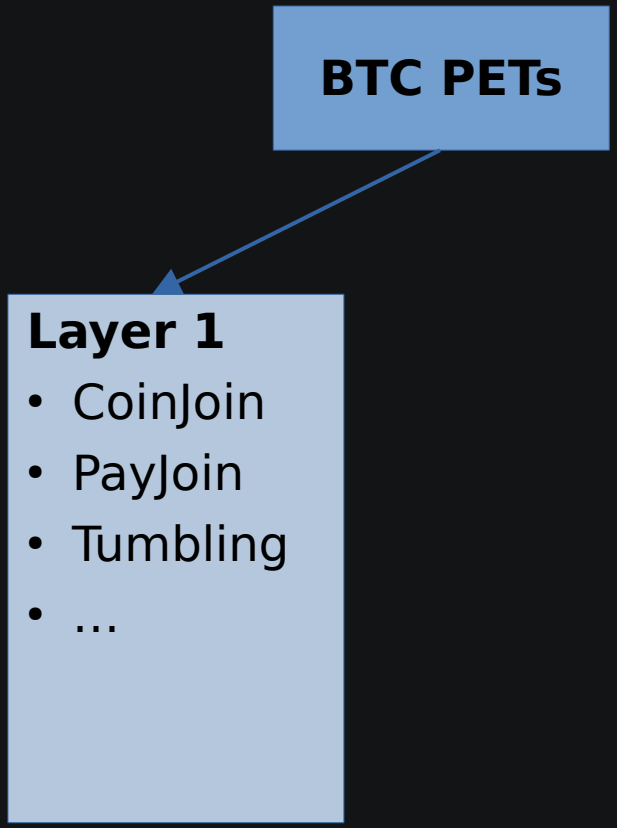
Improving Bitcoin’s privacy with Federated E-Cash Mints

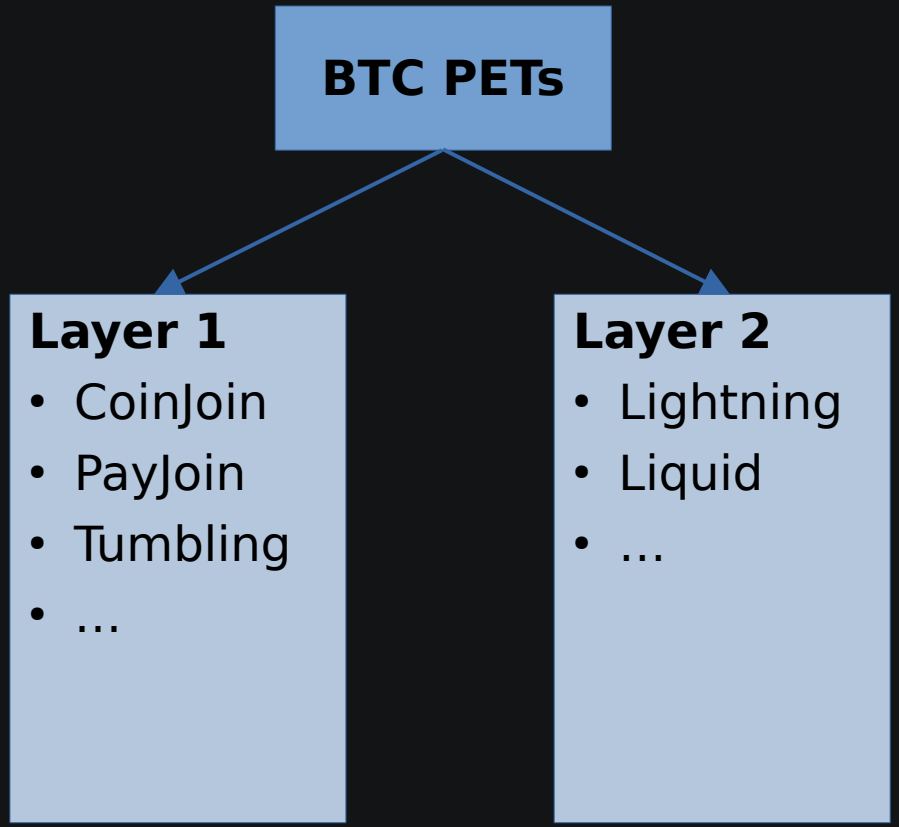
Twitter: @EricSirion github.com/fedimint

