Smart Contracts for Litecoin

Clemens Ley and Laura Tardivo

Litecoin Summit 2024

Bitcoin Computer

Overview

Classification

- Interoperable Blockchains (Stacks)
- Sidechains (Liquid, RSK)
- Rollups (BitVM, Citera)
- Block-order based (BRC20)
- UTXO-based (Ordinals, Runes, Bitcoin Computer)

Comparison

- Trustless Is there no trusted third party?
- Expressive Can all smart contracts be expressed?
- Efficient Can you compute a value without reading all txs?

Overview

	Trustless	**Expressive**	**Efficient**
	Is there no trusted third party?	Can all smart contracts be expressed?	Can you compute a value without reading all txs?
Ethereum			
Interoperable			
Sidechain			
Rollup			
Order based			
UTXO based			
Bitcoin Computer			

Overview

	Trustless	Expressive	Efficient
	Is there no trusted third party?	Can all smart contracts be expressed?	Can you compute a value without reading all txs?
Ethereum	Yes	Yes	No
Interoperable			
Sidechain			
Rollup			
Order based			
UTXO based			
Bitcoin Computer			

Interoperable Blockchains

Stacks, Internet Computer, BOB

- A separate blockchain (L2) that
  - can read from and write to L1
  - use L1 asset in the consensus algorithm of the L2
- How to use:
  - Use an exchange to get L2 asset
  - Use functionality of the L2
  - Use exchange to get L1 asset

Sidechains

Liquid, Rootstock

- A separate blockchain (L2) connected to L1 via two-way-peg
- How to use:
  - Send L1 asset into custody of a federation
  - The federation will issue you L2 asset
  - Use the functionality of the L2
  - Send L2 asset to the federation, they will give you L1 asset

Rollups

BitVM, Optimism & Arbitrum on Ethereum

- Like a sidechains but the federation is replaced by a smart contract and data is stored on the L1
- How to use:
  - Deposit L1 asset into rollup smart contract on L1
  - To use L2
    - Send L2 transaction to an aggregator
    - Aggregator evaluates L2 transactions and publishes L2 transactions and state hash on L1
    - Smart contract on L1 guarantees that the evaluation is valid (see next slide for details)
  - Send withdraw request to aggregator to get L1 asset

Rollups - Validation

How does the L1 contract ensure the validity of L2 batch?

- Optimistic
  - Aggregator publishes a L2 batch to L1 contract
  - Validators can provide a fraud proof to L1 smart contract
  - If the fraud proof is correct, the aggregator is fined
  - Otherwise the validator is fined

- Zero knowledge
  - Aggregator publishes L2 batch and validity proof to L1 contract
  - Contract verifies the proof
  - STARKS: trustless but expensive
  - SNARKS: less expensive but require a trusted setup

Overview

	Trustless	Expressive	Efficient
	Is there no trusted third party?	Can all smart contracts be expressed?	Can you compute a value without reading all txs?
Ethereum	Yes	Yes	No
Interoperable	No	Yes	No
Sidechain	No	Yes	No
Rollup	No	Yes	No
Order based			
UTXO based			
Bitcoin Computer			

80% of smart contracts on Ethereum are tokens

What can Litecoin do?

Layer 1

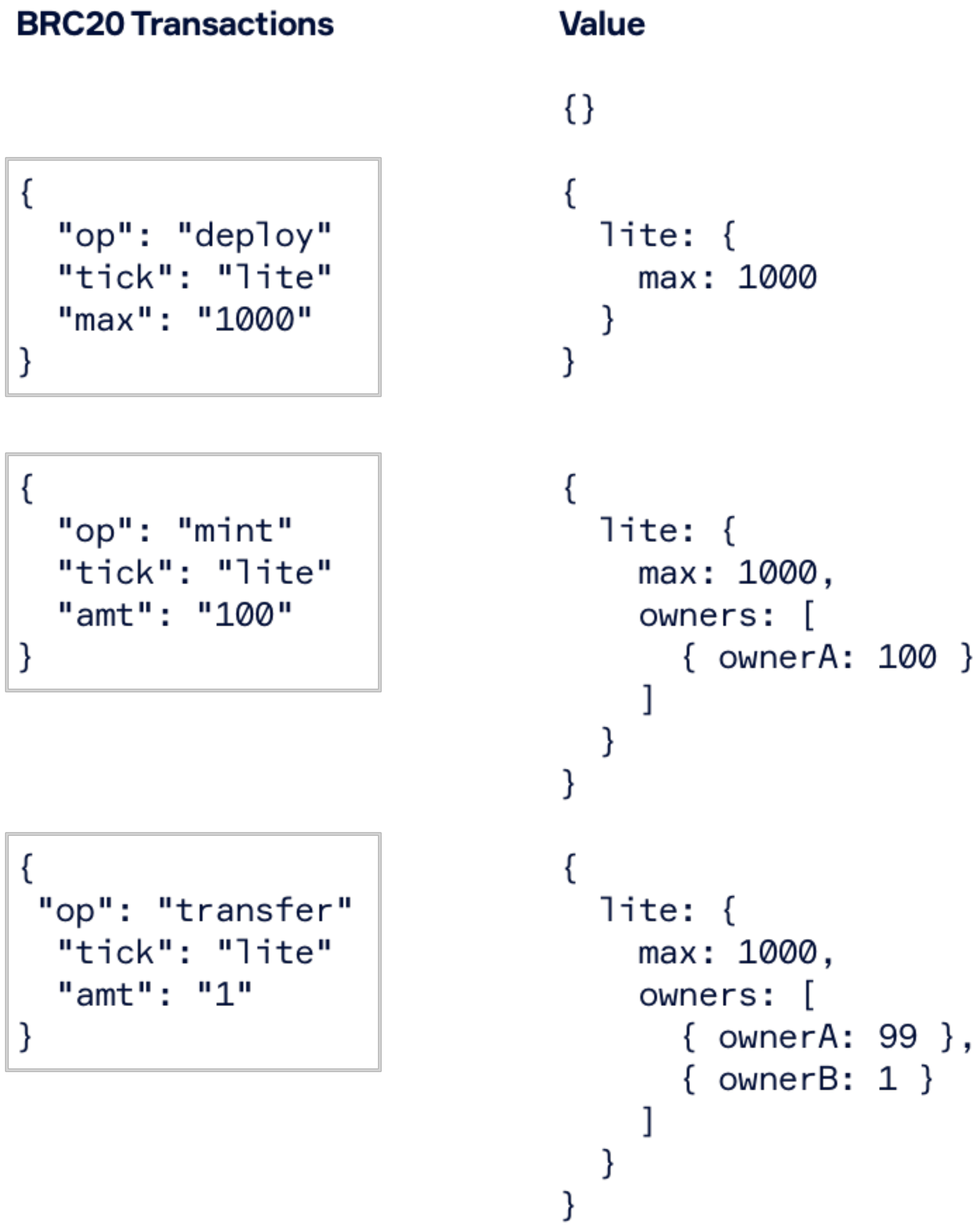
Ordinals, Runes, BRC20, Omni, Counterparty, Bitcoin Computer

