used.
  - It is referred to as a Confidential Transaction.
  - The identities of the sender and recipient cannot remain confidential.
- It is confidential yet verifiable.
  - The aggregate of the total INPUT and the total OUTPUT equals zero.
  - Neither negative nor excessive.

Scripts

Opcode

New
OP_CHECKSIGFROMSTACK
OP_DETERMINISTICRANDOM
OP_INSPECTINPUT
OP_INSPECTOUTPUT
OP_COVENANT
OP_PUSHCURRENTINPUTINDEX
OP_CHECKSIGFROMSTACKVERIFY
OP_CHECKMULTISIGFROMSTACK
OP_CHECKMULTISIGFROMSTACKVERIFY

Enabled
OP_CAT
OP_SUBSTR
OP_LEFT
OP_RIGHT
OP_INVERT
OP_AND
OP_OR
OP_XOR
OP_MUL
OP_DIV
OP_MOD
OP_LSHIFT
OP_RSHIFT

Simplicity

It can be expressed in a Rust-like language known as SimplicityHL.

It operates independently of the Bitcoin script and functions directly on Simplicity.



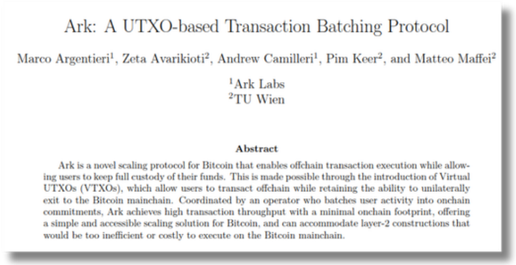
ARK

Ark Protocol

https://ark-protocol.org/

The Ark protocol was initially conceived as an onboarding protocol for the Lightning Network, but was later redesigned to become a standalone L2.

Currently, Ark Labs and Second are well-known implementers.



Ark: A UTXO-based Transaction Batching Protocol

Marco Argentieri[1], Zeta Avarikioti[2], Andrew Camilleri[1], Pim Keer[2], and Matteo Maffei[2]

[1]Ark Labs
[2]TU Wien

Abstract

Ark is a novel scaling protocol for Bitcoin that enables offchain transaction execution while allowing users to keep full custody of their funds. This is made possible through the introduction of Virtual UTXOs (VTXOs), which allow users to transact offchain while retaining the ability to unilaterally exit to the Bitcoin mainchain. Coordinated by an operator who batches user activity into onchain commitments, Ark achieves high transaction throughput with a minimal onchain footprint, offering a simple and accessible scaling solution for Bitcoin, and can accommodate layer-2 constructions that would be too inefficient or costly to execute on the Bitcoin mainchain.

ARK LABS

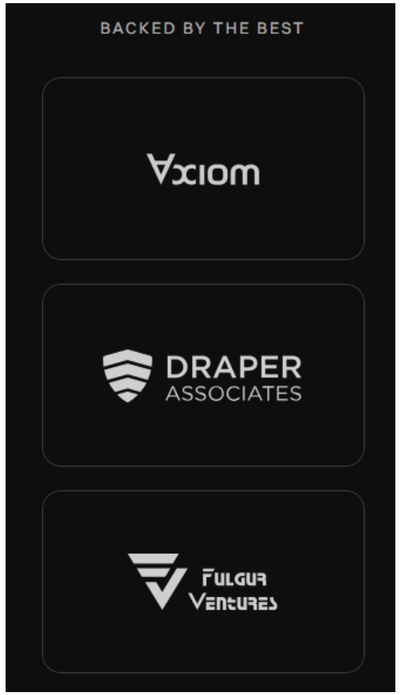
second

Ark Labs

https://arklabs.xyz/
https://arkadeos.com/

Arkade, a subsidiary of Ark Labs, specializes in the development of the Ark implementation of arkd and associated wallets.
The Ark protocol was introduced in 2023, and Ark Labs commenced operations in mid-2024.

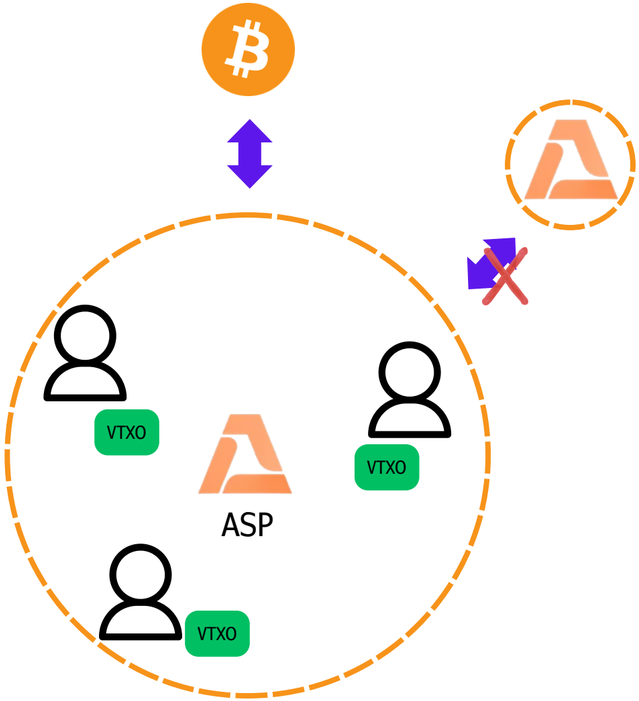
They have been the primary implementers of the Ark protocol and have introduced the Arkade brand as a product.
Its features encompass the integration of libraries and smart contract.
Additionally, it seems to incorporate a TEE (Trusted Execution Environment).