Blockstream

Bitcoin PETs Today

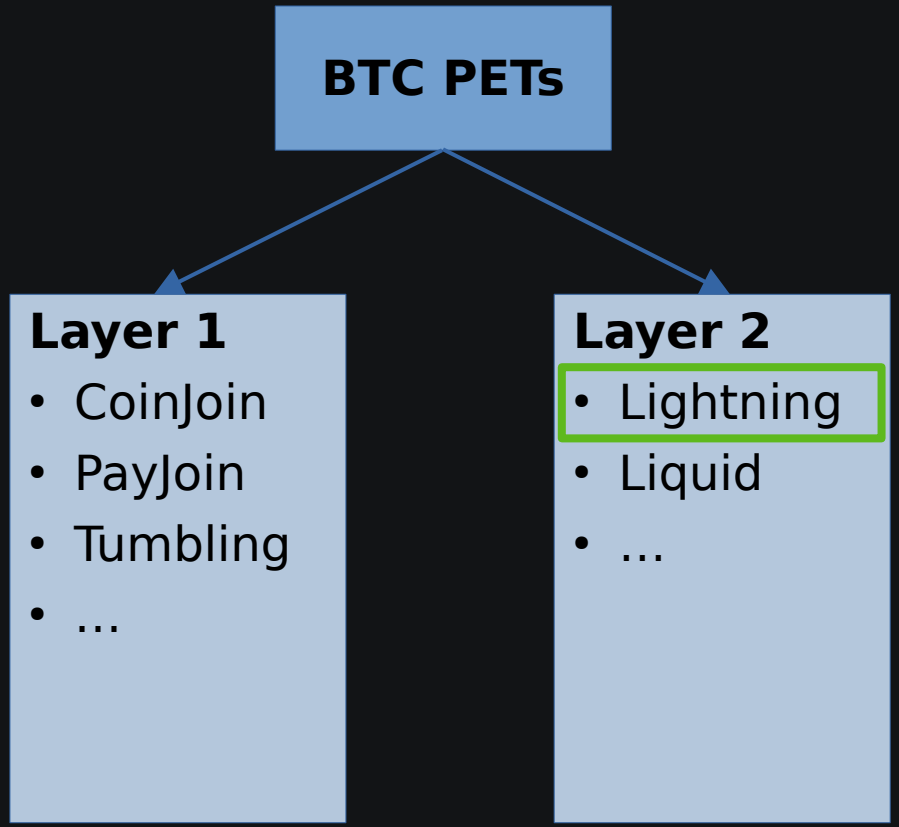


Bitcoin PETs Today



Blockstream

Bitcoin PETs Today

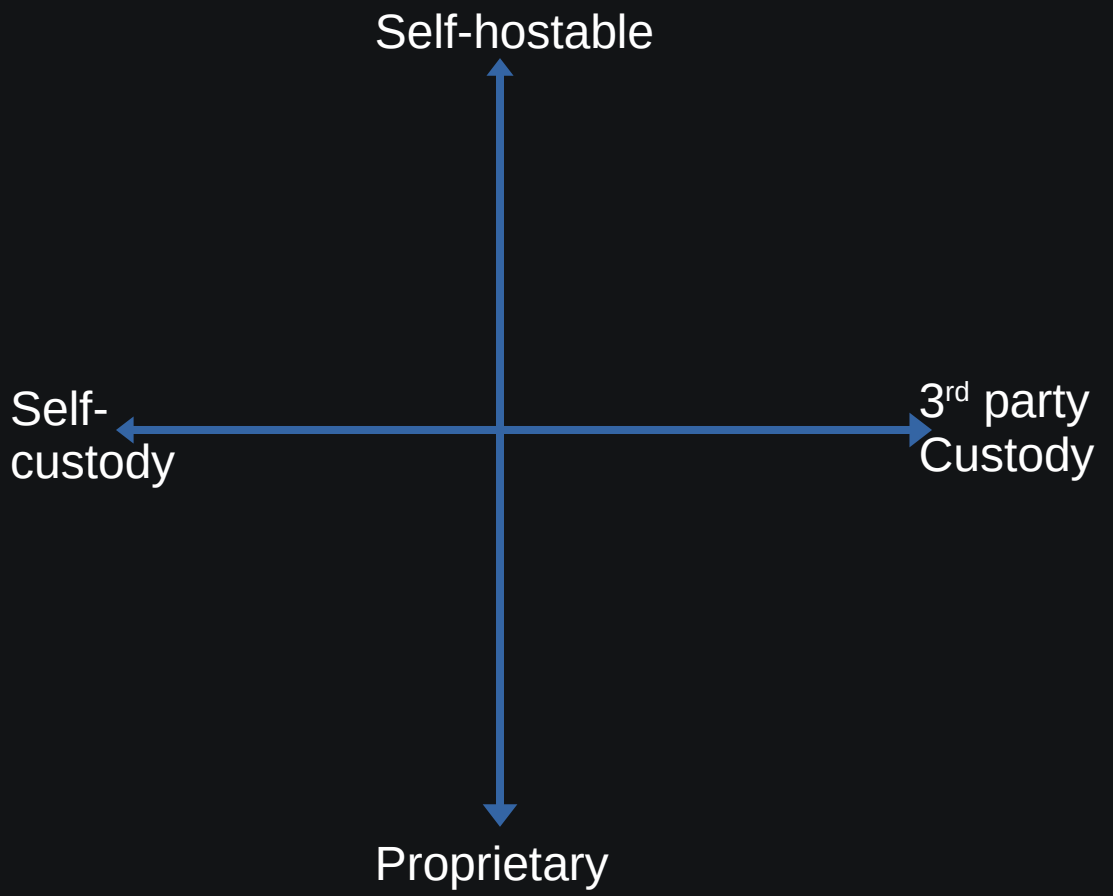


Blockstream

Lightning Wallets

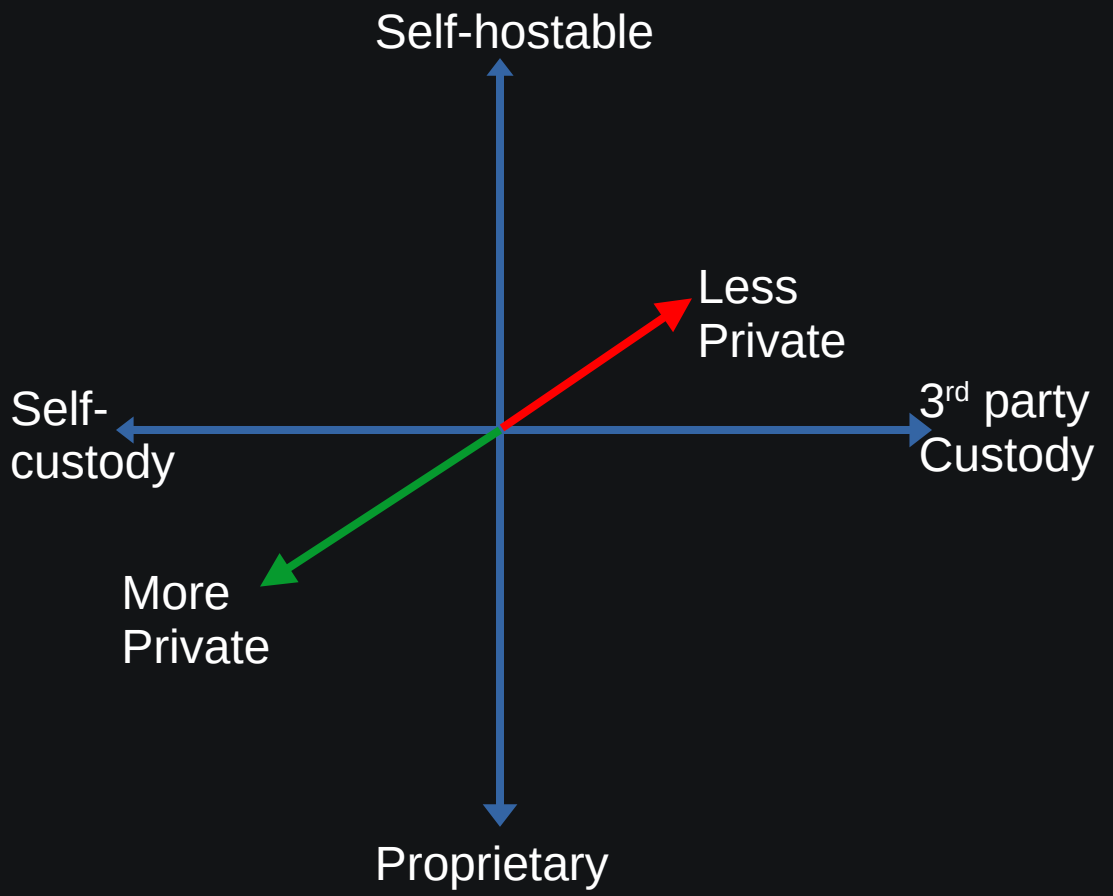
Blockstream

Lightning Wallets



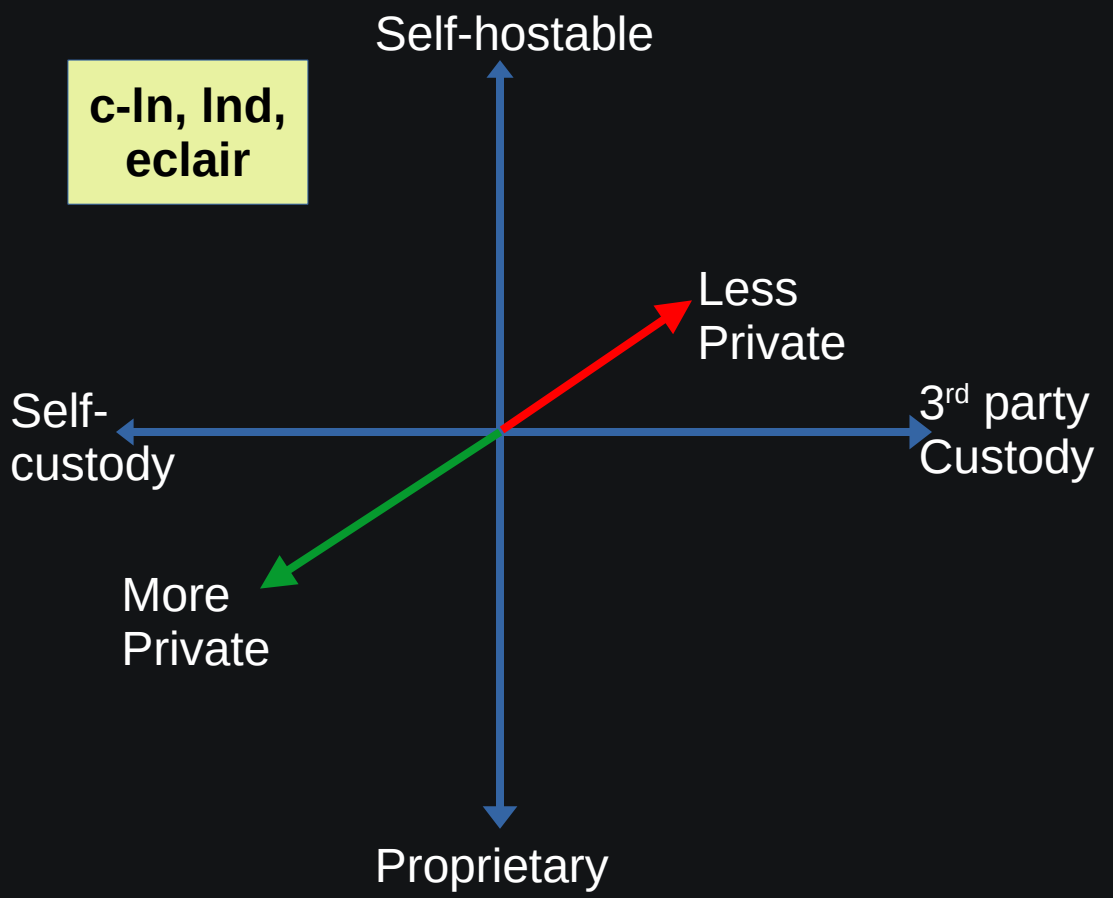
Blockstream

Lightning Wallets



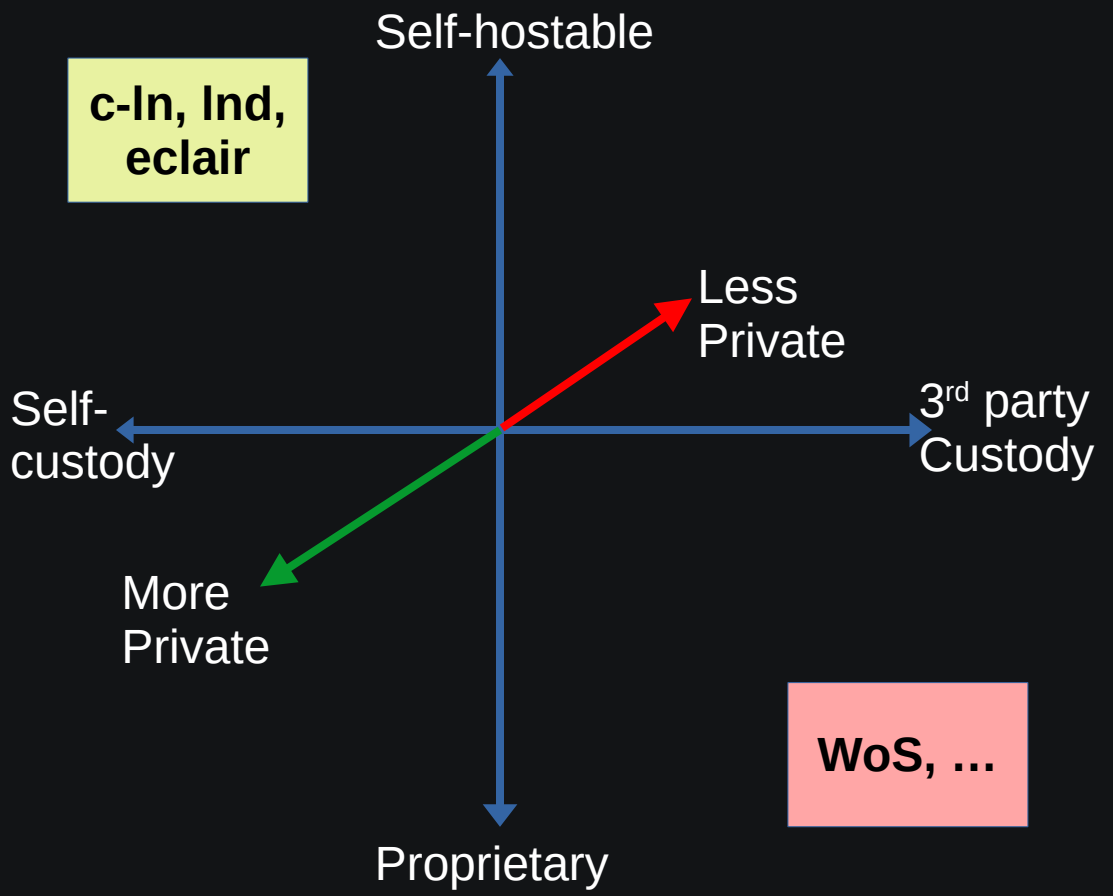
Blockstream

Lightning Wallets

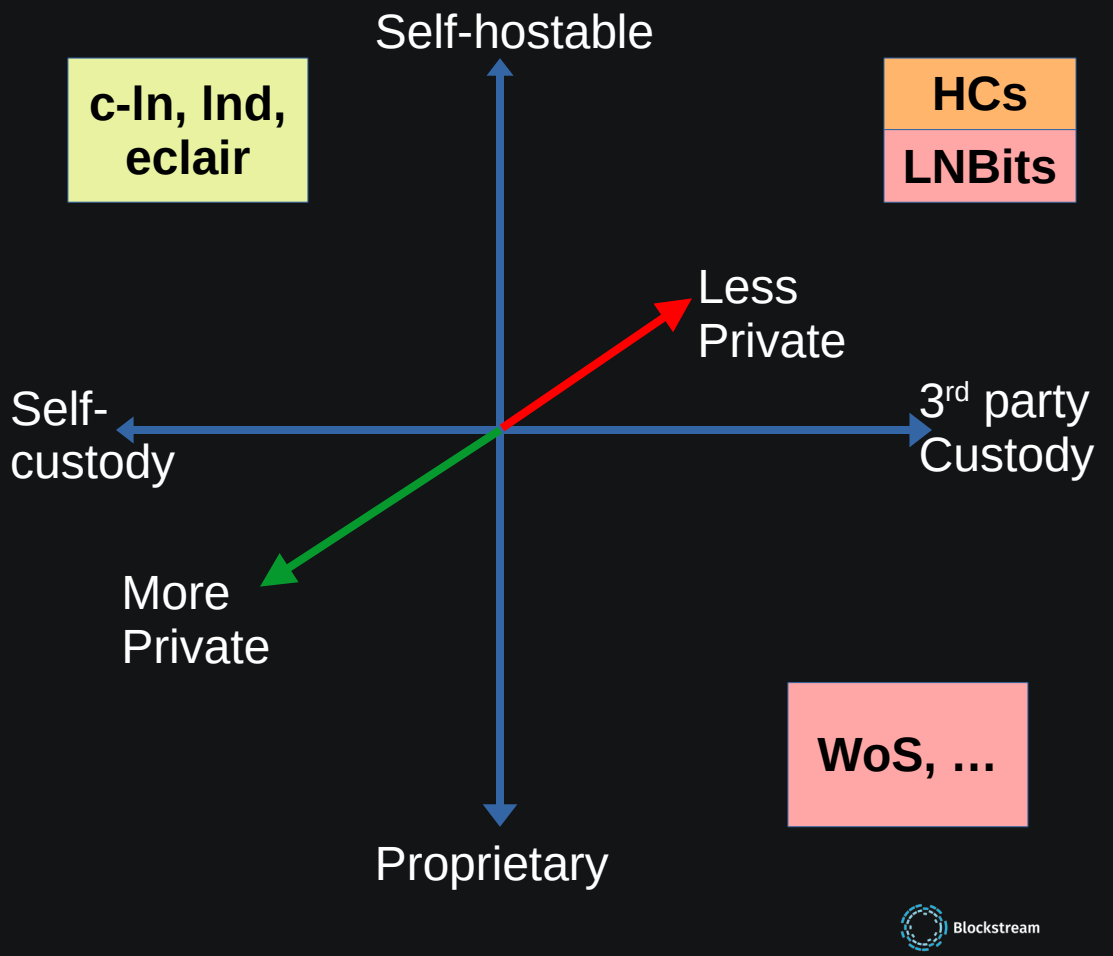


Blockstream

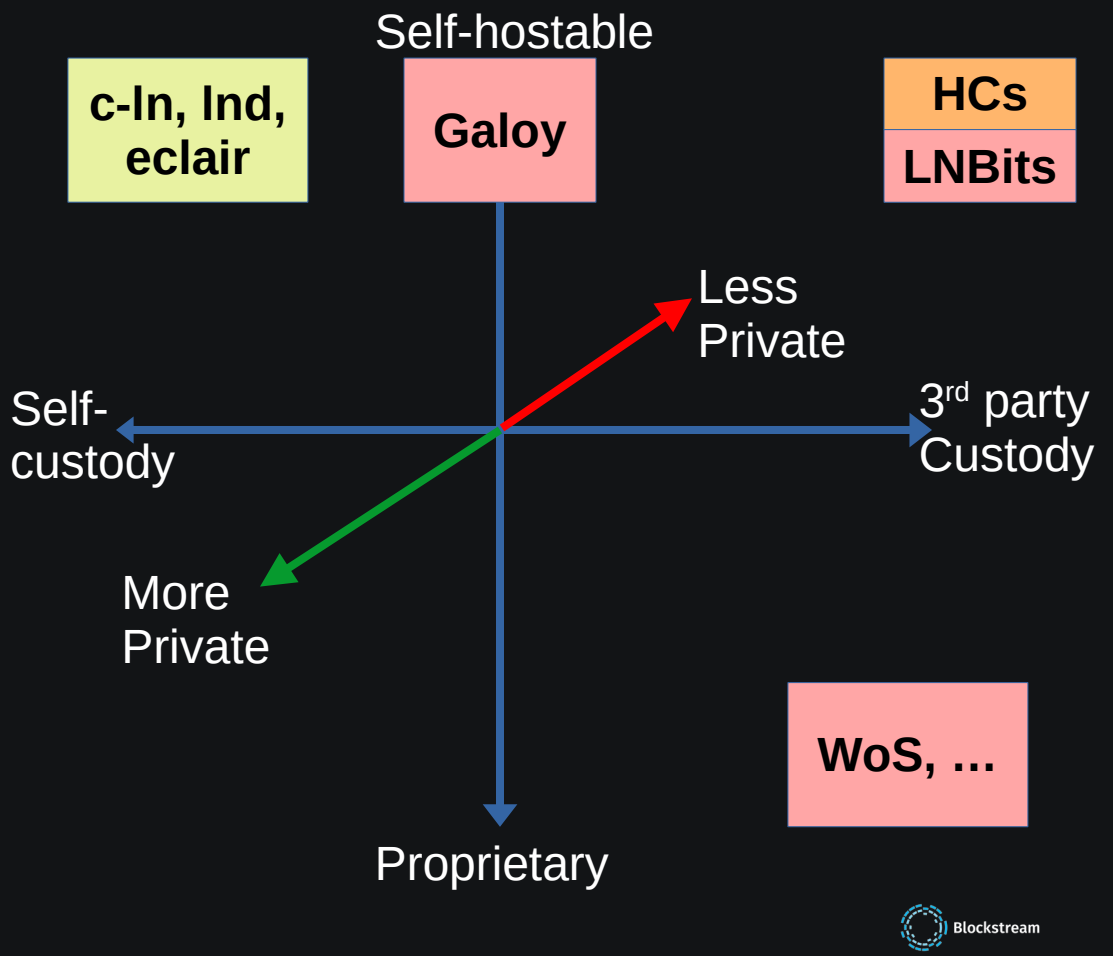