- No extra blockchain, no trusted third party, just metadata on chain
- How to use:
  - Add metadata to a transaction to create or update a value
  - Parse the metadata on the blockchain to compute/read the value
- Two variants:
  - Block-order based
  - UTXO based

Layer 1

Block-order based

- Broadcast transaction with meta data
- Read transactions in block order
- Update a value after each transaction
- Advantages
  - Self custody
- Disadvantages
  - Not efficient
  - Not expressive
  - Not composable



BRC20 Transactions

Value

```
{}
```

```
{
  "op": "deploy"
  "tick": "lite"
  "max": "1000"
}
```

```
{
  lite: {
    max: 1000
  }
}
```

```
{
  "op": "mint"
  "tick": "lite"
  "amt": "100"
}
```

```
{
  lite: {
    max: 1000,
    owners: [
      { ownerA: 100 }
    ]
  }
}
```

```
{
 "op": "transfer"
  "tick": "lite"
  "amt": "1"
}
```

```
{
  lite: {
    max: 1000,
    owners: [
      { ownerA: 99 },
      { ownerB: 1 }
    ]
  }
}
```

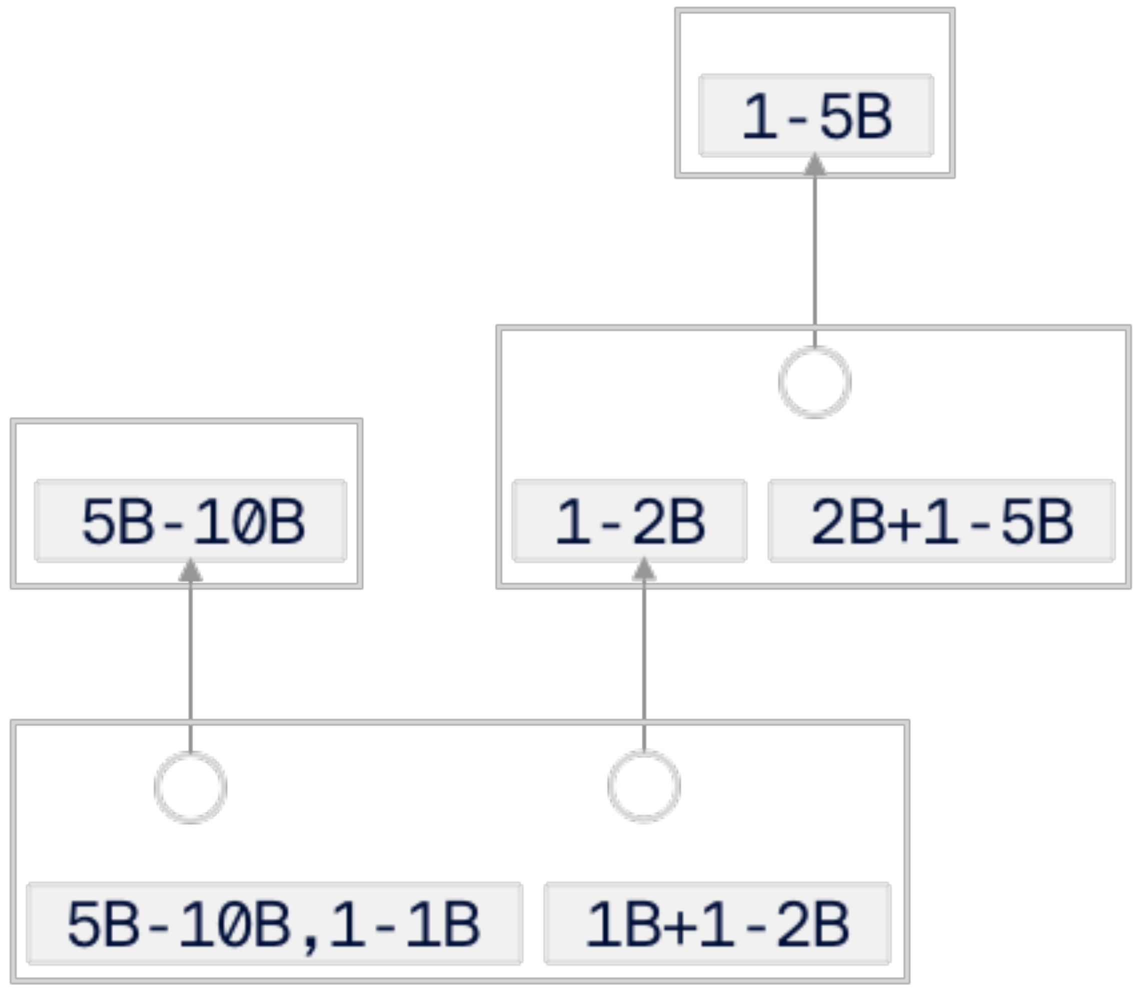
Bitcoin Computer

Layer 1

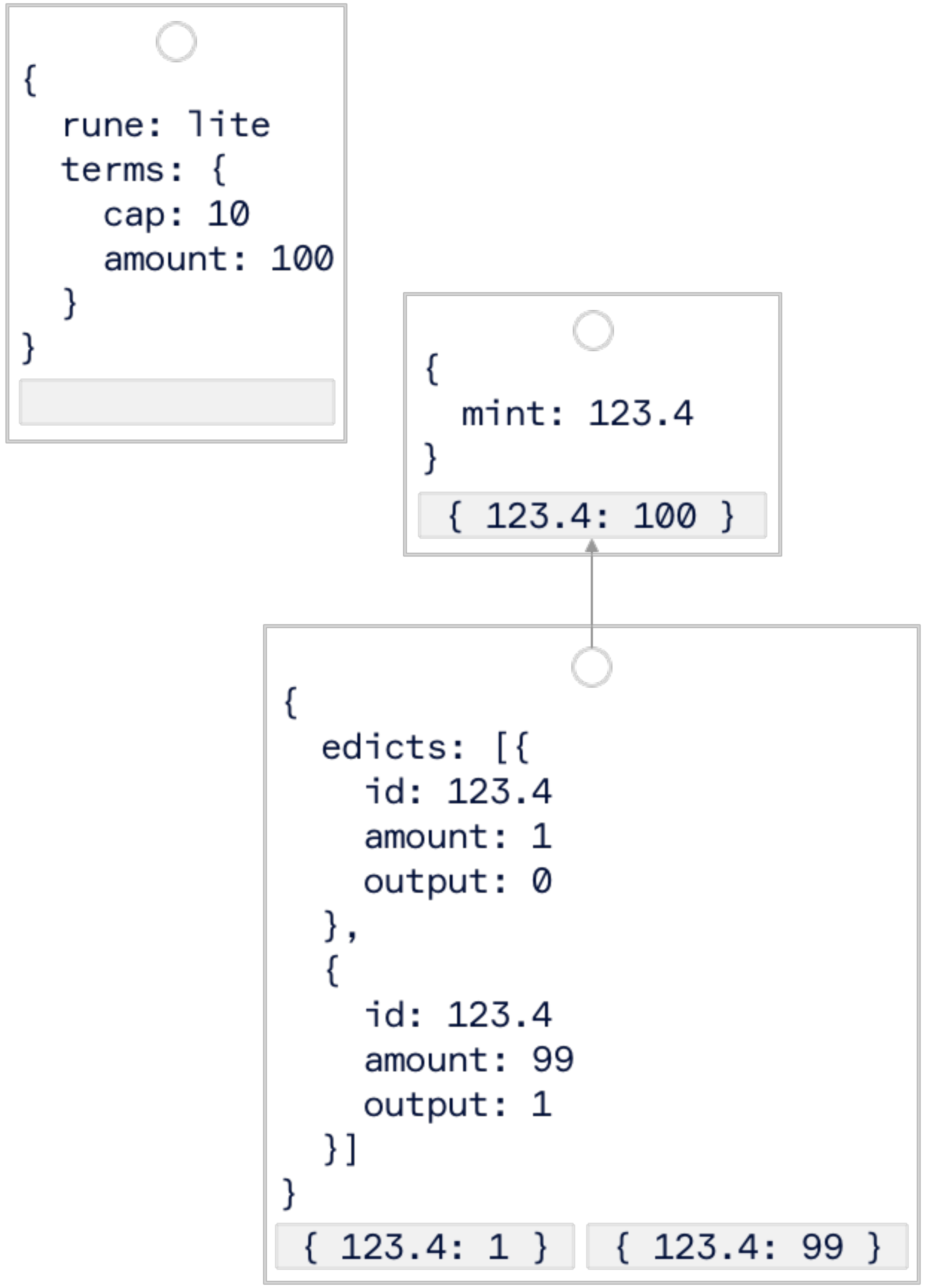
UTXO based

- Broadcast transaction with meta data
- Associate a value with each output, using the meta data and the values of the inputs spent
- Advantages
  - Self custody
  - More efficient
- Disadvantages
  - Not expressive

Ordinals Example



Runes Example



```
{
  rune: lite
  terms: {
    cap: 10
    amount: 100
  }
}
```

```
{
  mint: 123.4
}
```

{ 123.4: 100 }

```
{
  edicts: [{
    id: 123.4
    amount: 1
    output: 0
  },
  {
    id: 123.4
    amount: 99
    output: 1
  }]
}
```

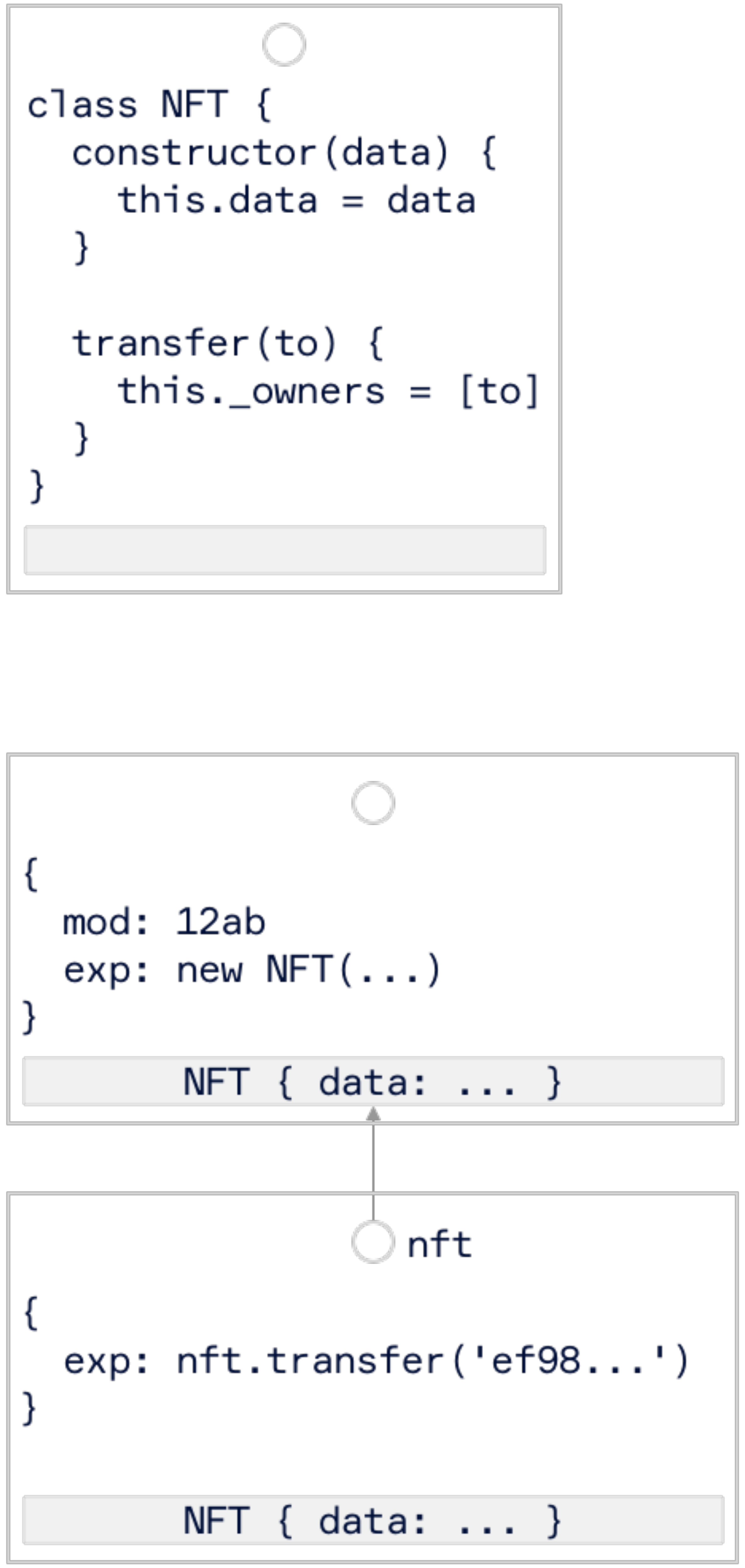
{ 123.4: 1 } { 123.4: 99 }

Layer 1

Bitcoin Computer

- Broadcast transaction with Javascript code
- Associate a value with each output, by evaluating the Javascript expression, using the values of the outputs spent for the variables
- Advantages
  - Self custody
  - Expressive
  - Efficient
  - Compatible