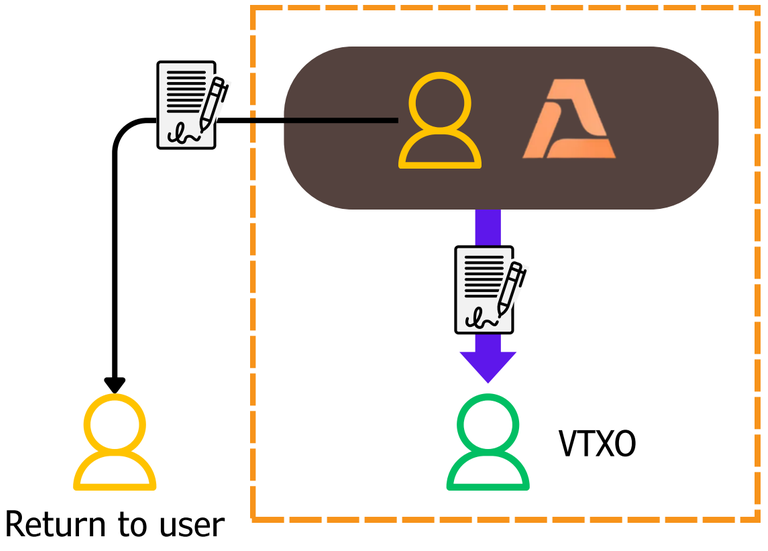


Arkade

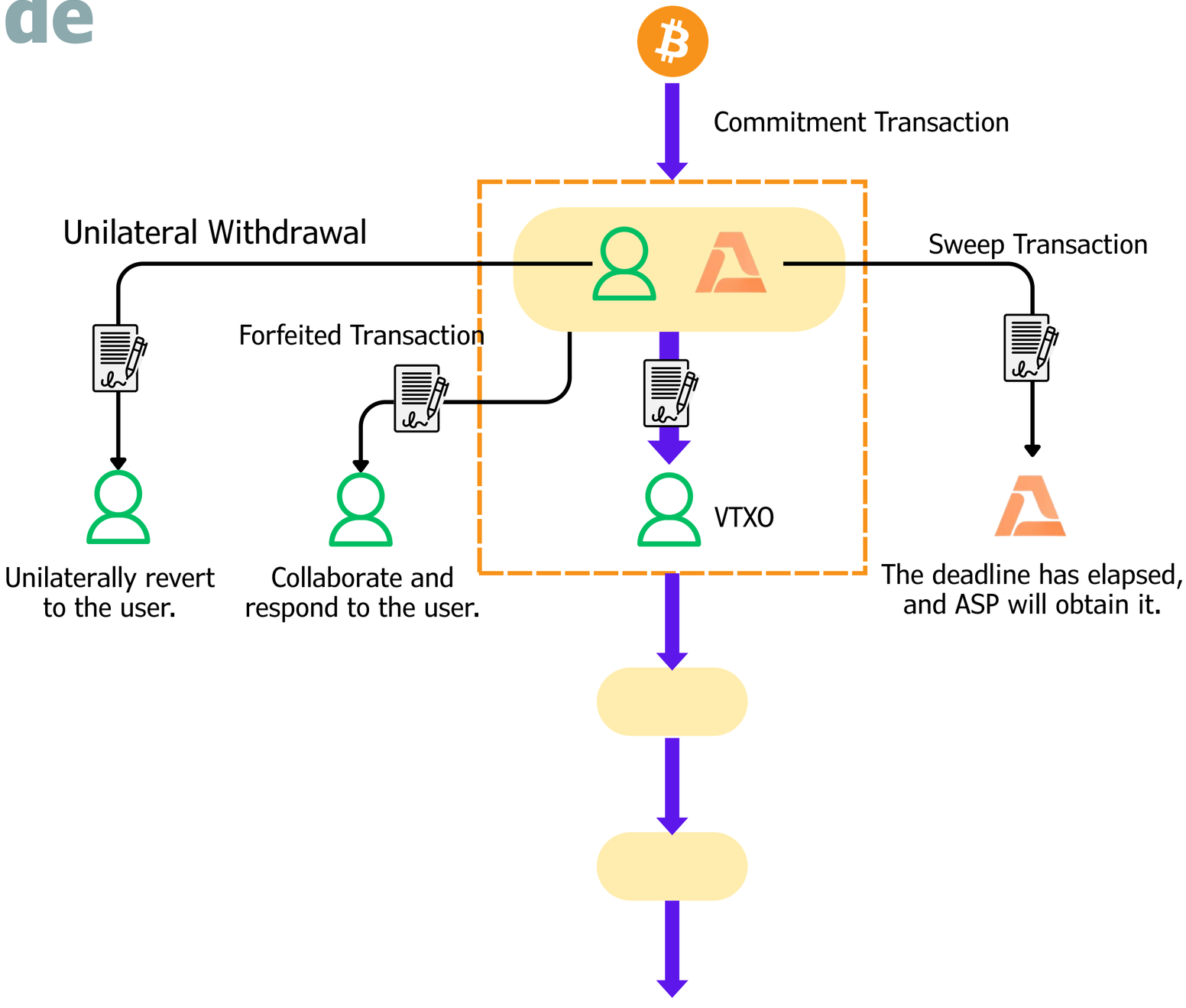
It is operated with clients connected to an ASP (Ark Service Provider).
ASPs do not communicate with each other, so it is not possible to transfer funds to another ASP (at least in the case of Arkade).

The ASP acts as a so-called operator and manages everything.
However, deposits from users to L2 are made via a script managed by the user and ASP.
The script conditions are weighted in favor of the user, so that the ASP cannot send funds without the user's signature, but the user can send funds with their own signature.





Arkade

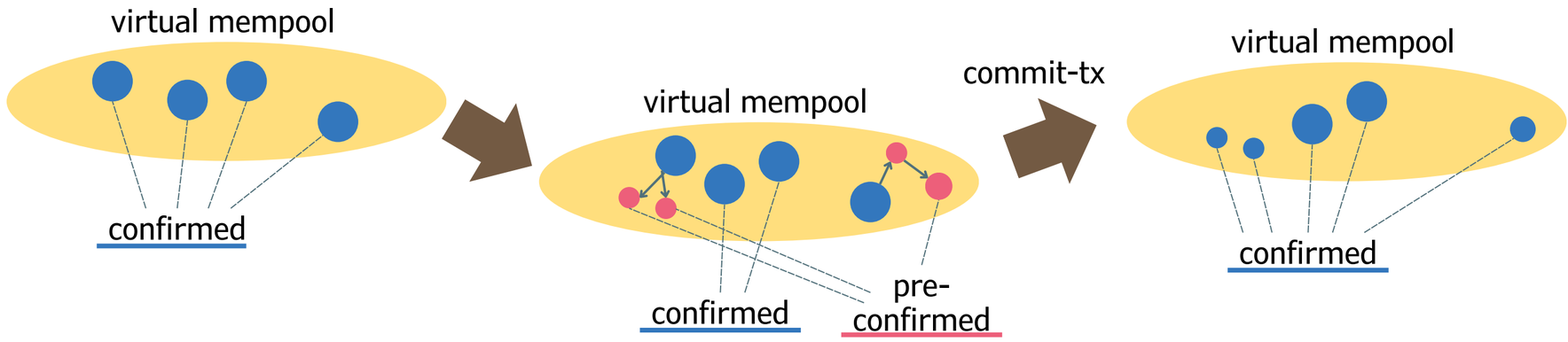


- Commitment Transaction
- Boarding Transaction
- Sweep Transaction
- Forfeited Transaction

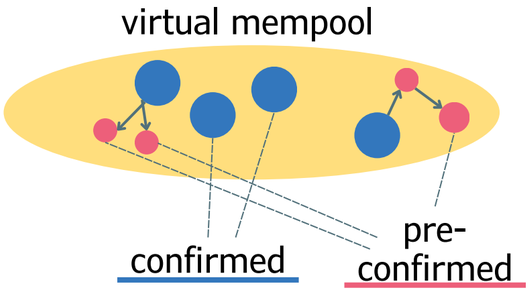
Arkade

A virtual mempool is maintained on the operator's ASP.
Each user possesses a distinct virtual UTXO within the virtual mempool space.
Users transmit and acquire virtual UTXOs.
The virtual UTXO during this period is referred to as a “pre-confirm” state.

The operator periodically records the contents of the virtual mempool onto the blockchain, thereby transitioning the virtual UTXO into a "confirmed" state.



Arkade



“Confirmed” VTXO is deemed “safe” as it is linked to the on-chain.

A "pre-confirmed" VTXO is merely endorsed by both the sender and the ASP administrator.
If a malicious sender and a compromised ASP administrator collaborate, they can engage in "double spending" by signing a VTXO that has already been allocated to another individual.

The motivation for not double-spending is explained as follows:

- The ASP will forfeit its credibility.
- Fraud will be discovered when returning to L1.

Arkade provides a hardware-protected execution environment that cryptographically verifies that the binaries running within it have not been modified.

Second

second https://second.tech/

Second is made up of former Blockstream employees.
This company was also founded in 2024.

A key feature is the ability to pay Lightning Network invoices with Ark payments, as well as eCash and other Ark servers.

It uses a different Ark protocol implementation than Arkade, and is thought to be incompatible.



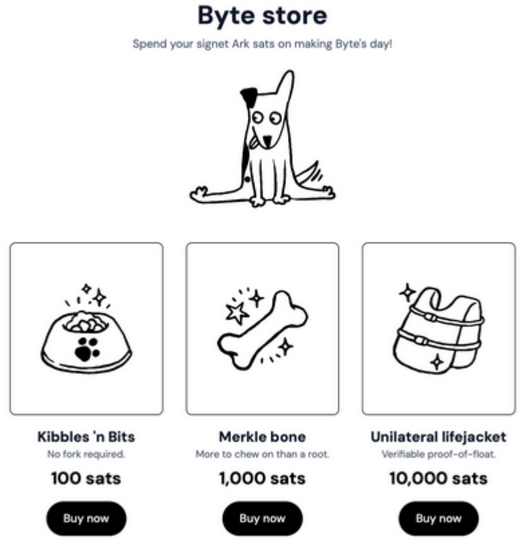
Steven Roose
CEO



Erik De Smedt
CTO



Neil Woodfine
CMO



RGB

RGB

The RGB-WG is one of the working groups within the non-profit organization LNP/BP Association, under the leadership of Dr. Maxim Orlovsky.

LNP/BP Association https://www.lnp-bp.org/

RGB Consortium https://consortium.rgb.tech/

Pandora Prime

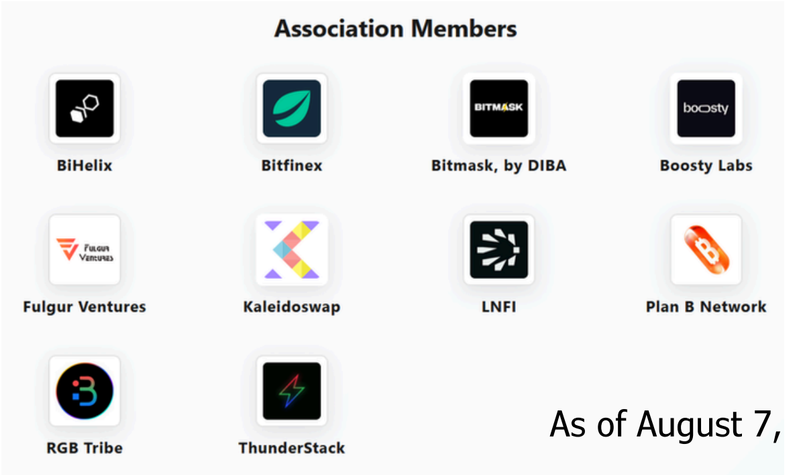


Dr. Maxim Orlovsky
dr-orlovsky · Their Majesty

On July 14, 2025, an entity known as the RGB Protocol Association was unveiled.

RGB Protocol Association https://rgbprotocol.org/

https://rgb.info/



As of August 7, 2025

Recent developments

A significant development occurred in July 2025.