Lightning Wallets



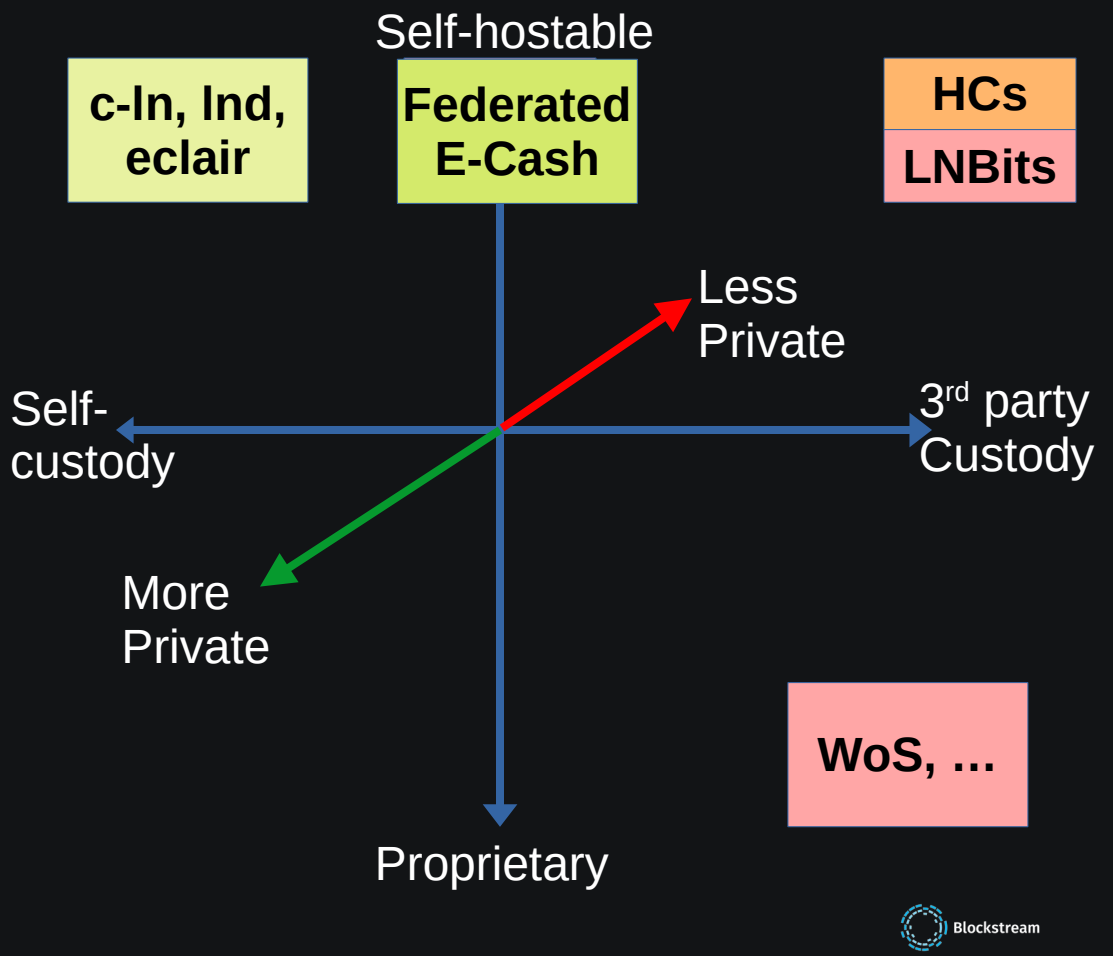
Lightning Wallets



Lightning Wallets



Lightning Wallets

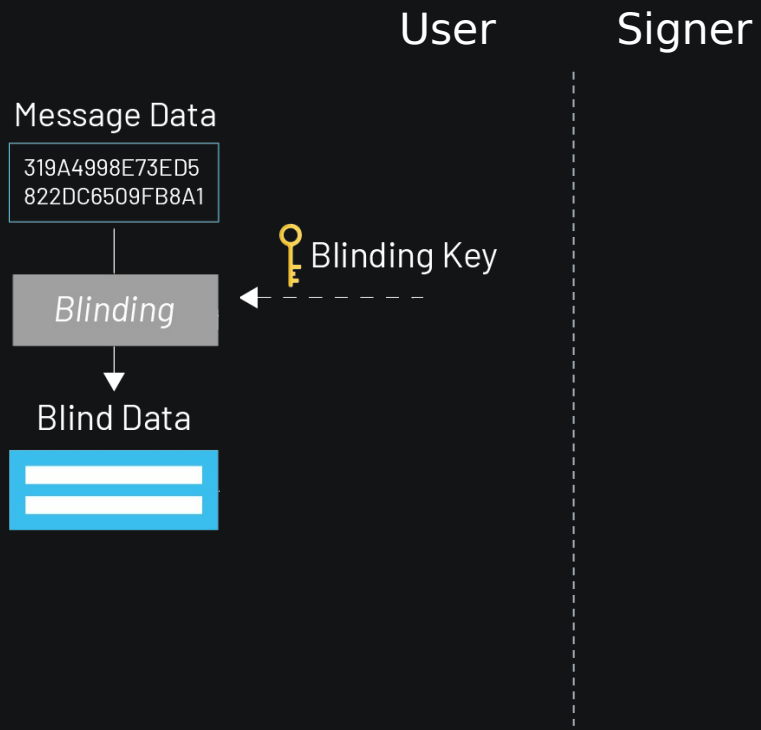


Federated E-Cash

Blockstream

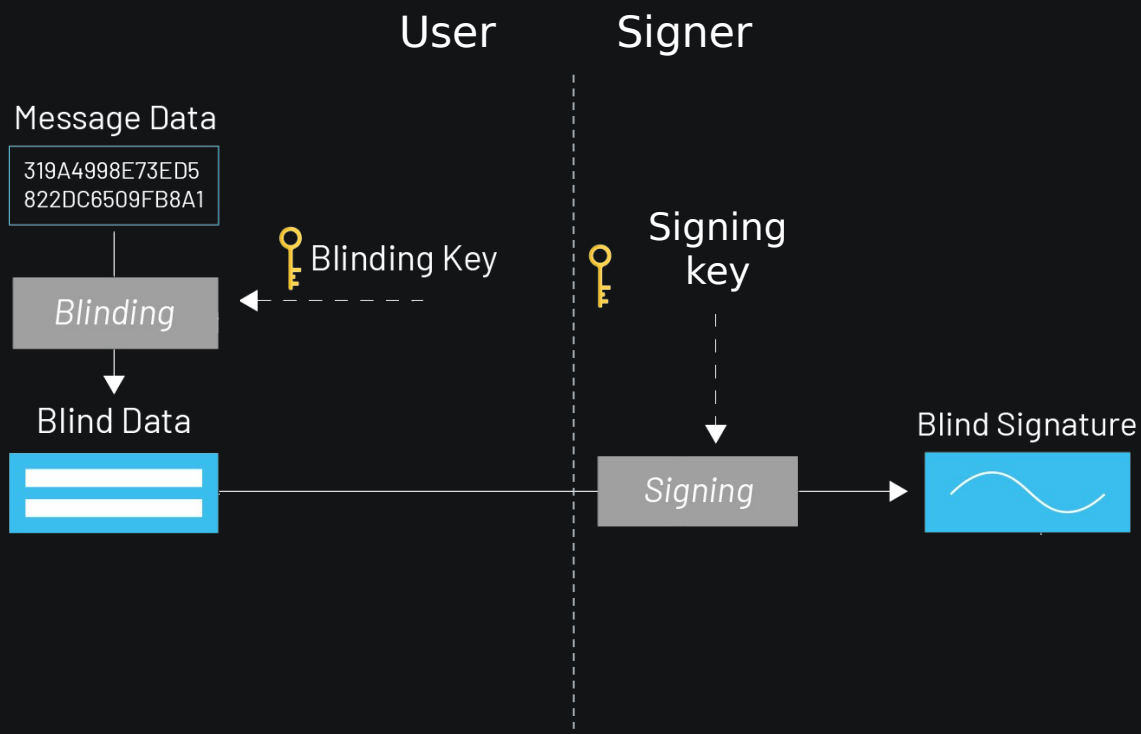
1 Traditional Chaumian E-Cash

Blind Signatures



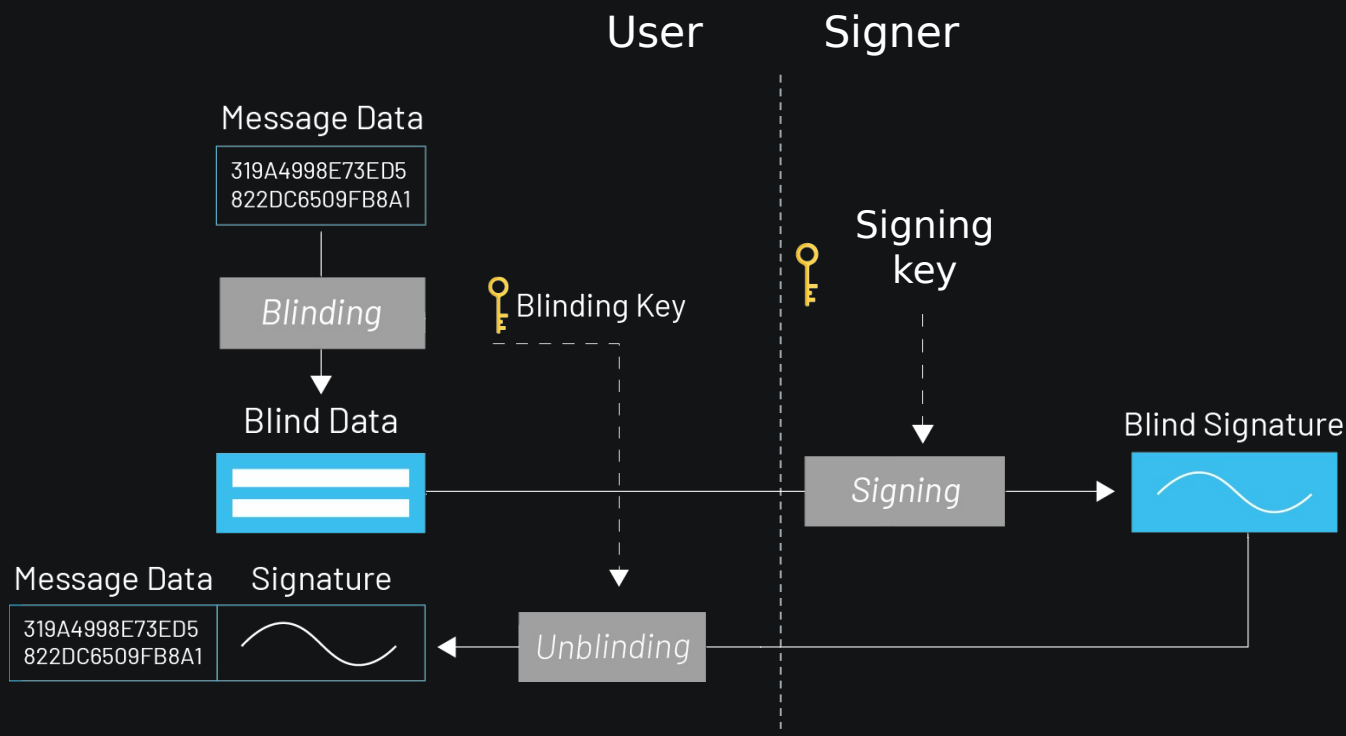
Blockstream

Blind Signatures



Blockstream

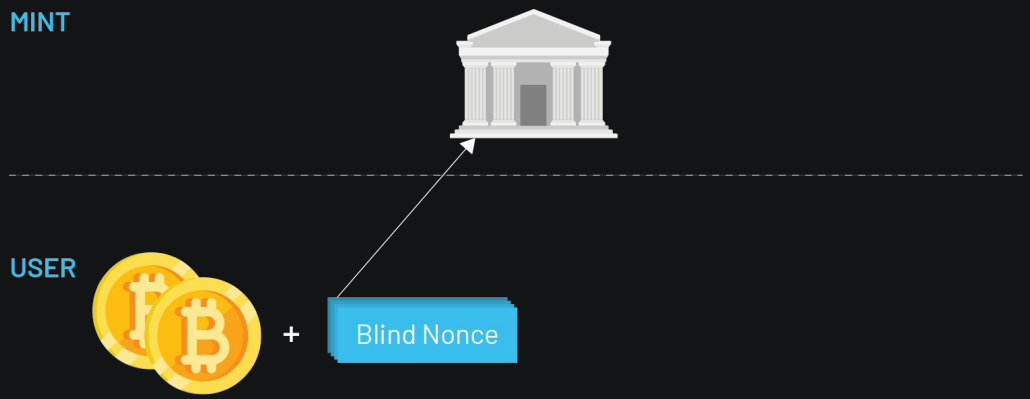
Blind Signatures



Blockstream

Traditional E-Cash **Issuance**