Non Fungible Token

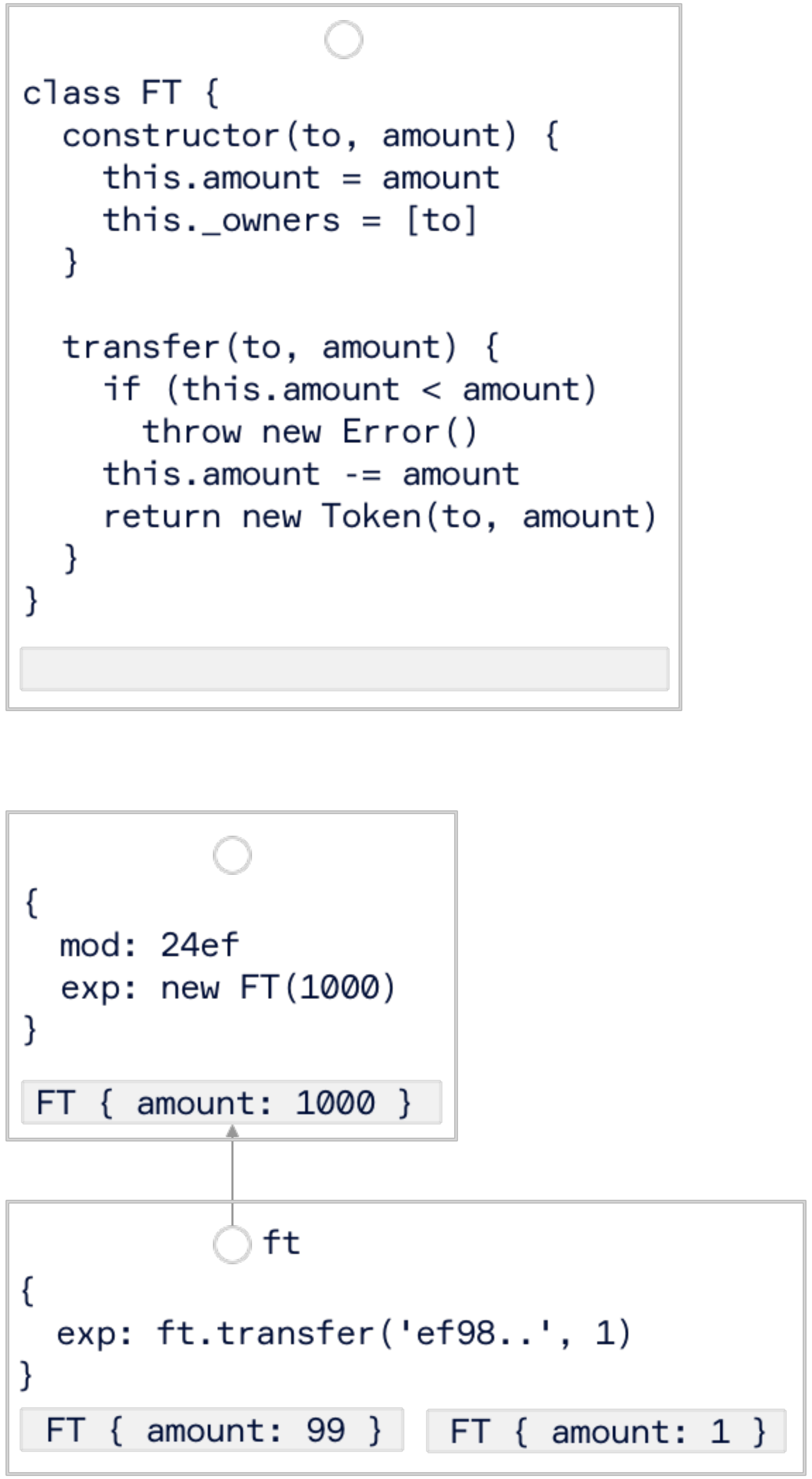


```
class NFT {
  constructor(data) {
    this.data = data
  }

  transfer(to) {
    this._owners = [to]
  }
}
```

```
{
  mod: 12ab
  exp: new NFT(...)
}
```

```
{
  exp: nft.transfer('ef98...')
}
```

Fungible Token



```
class FT {
  constructor(to, amount) {
    this.amount = amount
    this._owners = [to]
  }

  transfer(to, amount) {
    if (this.amount < amount)
      throw new Error()
    this.amount -= amount
    return new Token(to, amount)
  }
}
```

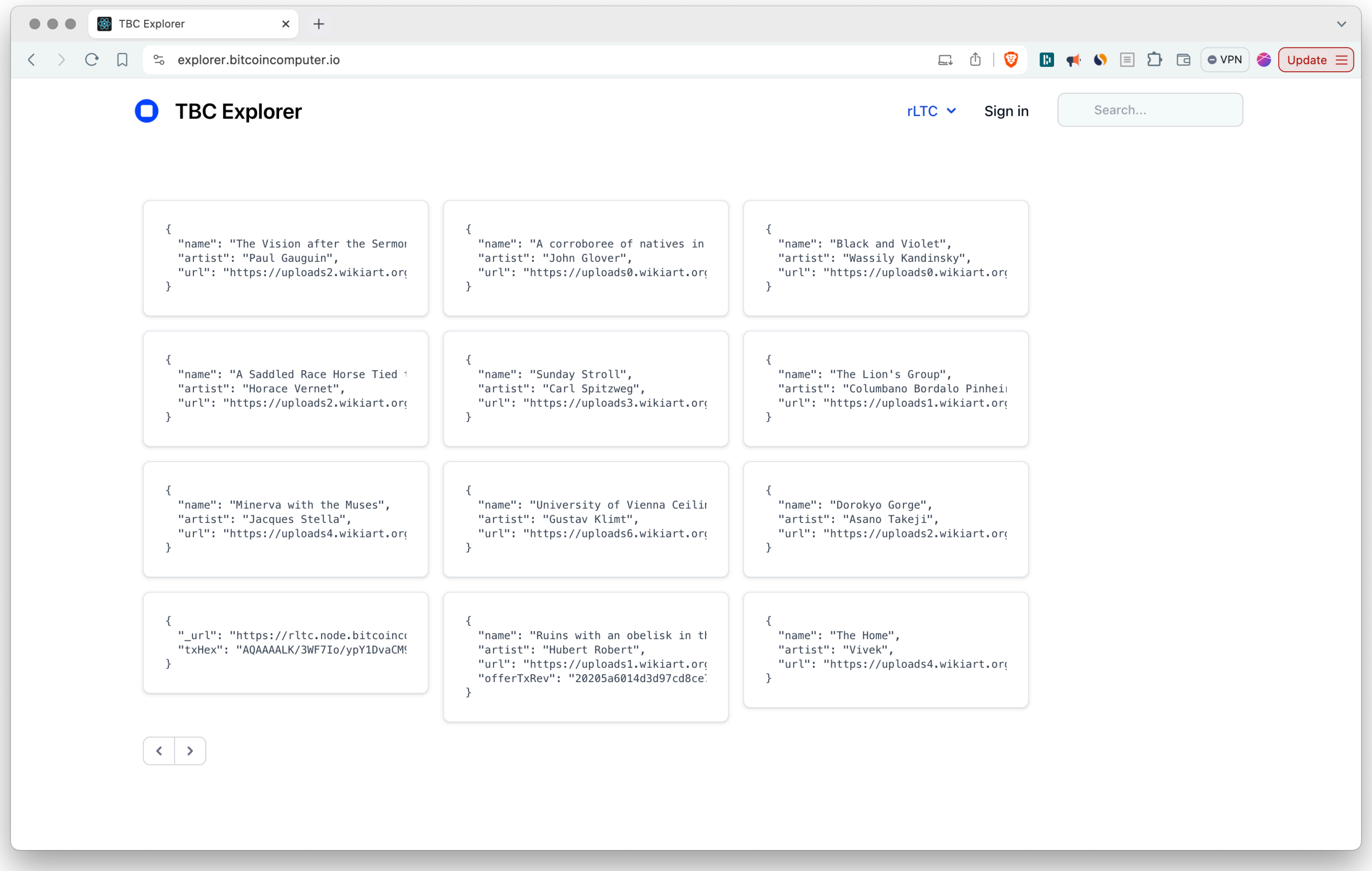
```
{
  mod: 24ef
  exp: new FT(1000)
}
```

```
{
  exp: ft.transfer('ef98..', 1)
}
```