- RGB v0.12 consensus has been released (the application is in its release candidate version).
  - Contracts are now compatible with forthcoming versions.
  - Installing zk-AluVM
  - Aside from that, several modifications have been implemented since version 0.11.
- The RGB Protocol Association has been established.
  - It appears to be a paid membership system.
  - RGB version 0.11.1 has been released.
- Official launch of USDT on RGB protocol.

RGB

RGB aims to establish infrastructure for the implementation of smart contracts on the Bitcoin network.

It is currently operable on Bitcoin L1 and the Lightning Network.

Recently, it appears that it has become feasible to not only issue tokens but also execute smart contracts.

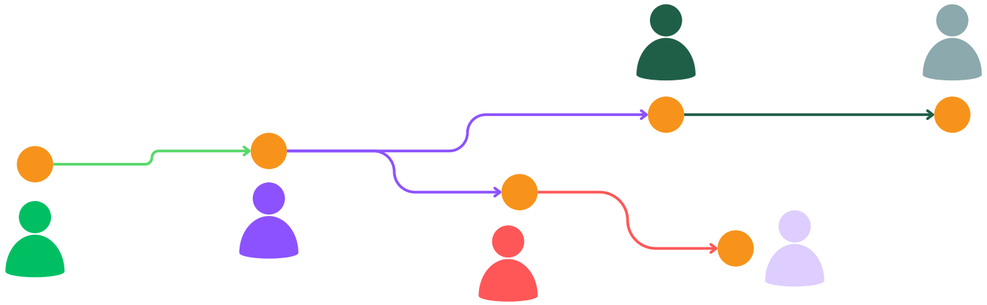


State Management

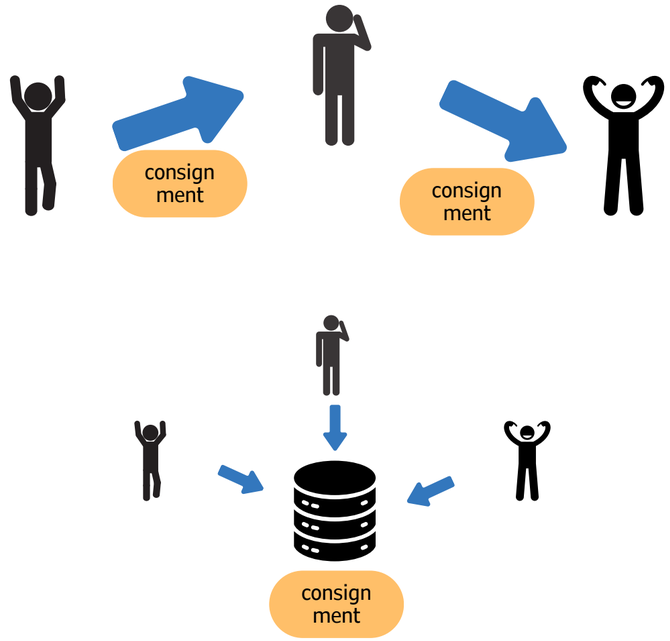
Sidechains and Rollups are techniques for overseeing the complete state.
Developing and implementing a method to verify the accuracy of the state is both challenging and costly. This is evident to all.



An alternative approach is to forgo a comprehensive state, allowing those involved to manage only the segments pertinent to their individual responsibilities.
This is the identical method employed by RGB.



Client-Side Validation



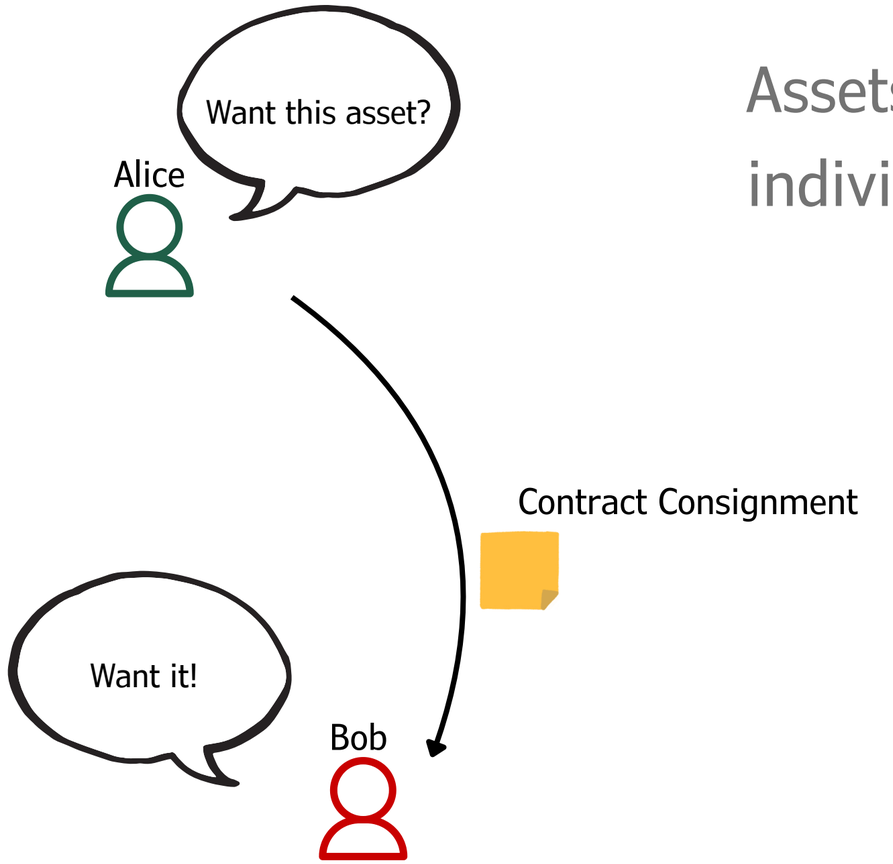
To avoid sharing state, communicate relevant state data to the other party in some way (this data is called “consignment”).

What is more crucial to consider is the accuracy of that state.
As each entity possesses its own state, it must independently verify its accuracy.

This process is referred to as Client-Side Validation (CSV), and RGB employs a technique known as TxO2.

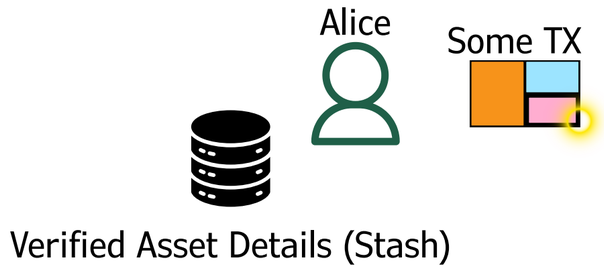
Method	Seal Definition	Seal Closing	Additional Requirements
PkO	Public key value	Transaction output	P2(W)PKH
TxO2	Transaction output	Transaction output	Requires Deterministic Bitcoin Commitments
PkI	Public key value	Transaction input	Taproot-only - Not working with legacy wallets
TxOI	Transaction output	Transaction input	Taproot-only - Not working with legacy wallets

RGB Action Overview



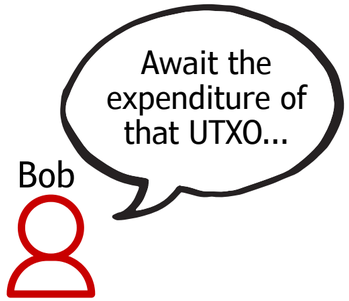
Assets and tokens may only be allocated to individuals who possess the requisite definition.

RGB Action Overview

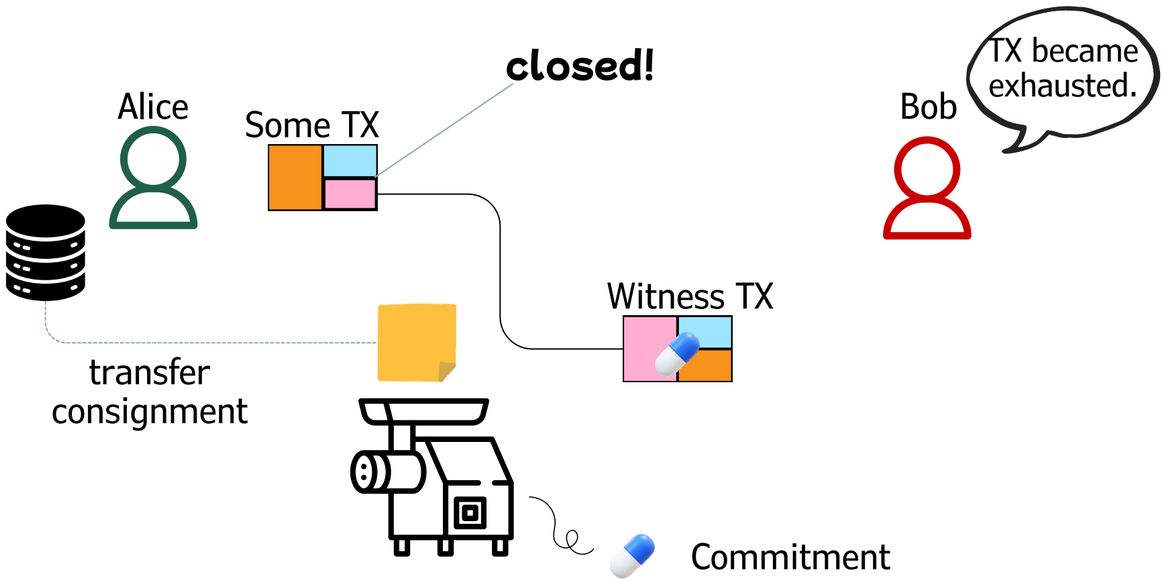


Alice concludes that the UTXO outPoint "references verified data."
This is referred to as the "seal definition."