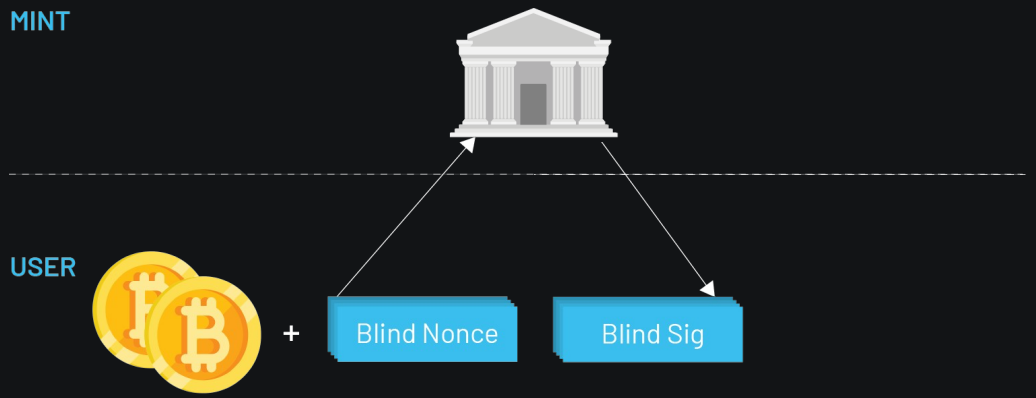
1. User Sends BTC + Blind Nonce to Mint



Blockstream

Traditional E-Cash **Issuance**

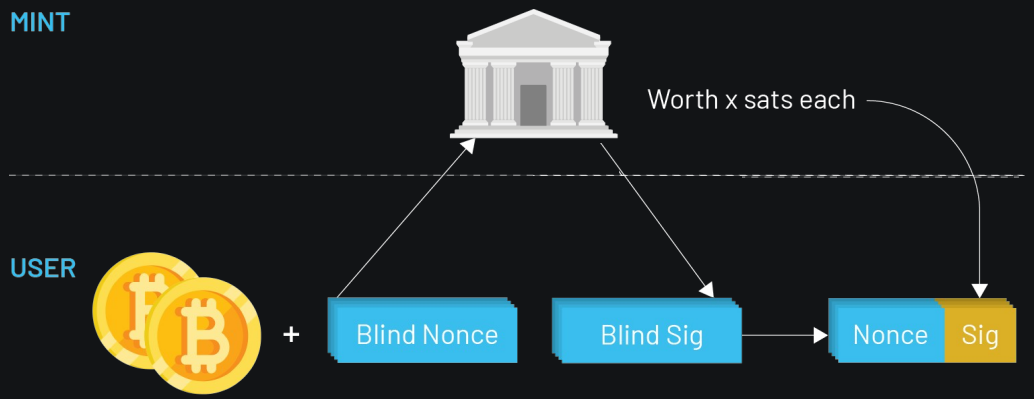
2. Mint Send Blind Sig to User



Blockstream

Traditional E-Cash **Issuance**

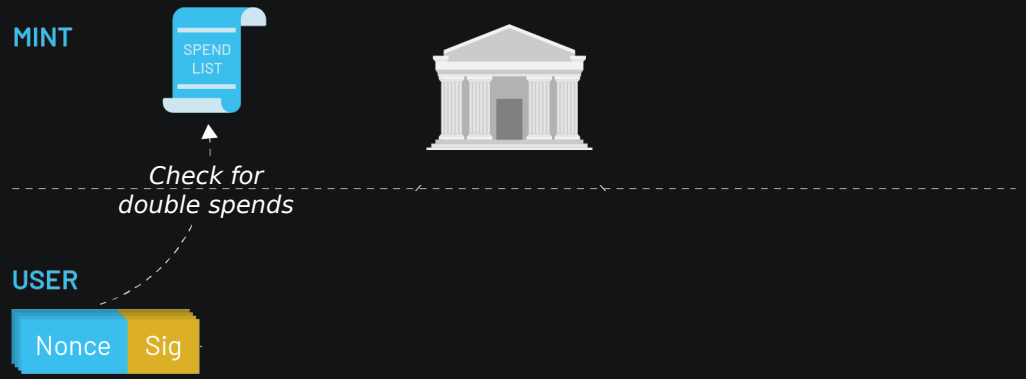
3. User Creates a Redeem Receipt



Blockstream

Traditional E-Cash **Spending**

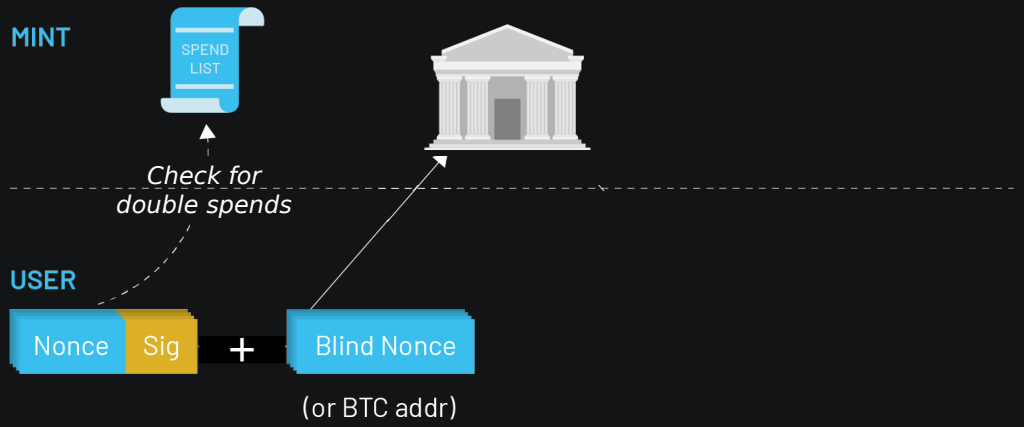
1. User Checks for Double Spends



Blockstream

Traditional E-Cash **Spending**

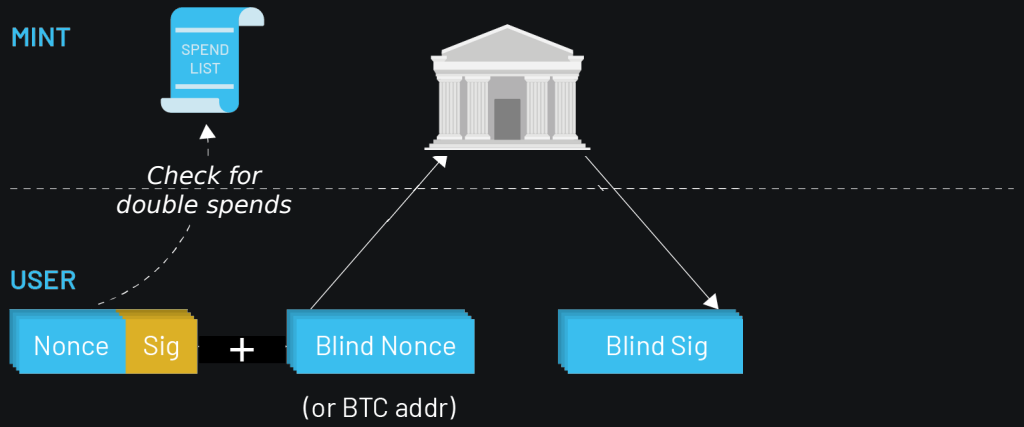