Overview

	Trustless	Expressive	Efficient
	Is there no trusted third party?	Can all smart contracts be expressed?	Can you compute a value without reading all txs?
Ethereum	Yes	Yes	No
Interoperable	No	Yes	No
Sidechain	No	Yes	No
Rollup	No	Yes	No
Order based	Yes	No	No
UTXO based	Yes	No	Yes
Bitcoin Computer	Yes	Yes	Yes

Conclusion



```
{
  "name": "The Vision after the Sermoı
  "artist": "Paul Gauguin",
  "url": "https://uploads2.wikiart.or
}
```

```
{
  "name": "A corroboree of natives in
  "artist": "John Glover",
  "url": "https://uploads0.wikiart.or
}
```

```
{
  "name": "Black and Violet",
  "artist": "Wassily Kandinsky",
  "url": "https://uploads0.wikiart.or
}
```

```
{
  "name": "A Saddled Race Horse Tied
  "artist": "Horace Vernet",
  "url": "https://uploads2.wikiart.or
}
```

```
{
  "name": "Sunday Stroll",
  "artist": "Carl Spitzweg",
  "url": "https://uploads3.wikiart.or
}
```

```
{
  "name": "The Lion's Group",
  "artist": "Columbano Bordalo Pinhei
  "url": "https://uploads1.wikiart.or
}
```

```
{
  "name": "Minerva with the Muses",
  "artist": "Jacques Stella",
  "url": "https://uploads4.wikiart.or
}
```

```
{
  "name": "University of Vienna Ceili
  "artist": "Gustav Klimt",
  "url": "https://uploads6.wikiart.or
}
```

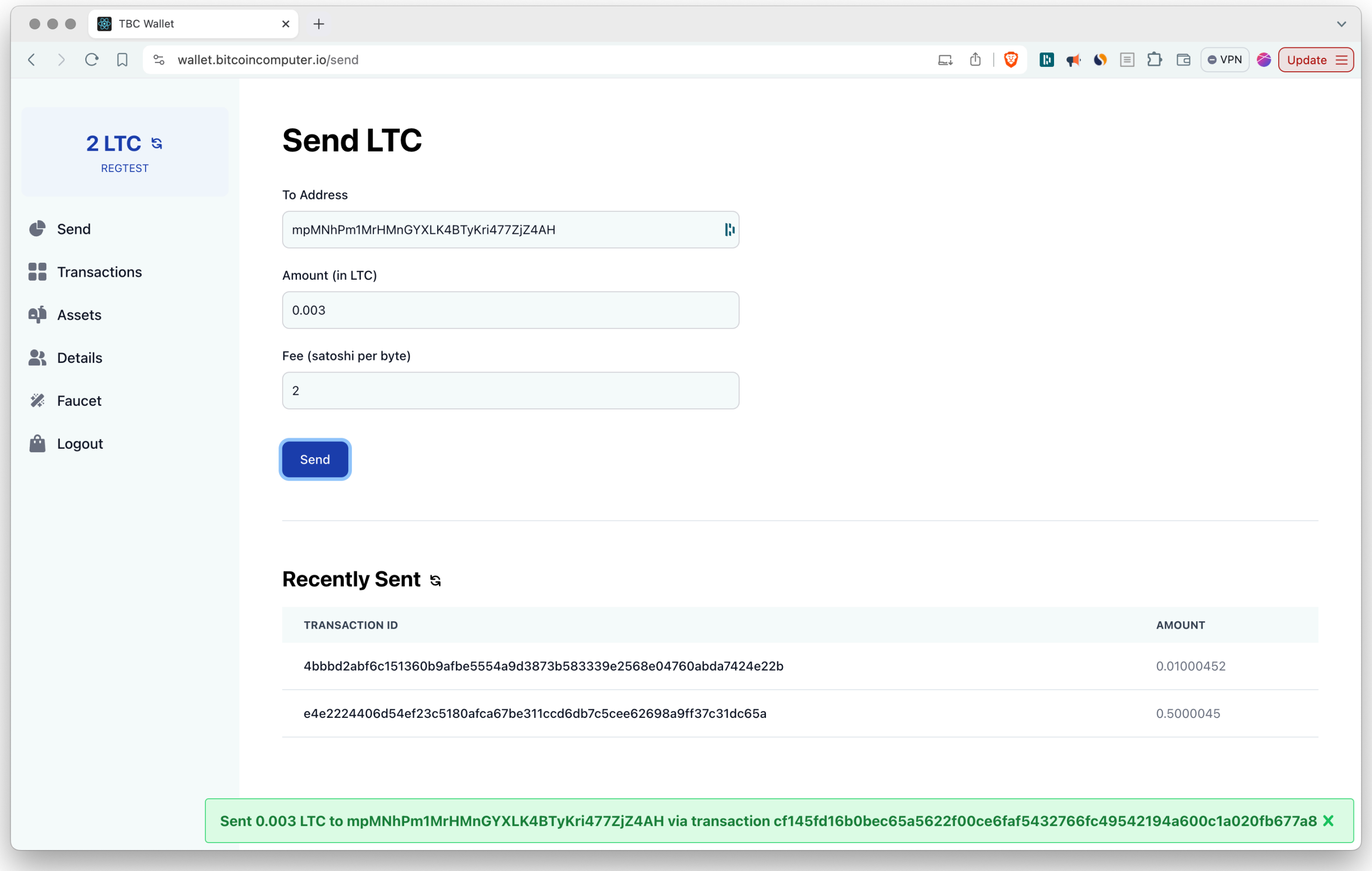
```
{
  "name": "Dorokyo Gorge",
  "artist": "Asano Takeji",
  "url": "https://uploads2.wikiart.or
}
```

```
{
  "_url": "https://rltc.node.bitcoinc
  "txHex": "AQAAAALK/3WF7Io/ypY1DvaCM
}
```

```
{
  "name": "Ruins with an obelisk in tl
  "artist": "Hubert Robert",
  "url": "https://uploads1.wikiart.or
  "offerTxRev": "20205a6014d3d97cd8ce
}
```

```
{
  "name": "The Home",
  "artist": "Vivek",
  "url": "https://uploads4.wikiart.or
}
```