When this outPoint is spent, it signifies that "an event has transpired."
In this instance, we intend for it to signify "Assets have been transferred to Bob."
Alice will inform Bob about it.



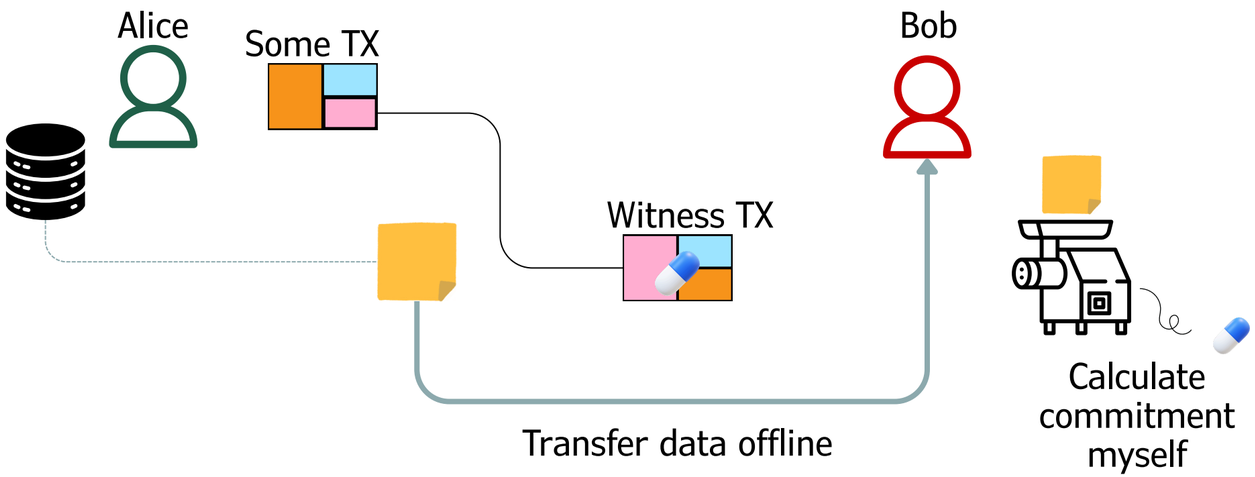
RGB Action Overview



In RGB, when Alice spends the outPoint defined in the seal, it is said that the seal is closed.
It cannot reference other transactions, thus preventing the possibility of double-spending.
It is referred to as a Single-use Seal because, once sealed, it remains securely closed.

In the transactions executed by Alice, asset information is concealed through hash calculations and embedded in Tapscript or OP_RETURN.

RGB Action Overview

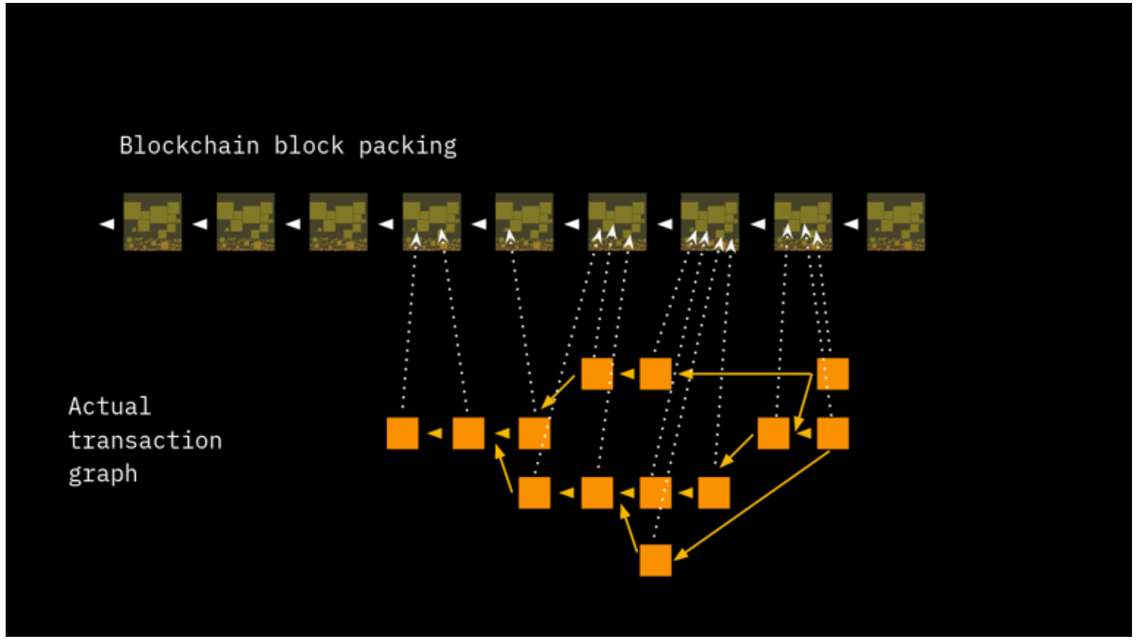


Transfers asset information data from Alice to Bob.
The data is referred to as “Transfer Consignment”.

Bob can independently calculate the consignment from the received data and confirm that the same information is incorporated in the Witness Transaction.

RGB Action Overview

The transfer from Alice to Bob was verified.
Consignment contains the entire history from asset issuance to this point, allowing each client to view the entire history from the roots to the present.



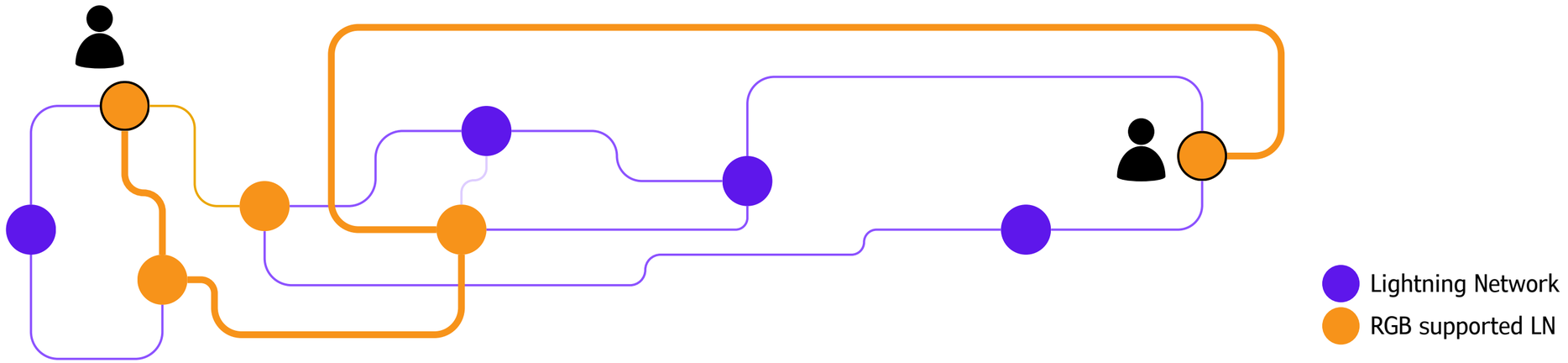
Given that multiple validations must be executed on the client side, this process is referred to as Client-Side Validation.

https://docs.rgb.info/distributed-computing-concepts/client-side-validation

Lightning Network support

- Amending the Commitment Transaction
- Therefore, the channel peers also need RGB-compatible nodes.
- Routing is also possible, but all routes must have the same conditions.

Evidently, the same holds true for Lightning Labs' Taproot Asset.