2. User Sends Blind Nonce to the Mint



Blockstream

Traditional E-Cash **Spending**

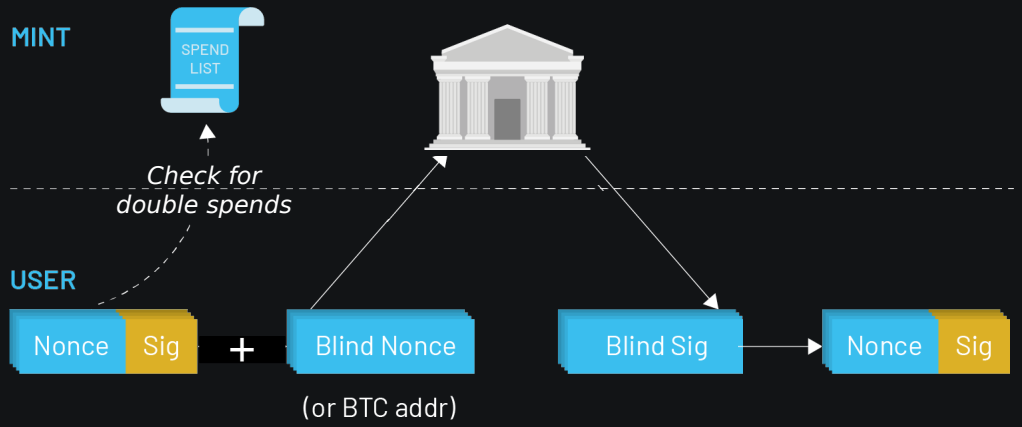
3. Mint Sends Blind Signature to the User



Blockstream

Traditional E-Cash **Spending**

4. User Creates a Redeem Receipt



Blockstream

Traditional E-Cash **Pros and Cons**

Pros
• Theoretically perfect anonymity • Scalable (*)

Traditional E-Cash **Pros and Cons**

Pros	Cons
• Theoretically perfect anonymity • Scalable (*)	• Centralized = Easy to attack - Token issuance - Collateral storage • No cross-mint transactions • Not easily auditable