explorer.bitcoincomputer.io



Send LTC

To Address: mpMNhPm1MrHMnGYXLK4BTyKri477ZjZ4AH

Amount (in LTC): 0.003

Fee (satoshi per byte): 2

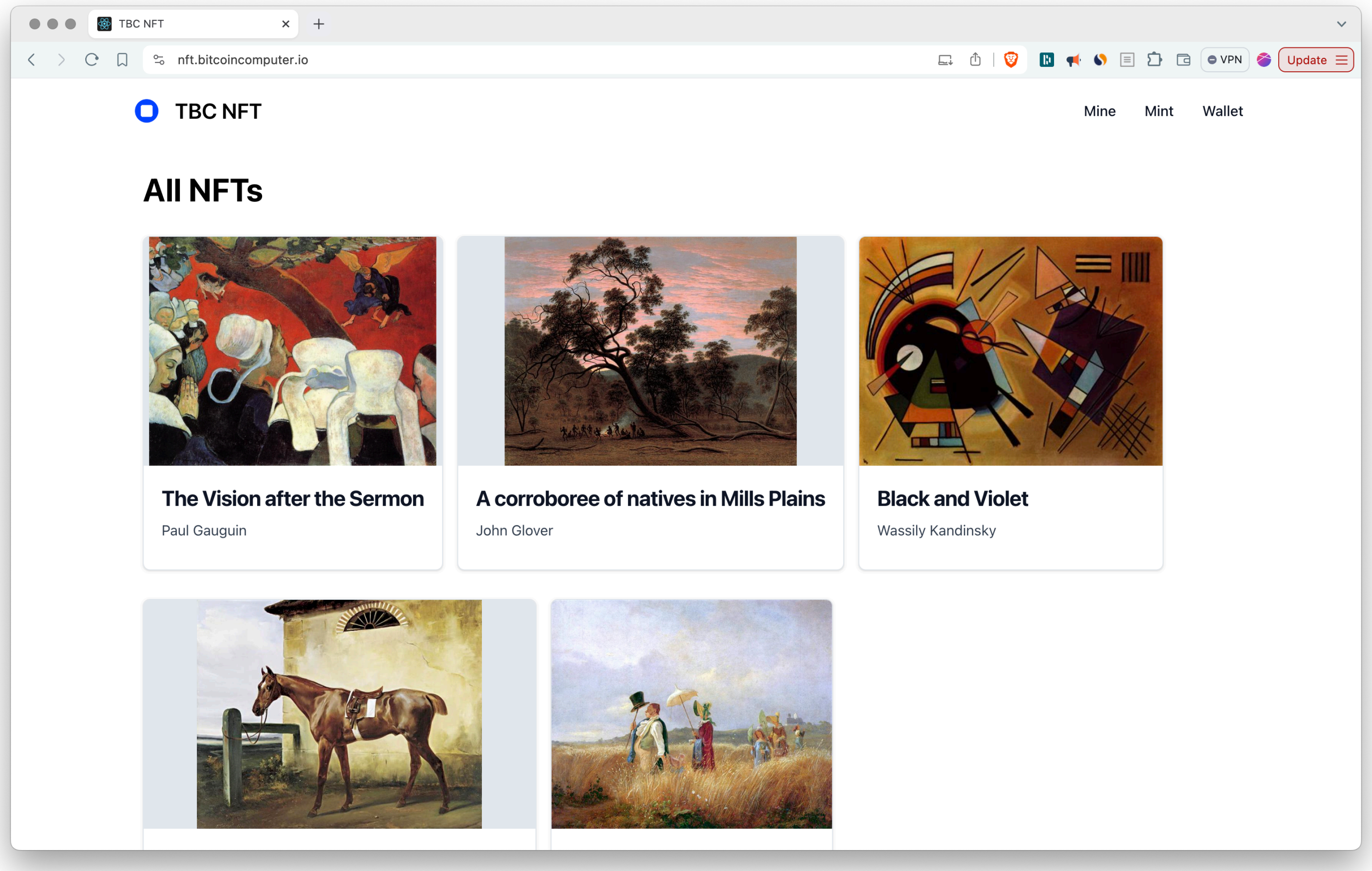
Send

Recently Sent

TRANSACTION ID	AMOUNT
4bbbd2abf6c151360b9afbe5554a9d3873b583339e2568e04760abda7424e22b	0.01000452
e4e2224406d54ef23c5180afca67be311ccd6db7c5cee62698a9ff37c31dc65a	0.5000045

Sent 0.003 LTC to mpMNhPm1MrHMnGYXLK4BTyKri477ZjZ4AH via transaction cf145fd16b0bec65a5622f00ce6faf5432766fc49542194a600c1a020fb677a8 X