Arch Network

Arch Network

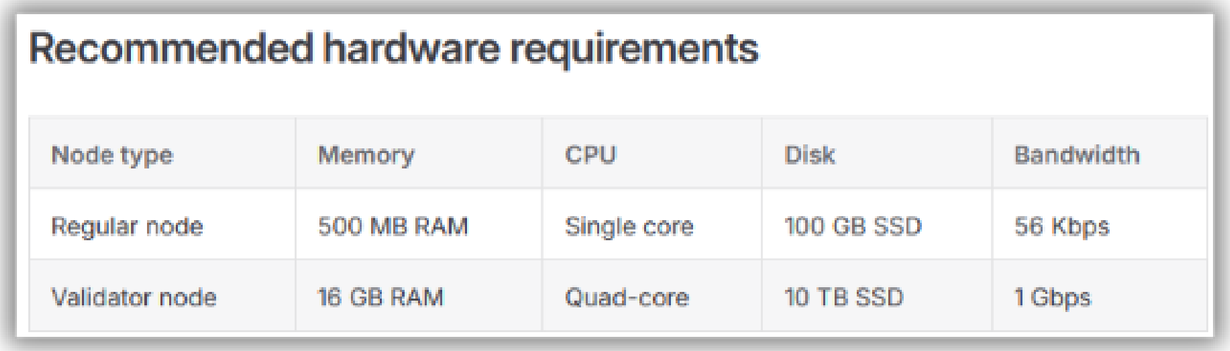


https://www.arch.network/

- No “bridge” needed
  - Deposit required
- ArchVM is built upon eBPF, a virtual machine utilized by Linux and Solana, and enhances it to facilitate direct access to the Bitcoin network for the creation and deployment of transactions.
- To execute a Bitcoin transaction from ArchVM, it is necessary to gather over 51% of the signatures (FROST).

Smart Contracts

- State management is based on the UTXO model.
  - It appears that L1 records the outcome of the transaction.
  - This indicates that processing can persist even across mempools, ensuring that throughput remains unaffected.



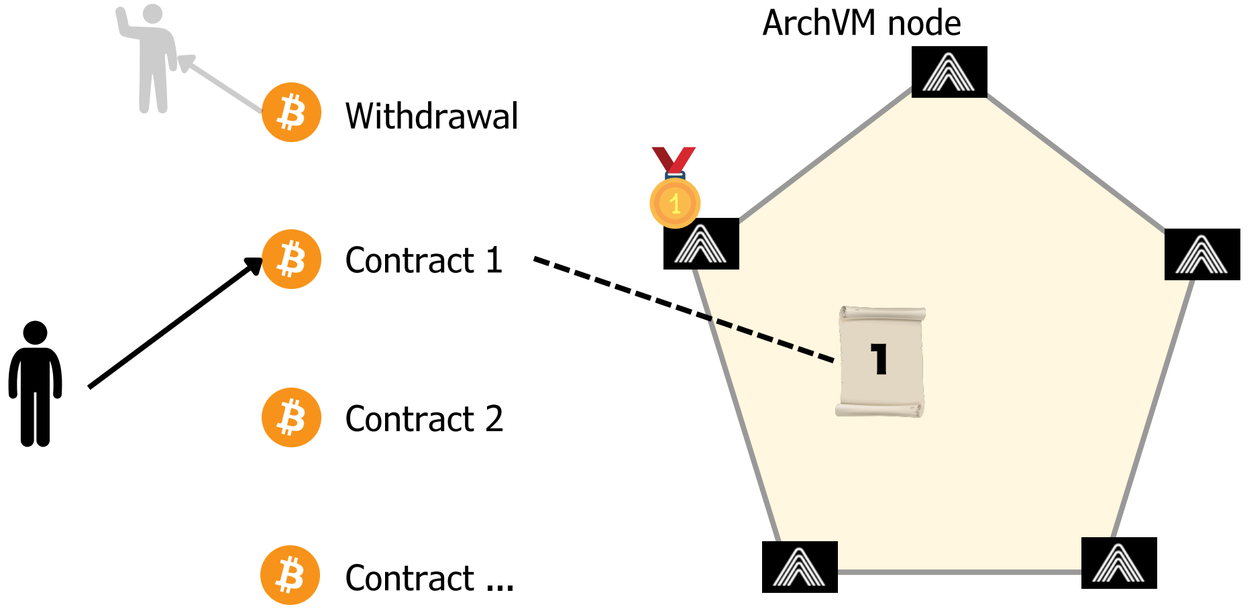
Recommended hardware requirements

Node type	Memory	CPU	Disk	Bandwidth
Regular node	500 MB RAM	Single core	100 GB SSD	56 Kbps
Validator node	16 GB RAM	Quad-core	10 TB SSD	1 Gbps

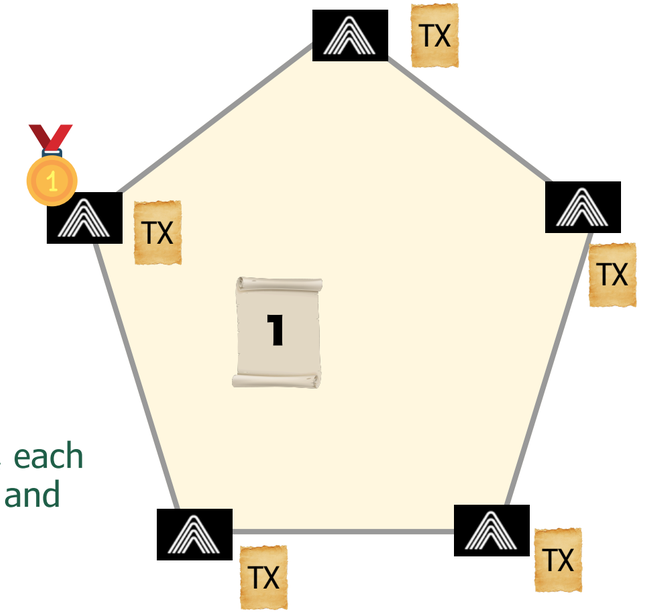
https://book.arch.network/docs/quick-start/requirements

ArchVM

- ArchVM receives and aggregates the signatures of validators using FROST+ROAST, and then broadcasts the transaction to the Bitcoin network.
  - ArchVM executes transactions when an extended system call is invoked on the smart contract or when state-related processing occurs.
  - The ultimate responsibility rests with the leader who publish the transaction.
- Users appear to have the ability to freely place smart contract and execute system calls to withdraw funds in Bitcoin.
  - A smart contract has a Bitcoin address, and users can "execute" it by transferring funds to that address.

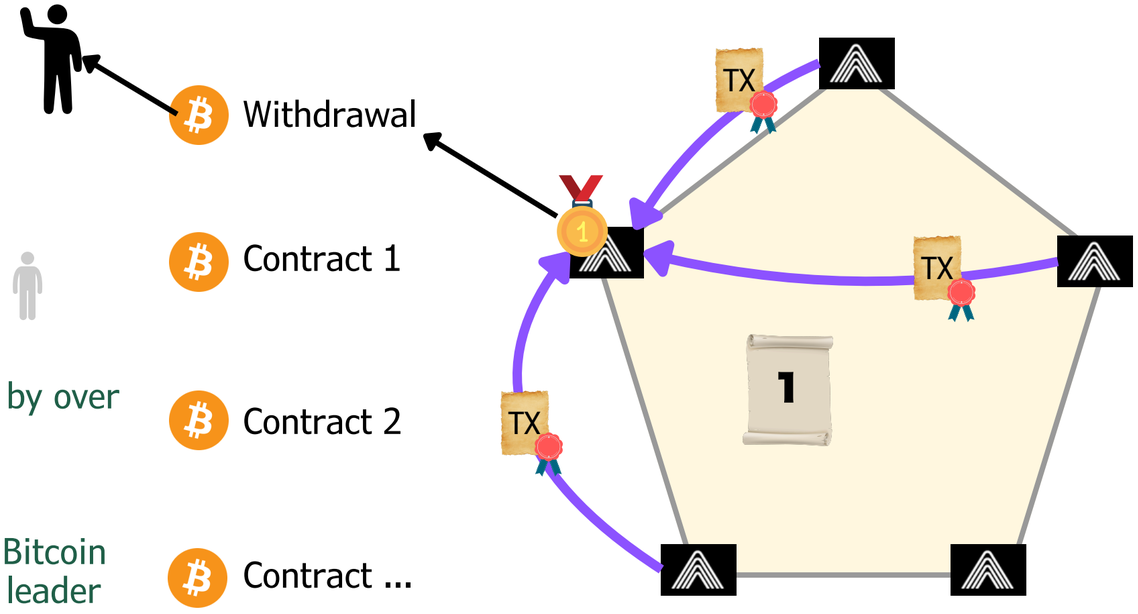


Users transfer funds to the designated Bitcoin address to execute the smart contract.



ArchVM can execute smart contracts and make Bitcoin transactions on its own.

Validators are also ArchVMs, each holding a partial FROST key and able to sign.



A Bitcoin transaction can be broadcasted if it is endorsed by over 51% of validators.

Signature aggregation and transaction broadcast to the Bitcoin network are executed by the leader ArchVM.