Traditional E-Cash **Pros and Cons**

Pros	Cons
• Theoretically perfect anonymity • Scalable (*)	• Centralized = Easy to attack - Token issuance - Collateral storage • No cross-mint transactions • Not easily auditable

Federations to the rescue!

Don’t trust one party completely, but instead t of n parties to not collude.

Federations to the rescue!

Don’t trust one party completely, but instead t of n parties to not collude.

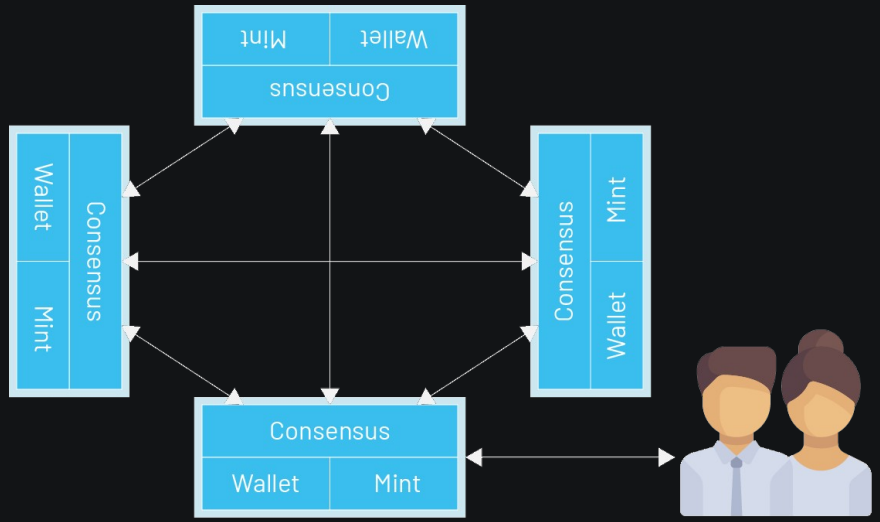
Token issuance → Threshold blind signatures

Collateral Storage → Bitcoin Multisig

2 Federated E-Cash

Federated **E-Cash**

Replicated State Machine implementing a multisig wallet and e-cash mint.



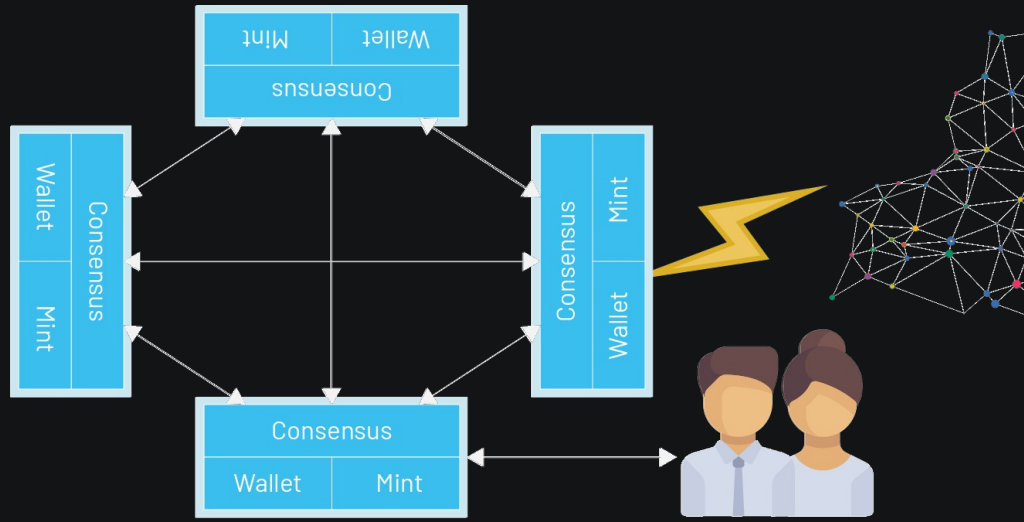
Blockstream

Federated E-Cash
Pros and Cons

Pros	Cons
• Theoretically perfect anonymity • Scalable (*)	• ~~Centralized = Easy to attack~~ ~~- Token issuance~~ ~~- Collateral storage~~ • No cross-mint transactions • Not easily auditable