wallet.bitcoincomputer.io



All NFTs

The Vision after the Sermon
Paul Gauguin

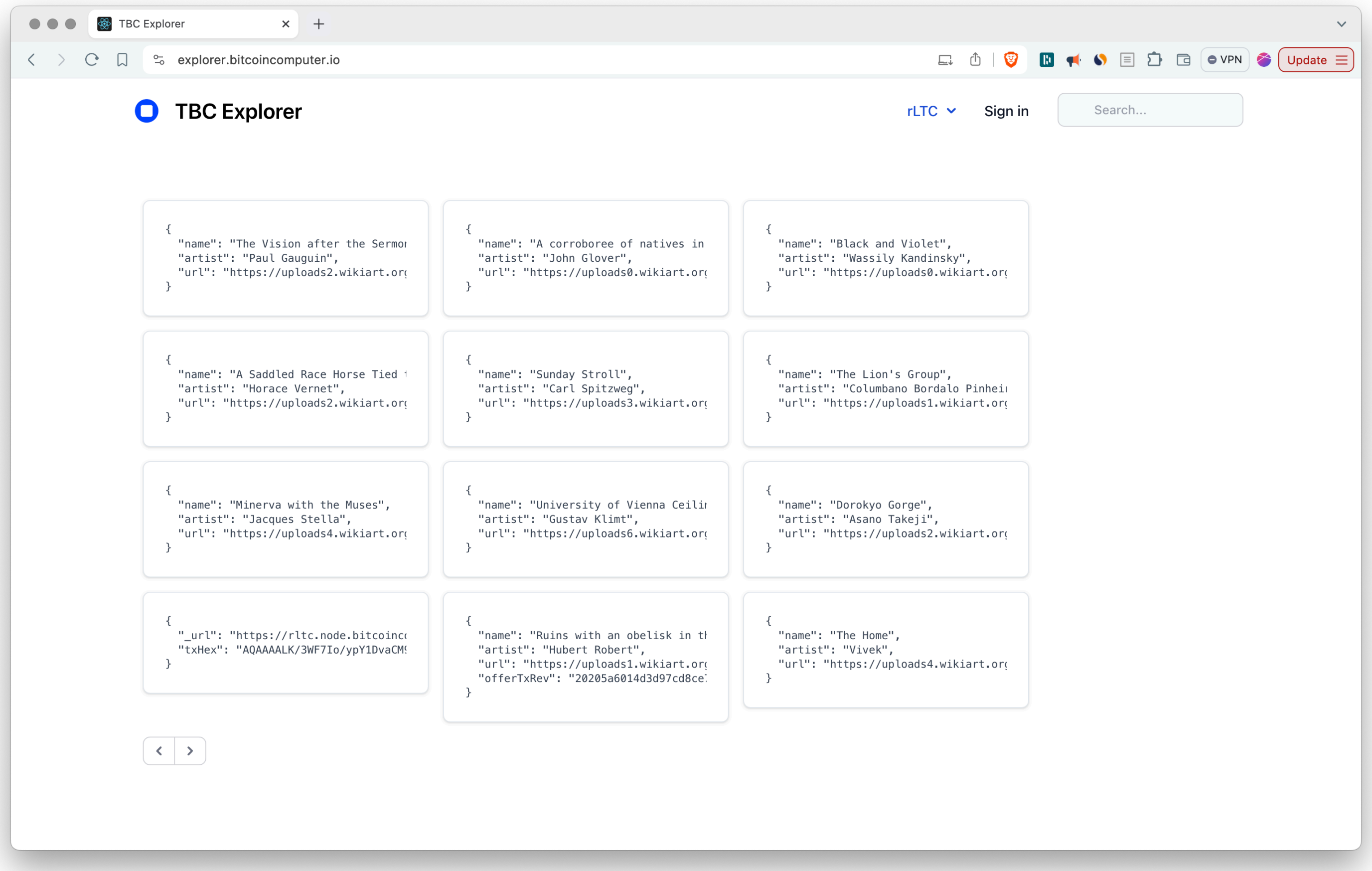
A corroboree of natives in Mills Plains
John Glover