FROST

Flexible **R**ound-**O**ptimized **S**chnorr **T**hreshold Signatures

- A Schnorr-based threshold signature protocol aimed at enhancing the efficiency of Bitcoin multisignature transactions.
- Support m-of-n
  - MuSig supports n-of-n
- Aggregation results in a single-key Schnorr signature
  - No need to worry about script length
- Two rounds of signatures
  - Malicious signers impede the process.
    - Enhancing reliability with the ROAST protocol.

ROAST

Robust **A**synchronous **S**chnorr **T**hreshold Signatures

- A procedure that serves as a wrapper for threshold signature schemes such as FROST, aimed at improving reliability in asynchronous networks.
  - Protocol, not signature computation
- A pool of signers is established, and if an individual fails to submit a signature, a combination is generated that excludes that person, allowing the process to proceed.
- Determining who will gather signatures falls outside the purview of ROAST.
  - Arch employs a delegated Proof of Stake (dPoS) consensus mechanism to identify validators.
  - Designate a leader and a deputy leader from the validators to gather signatures.
- The leader presents the transaction for signature to the network, where the validators authenticate and deploy it.
- The leader aggregates and broadcasts the signed transaction.

Babylon

Staking on Babylon

https://babylonlabs.io/

- Users stake by sending Bitcoin to Babylon script address.
  - Staking Transaction: Staked until the specified deadline
  - Unbonding Transaction: Retracted prior to deadline
  - Slashing Transaction: Confiscation due to violation

Timelock Path

```
<StakerPK> OP_CHECKSIGVERIFY  <TimelockBlocks> OP_CHECKSEQUENCEVERIFY
```

Unbonding Path

```
<StakerPk> OP_CHECKSIGVERIFY
<CovenantPk1> OP_CHECKSIG <CovenantPk2> OP_CHECKSIGADD ... <CovenantPkN> OP_CHECKSIGADD
<CovenantThreshold> OP_NUMEQUAL
```

<StakerPK> is user's key

https://docs.babylonlabs.io/guides/overview/babylon_genesis/specifications/bitcoin_staking_scripts/

- A single BTC stake can secure multiple chains and earn rewards from each chain.
- The unbonding period is short (a few days).
- If a user violates the rules, a portion of their stake will be automatically confiscated.

Rewards will be disbursed in Babylon's native token(BABY) instead of BTC.

At worst, the BTC sent by the user will be returned when it expires(Timelock Path).

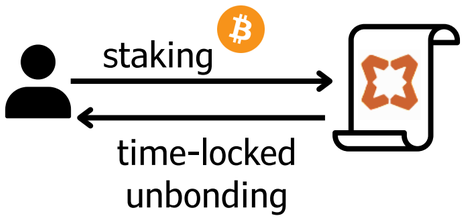
Challenges associated with PoS chains

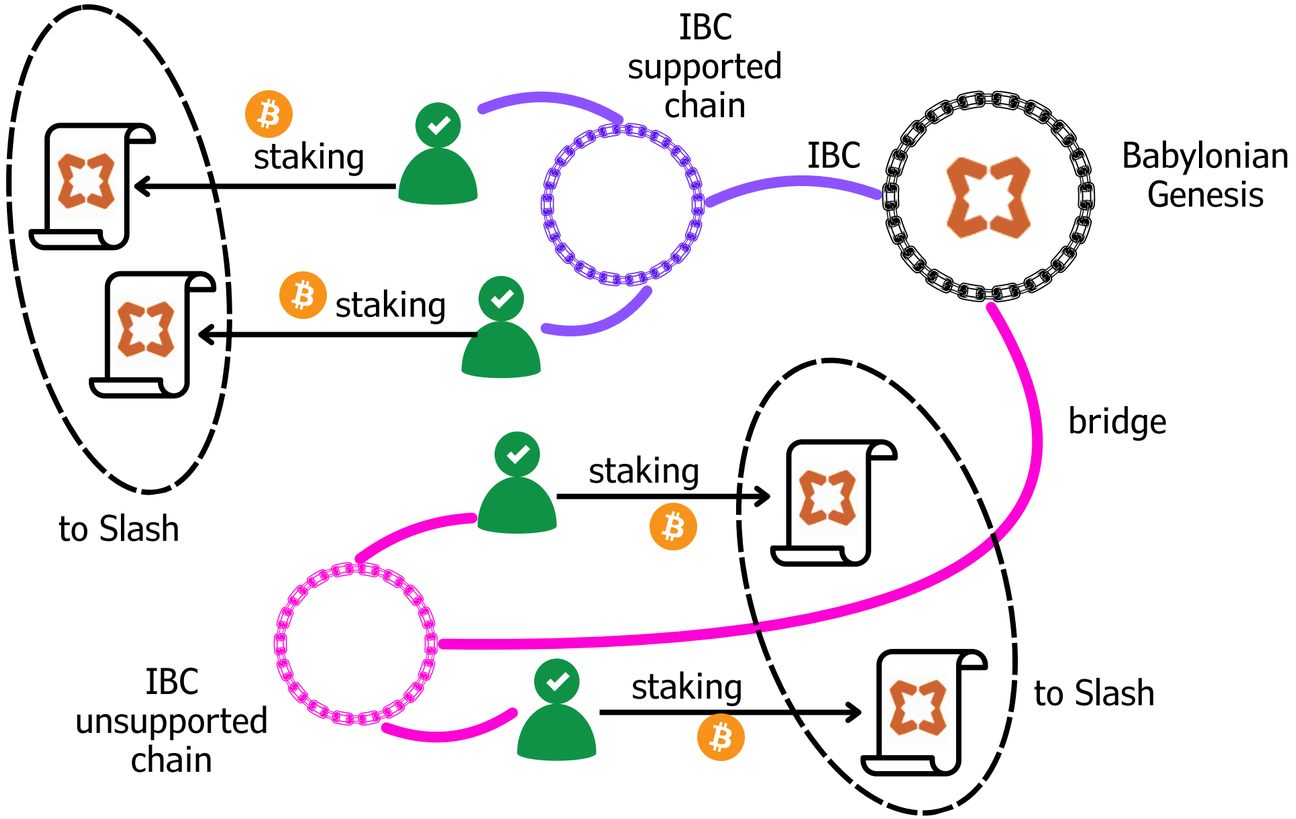
Babylon is a service that enhances the security of Proof of Stake (PoS) chains.

- PoS chains exhibit several security vulnerabilities during their initial launch phase or when the total supply is limited, leading to a diminished market value.
  - Limited validators and insufficient validation
  - The expense associated with becoming a validator is minimal, facilitating the entry of malicious individuals into this role.
  - Even if the attack is discovered, the attacker has little to lose.

Enhancing the security of PoS chains

- Mandate validators to stake to Babylon.
- If a validator engages in dishonest behavior on an external PoS chain, they will face repercussions on the Babylon side as well.
    - Babylon cryptographically verifies fraud reports from external PoS chains and slashes the attacker.