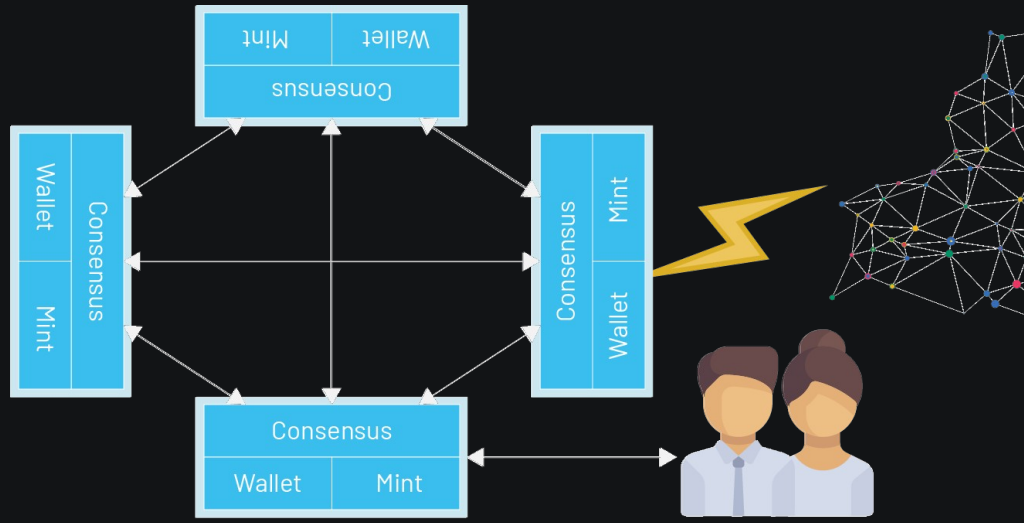
Blockstream

Federated E-Cash **with LN Integration**



Blockstream

Federated E-Cash **with LN Integration**



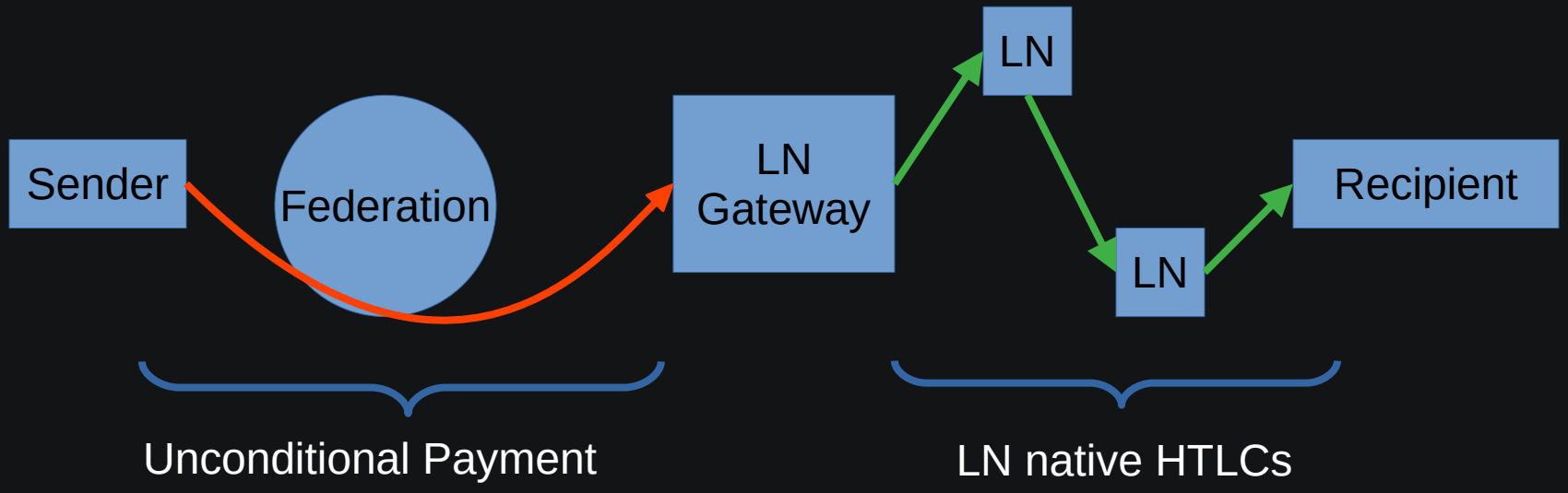
Version 1: Fully trusted LN gateway

Version 2: HTLCs inside the federation

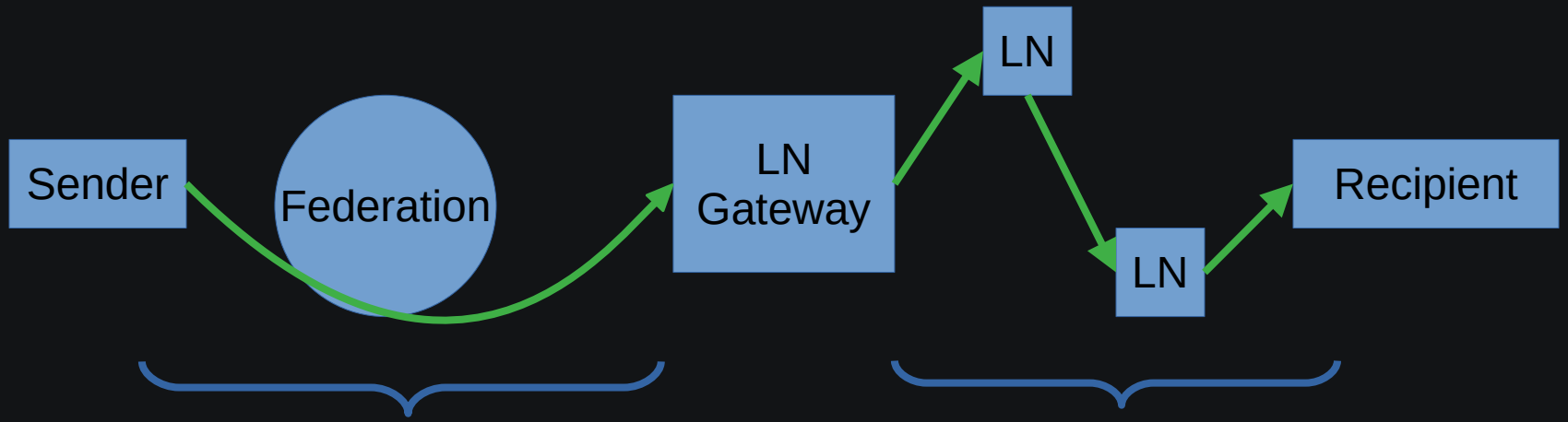
Version 3: Federated LN node

Blockstream

Version 1 **LN Integration:**



Version 2 **LN Integration:**

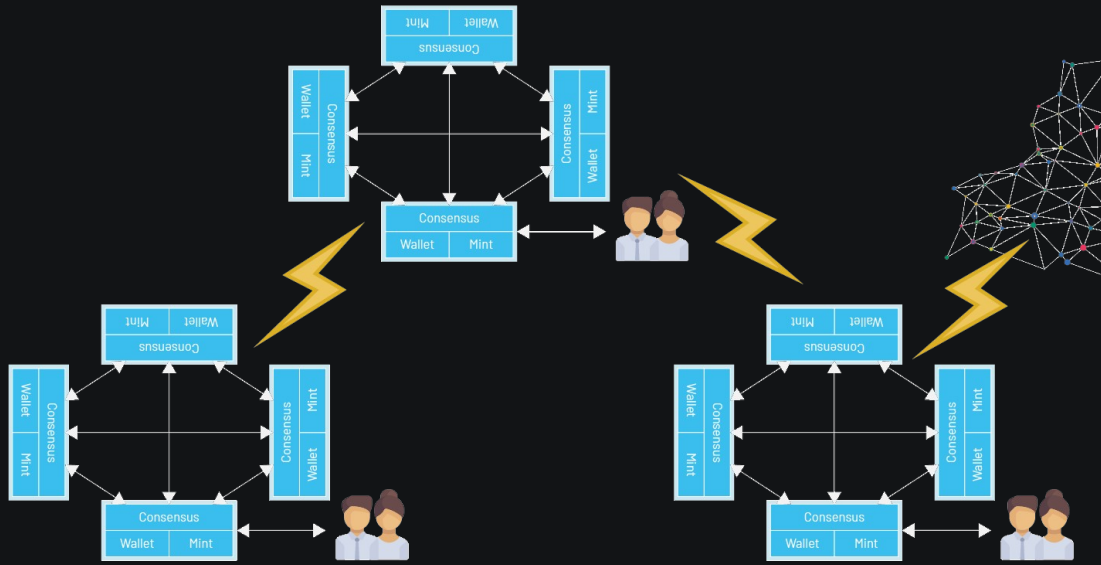


Payment if:

- Preimage is presented
- Timelock hasn’t expired

LN native HTLCs

Federation of **Federations with LN Integration**



Blockstream

Federated E-Cash

- Private
- Scalable
- Trust-minimized

More at

fedimint.org

Blockstream