Black and Violet
Wassily Kandinsky

nft.bitcoincomputer.io

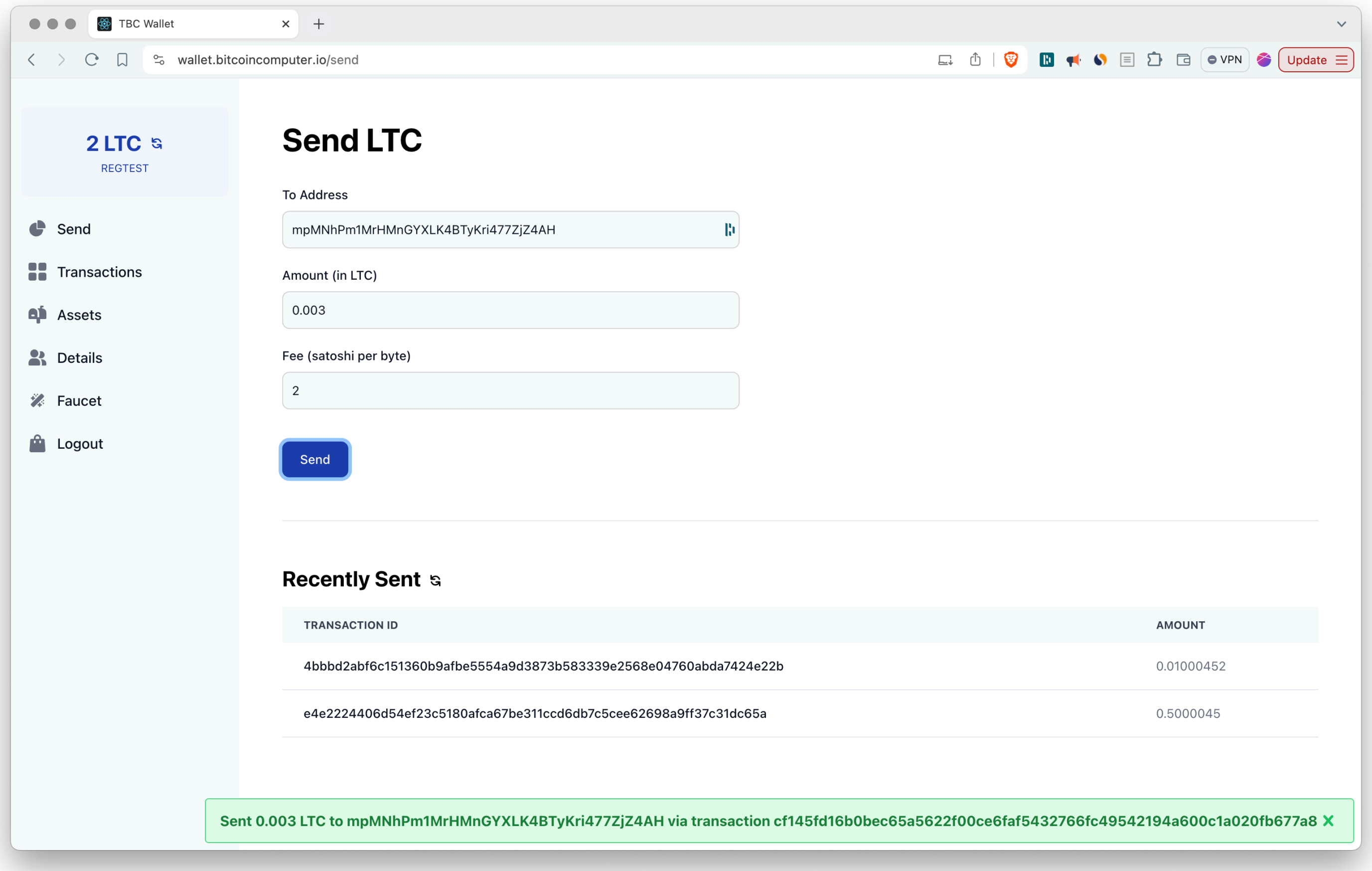
docs.bitcoincomputer.io

Thank you!



```
{
  "name": "The Vision after the Sermoı
  "artist": "Paul Gauguin",
  "url": "https://uploads2.wikiart.or(
}

{
  "name": "A corroboree of natives in
  "artist": "John Glover",
  "url": "https://uploads0.wikiart.or(
}

{
  "name": "Black and Violet",
  "artist": "Wassily Kandinsky",
  "url": "https://uploads0.wikiart.or(
}

{
  "name": "A Saddled Race Horse Tied
  "artist": "Horace Vernet",
  "url": "https://uploads2.wikiart.or(
}

{
  "name": "Sunday Stroll",
  "artist": "Carl Spitzweg",
  "url": "https://uploads3.wikiart.or(
}

{
  "name": "The Lion's Group",
  "artist": "Columbano Bordalo Pinheiı
  "url": "https://uploads1.wikiart.or(
}

{
  "name": "Minerva with the Muses",
  "artist": "Jacques Stella",
  "url": "https://uploads4.wikiart.or(
}

{
  "name": "University of Vienna Ceiliı
  "artist": "Gustav Klimt",
  "url": "https://uploads6.wikiart.or(
}

{
  "name": "Dorokyo Gorge",
  "artist": "Asano Takeji",
  "url": "https://uploads2.wikiart.or(
}

{
  "_url": "https://rltc.node.bitcoinc(
  "txHex": "AQAAAALK/3WF7Io/ypY1DvaCM(
}

{
  "name": "Ruins with an obelisk in tl
  "artist": "Hubert Robert",
  "url": "https://uploads1.wikiart.or(
  "offerTxRev": "20205a6014d3d97cd8ce]
}

{
  "name": "The Home",
  "artist": "Vivek",
  "url": "https://uploads4.wikiart.or(
}
```

explorer.bitcoincomputer.io



Send LTC

To Address: mpMNhPm1MrHMnGYXLK4BTyKri477ZjZ4AH

Amount (in LTC): 0.003

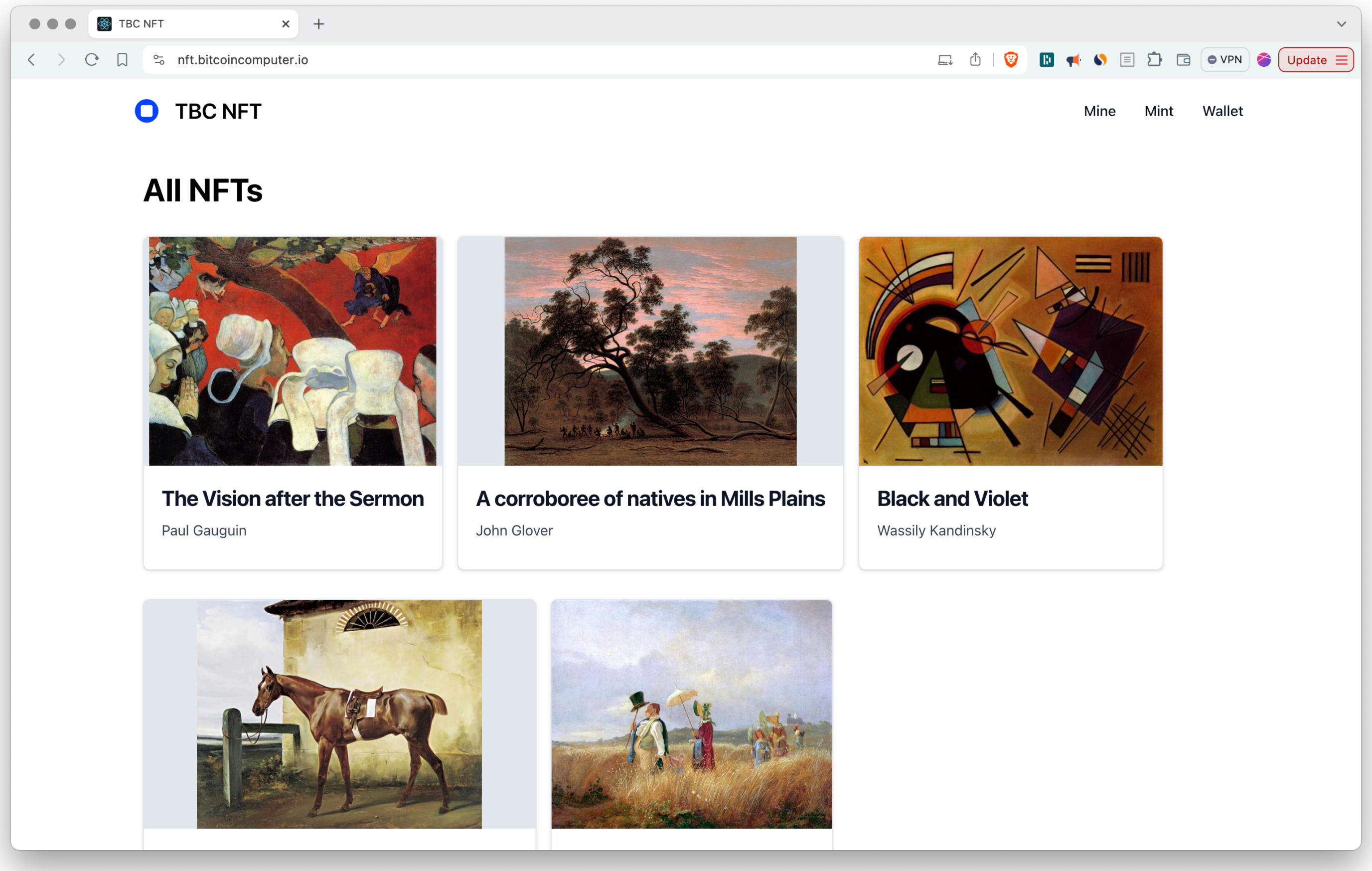
Fee (satoshi per byte): 2

Recently Sent

TRANSACTION ID	AMOUNT
4bbbd2abf6c151360b9afbe5554a9d3873b583339e2568e04760abda7424e22b	0.01000452
e4e2224406d54ef23c5180afca67be311ccd6db7c5cee62698a9ff37c31dc65a	0.5000045

Sent 0.003 LTC to mpMNhPm1MrHMnGYXLK4BTyKri477ZjZ4AH via transaction cf145fd16b0bec65a5622f00ce6faf5432766fc49542194a600c1a020fb677a8 X

wallet.bitcoincomputer.io



All NFTs

The Vision after the Sermon
Paul Gauguin

A corroboree of natives in Mills Plains
John Glover

Black and Violet
Wassily Kandinsky

nft.bitcoincomputer.io

docs.bitcoincomputer.io