BRC-20 Version 2.0

BRC 2.0

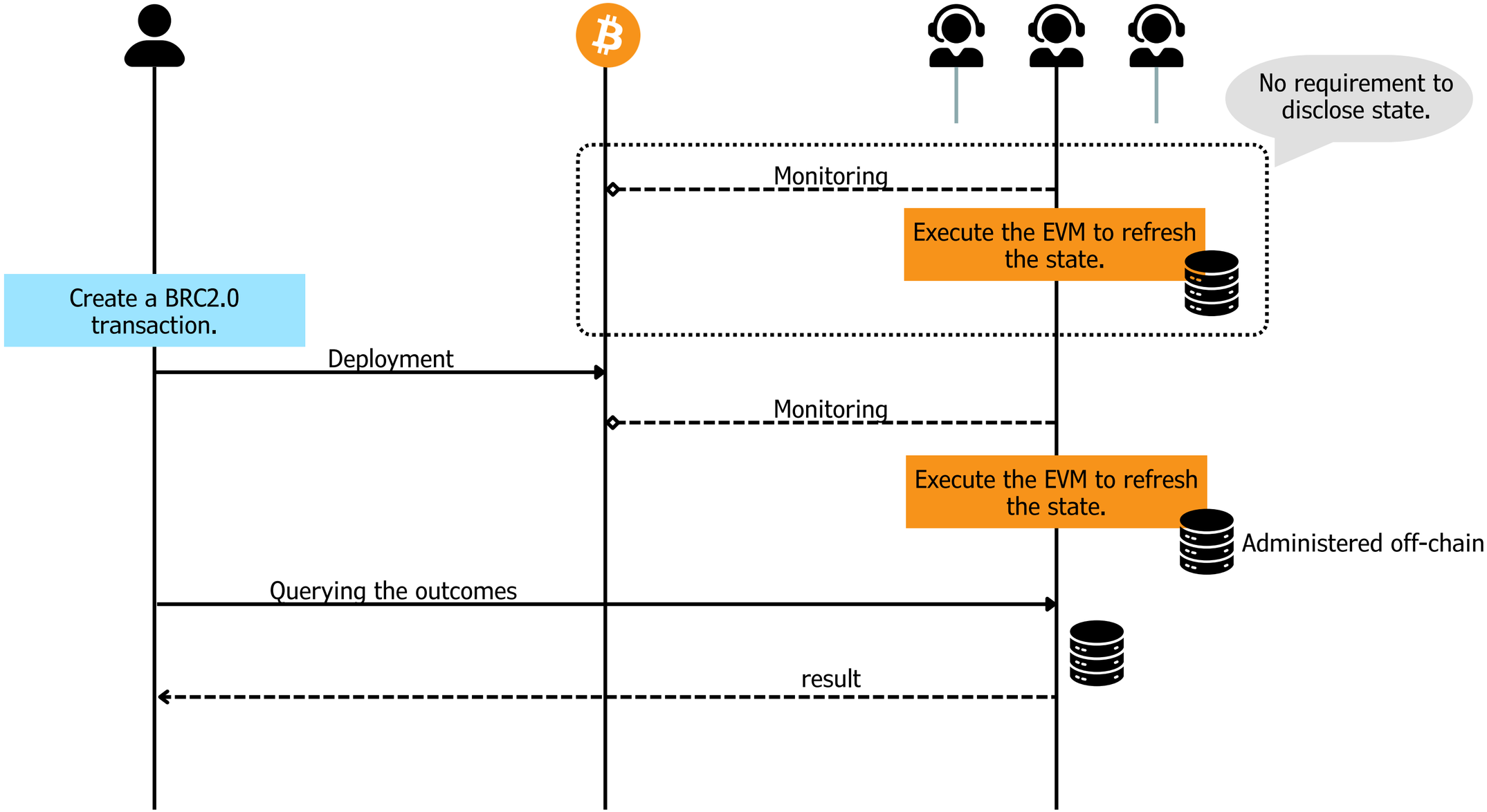


[Best in Slot]

https://bestinslot.xyz/

There is a token called BRC-20 that uses Ordinals' Inscription. v2.0 was released to mainnet on September 1, 2025.

- EVM functions, but L2 does not.
- This is not aimed at improving TPS.
- An application that operates on the EVM is encoded within the Ordinals Inscription data, which the server retrieves from Bitcoin L1 to update the off-chain state.


No requirement to disclose state.
Monitoring
Execute the EVM to refresh the state.
Create a BRC2.0 transaction.
Deployment
Monitoring
Execute the EVM to refresh the state.
Administered off-chain
Querying the outcomes
result

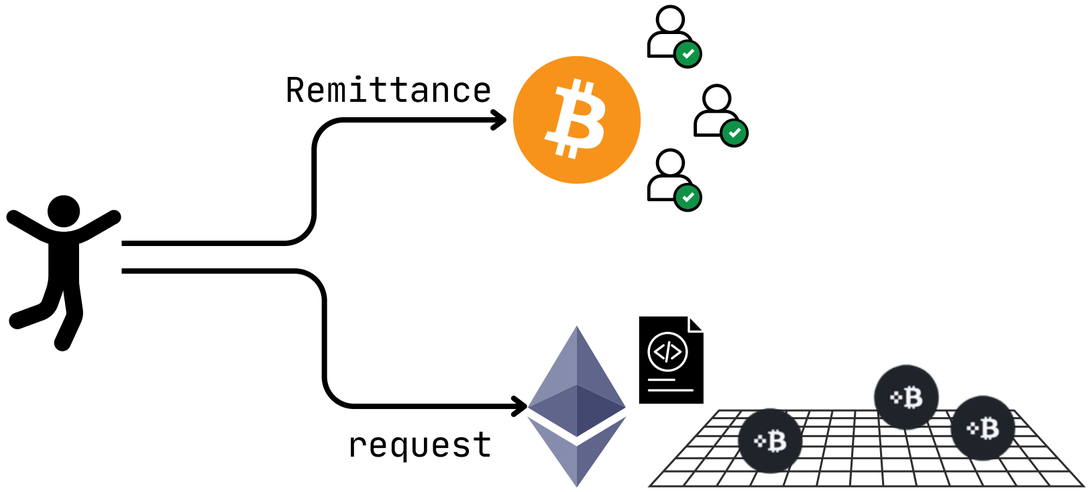
tBTC v2

tBTC v2

THRESHOLD

https://www.threshold.network/

- Threshold Network
  - Keep Network and NuCypher merged
  - The foundational token of the DAO is the T token (Threshold token).
- tBTC is a protocol that serves as a bridge between Bitcoin and EVM chain
  - ERC-20 wrapped token
    - 1 tBTC = 1 BTC
- The user perform smart contract while transferring BTC to the bridge address.



It is not Layer 2; therefore, it does not validate at Bitcoin L1.

Signer

- At present, only nodes involved in key generation possess the capability to sign.
  - GG18 algorithm(ECDSA)
  - Keys are generated by members who have staked a specified quantity of T tokens.
  - Key generation occurs periodically or as required.
    - The algorithm will be switched to FROST, BitVM, etc. once they mature.

Spark

Spark

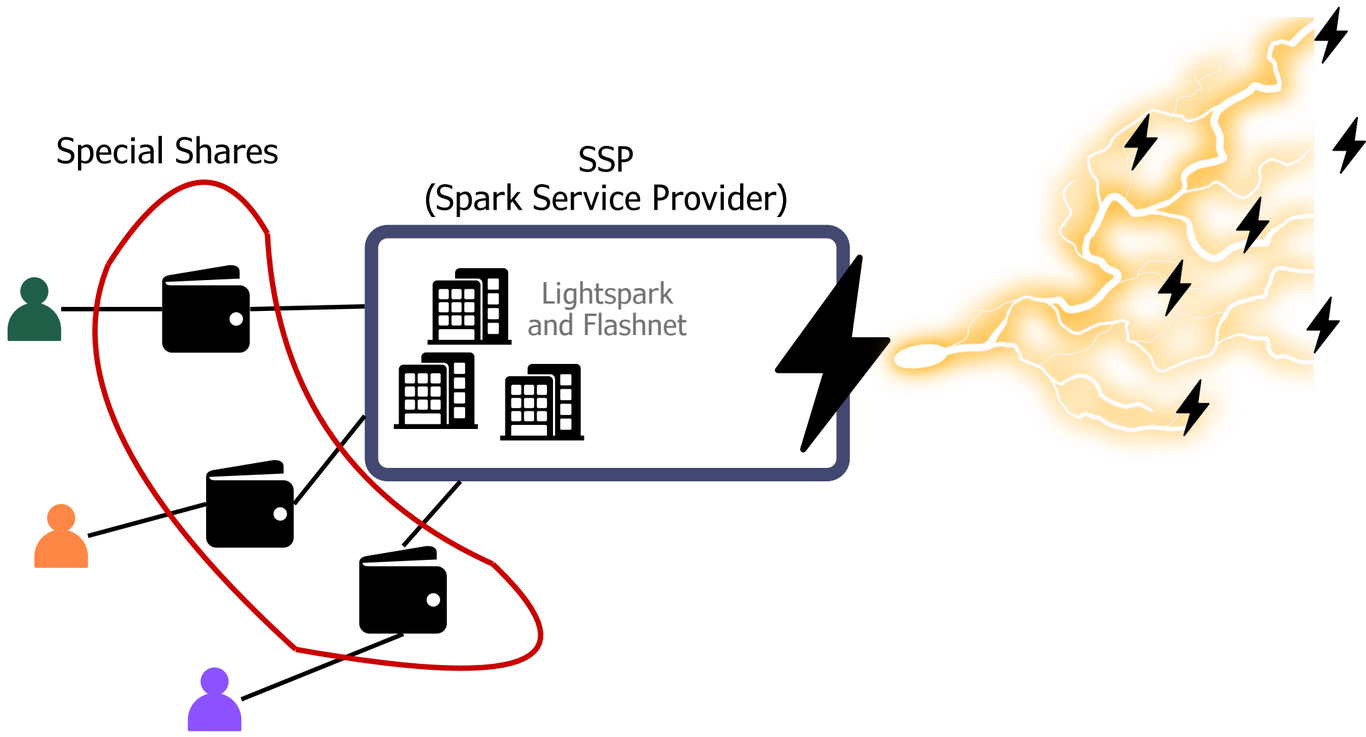


https://www.lightspark.com/

- Operating on mainnet (private beta on October 2025?)
- No VMs, no Rollups, focusing exclusively on payments.
- Tokens can be issued.
  - Supports Taproot Assets, RGB, LRC-20, and additional formats.
- There are no fees associated with L2, while the fees between LN and Spark are 0.25% or 0.15%.

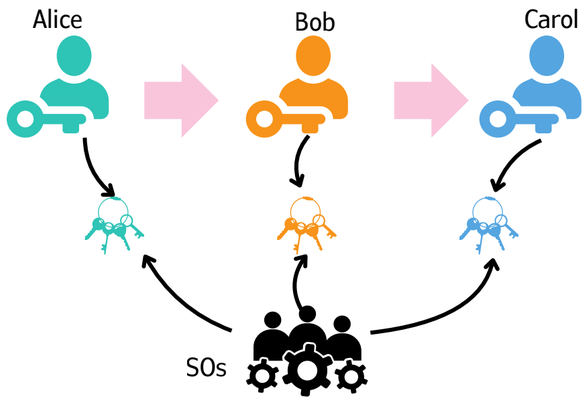
Spark

- L2 of the Federated Statechain approach.
- It appears feasible to withdraw unilaterally.
    - This is the reason it is referred to as "self-custody."



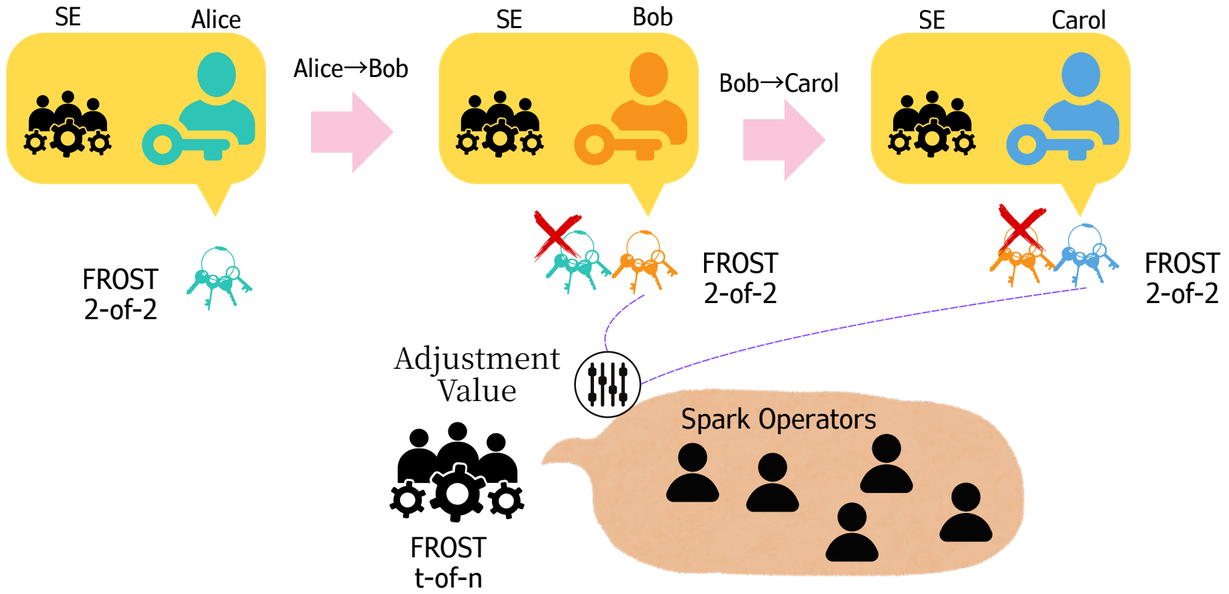
Spark UTXO Delegation

- Federation-style Statechain methodology
  - A system for the delegation and re-delegation of UTXO ownership off-chain.
  - Co-sign transactions utilizing the FROST threshold signature protocol.
  - The members of the Federation are Lightspark and Flashnet.
- Delegating ownership of UTXO on Layer 2 produces an effect equivalent to transferring funds.
  - Integrating FROST with multisig facilitates adaptable operator combinations while maintaining the necessity of user signatures.



Spark UTXO Delegation

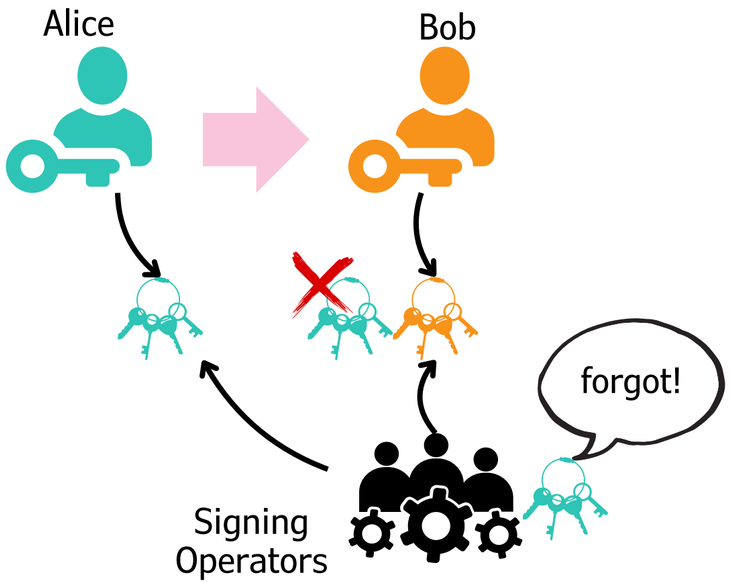
- Operators create t-of-n threshold signing keys utilizing FROST.
- Users and operators (Statechain Entities, SE) also create 2-of-2 threshold signing keys using FROST.
- When signing, each individual presents their own key, and if the number collected exceeds the threshold, they are able to sign.
- If the owner of a UTXO changes, adjusting the operator's FROST key enables the UTXO to be spent using the new owner's signature.



Trust Model

- The operator is required to eliminate the key set of the prior UTXO owner, thereby also creating a potential for collusion.
- They do issue revoked certificates; however, due to the potential for forgery, it appears they have ultimately opted for a "unilateral exit."

https://docs.spark.money/learn/trust-model



Drivechain

LayerTwo Labs

https://www.drivechain.info/



Paul Sztorc
@Truthcoin

- Drivechain is proposed by Paul Sztorc, the CEO.
- business
  - Drivechain advancement and dissemination
  - Sidechain Design
  - Prediction markets, the revival of Namecoin, etc...
- $3 million in funding received in December 2022
- There appears to be a growing interest in addressing the Bitcoin situation.
  - The definitive scaling solution that will guarantee Bitcoin's future sustainability, incorporate all innovations, and accommodate the varied needs of its users.
    - User-selectable consensus
    - Permissionless Innovation
      - Anyone can try out new features and rulesets.

Drivechain

- A proposal to enhance functionality via sidechains while minimizing significant alterations to Bitcoin L1.
- Proposed as BIP-300 (2017) / BIP-301 (2019).
  - Both proposals are soft forks and are presently in Draft.
- The discussion seems to be in progress.

BIP-300: Hashrate Escrows

- Consider it as a component of a bridge.
- peg-in
  - Prepare a formatted script.
  - When a user transfers funds to that script address, a token is issued on the sidechain.
  - It will simply be locked, preventing the operator from accessing it.
- peg-out
  - When funds are burned on the sidechain, a peg-out request is issued.
  - Bitcoin miners vote on peg-out requests by embedding data in coinbase transactions.
  - The voting period spans approximately three months, and approval is granted only when more than 51% of votes are cast.
  - After approval, the peg-out amount will be returned to the user within the locked funds.

BIP-300: QA

https://drivechain.info/faq/index.html

- Peg-in only locks up funds and operators cannot use them.
- Peg-out may only occur within the peg-in amount.
- Isn't it taking an excessive amount of time to peg out?
  - The exchange will serve as an intermediary, allowing users to reduce the duration by utilizing HTLC with the exchange (FAQ).

BIP-301: Blind Merged Mining

- Merged mining is a process in which miners validate blocks on the sidechain.
  - Rootstock is also a merged mining system; however, the methodology differs.
- The miner incorporates the sidechain block hash into the coinbase transaction. Upon approval of that block, the sidechain block receives approval as well.
- Sidechain miners obtain rewards from the sidechain, while Bitcoin miners receive rewards from the sidechain miners.



BIP-301: Blind Merged Mining

1. The sidechain approver creates a sidechain block and sends a transaction to the Bitcoin side saying, "Include this value in the coinbase transaction and give a reward to the miner who approved it."
2. Bitcoin miners familiar with BIP-301 analyze the transaction and generate a coinbase transaction for mining purposes.
3. Once the miner's block is validated by Bitcoin, the sidechain similarly regards the block as confirmed.
4. Sidechain miners compensate the Bitcoin miners.

Drivechain

- permissionless innovation
  - New features may be implemented without authorization.
  - This would remove the incentive to transition to an alternative chain.
  - Users may choose to opt in.
  - If issues arise, it can be deactivated through a soft fork.
- The value is 1:1 with Bitcoin

THANK YOU