IOV

Blockchain Communication Protocol

Karim Ganem - CEO IOV - karim@iov.one

Antoine Herzog - CIO IOV - antoine@iov.one

Benjamin Simatos - CFO IOV - benjamin@iov.one

IOV: A Browser of Value

Version 1.3

Antoine Herzog[a], Serge Karim Ganem[b], and Florin Dzeladini[c]

[a]antoine@iov.one; [b]karim@iov.one; [c]florin@iov.one

Abstract

A Browser of Value would allow users to store and exchange multiple types of values without the need to download an electronic wallet each time a new blockchain is being created.

The decentralization of blockchains has created a diversified ecosystem of autonomous blockchains, with each system requiring different protocols to access coins and values. The lack of standardization makes it very difficult for a current electronic wallet to send a transaction or to query several different blockchains.

We propose a solution to empower the end-user and remove the need to download multiple wallets.

blockchain per token.

Ethereum approach and the ERC20 Token

In November 2015, Ethereum published a first specification to store and exchange many different tokens on the Ethereum blockchain. It allowed dapps and wallets to handle tokens across multiple interfaces/dapps. This specification also allowed projects to be funded via ICOs (Initial Coin Offerings).

Current limitations. Unfortunately this specification only exists in the Ethereum blockchain. Besides, the

IOV SAS - French Blockchain company born in March 2018

BATTLEFIELD RUNNER UP

IOV

IOV Technology Today

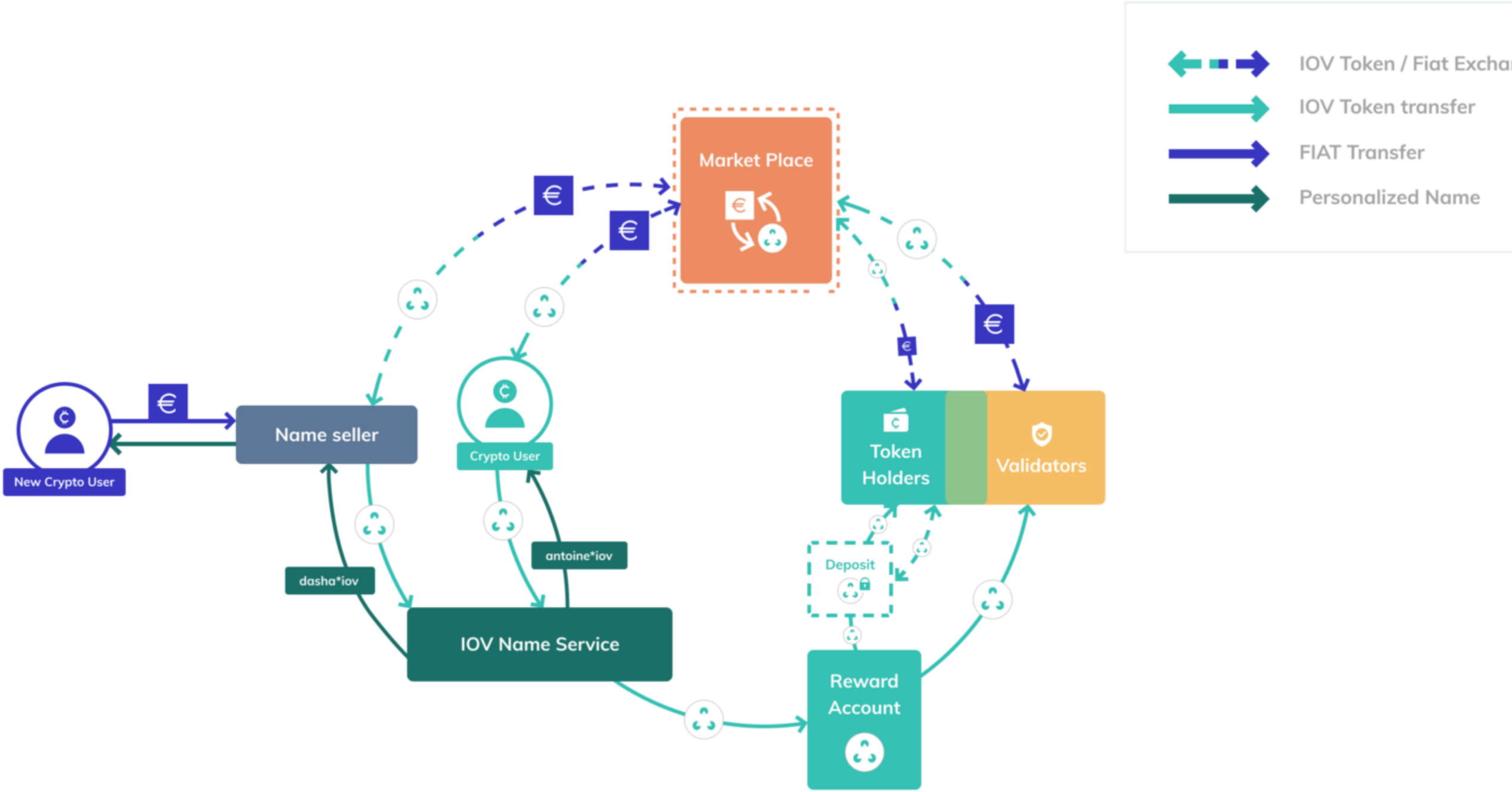
- IOV Name Service (close to launch Q2 2019)

- Blockchain Communication Protocol & IOV-core

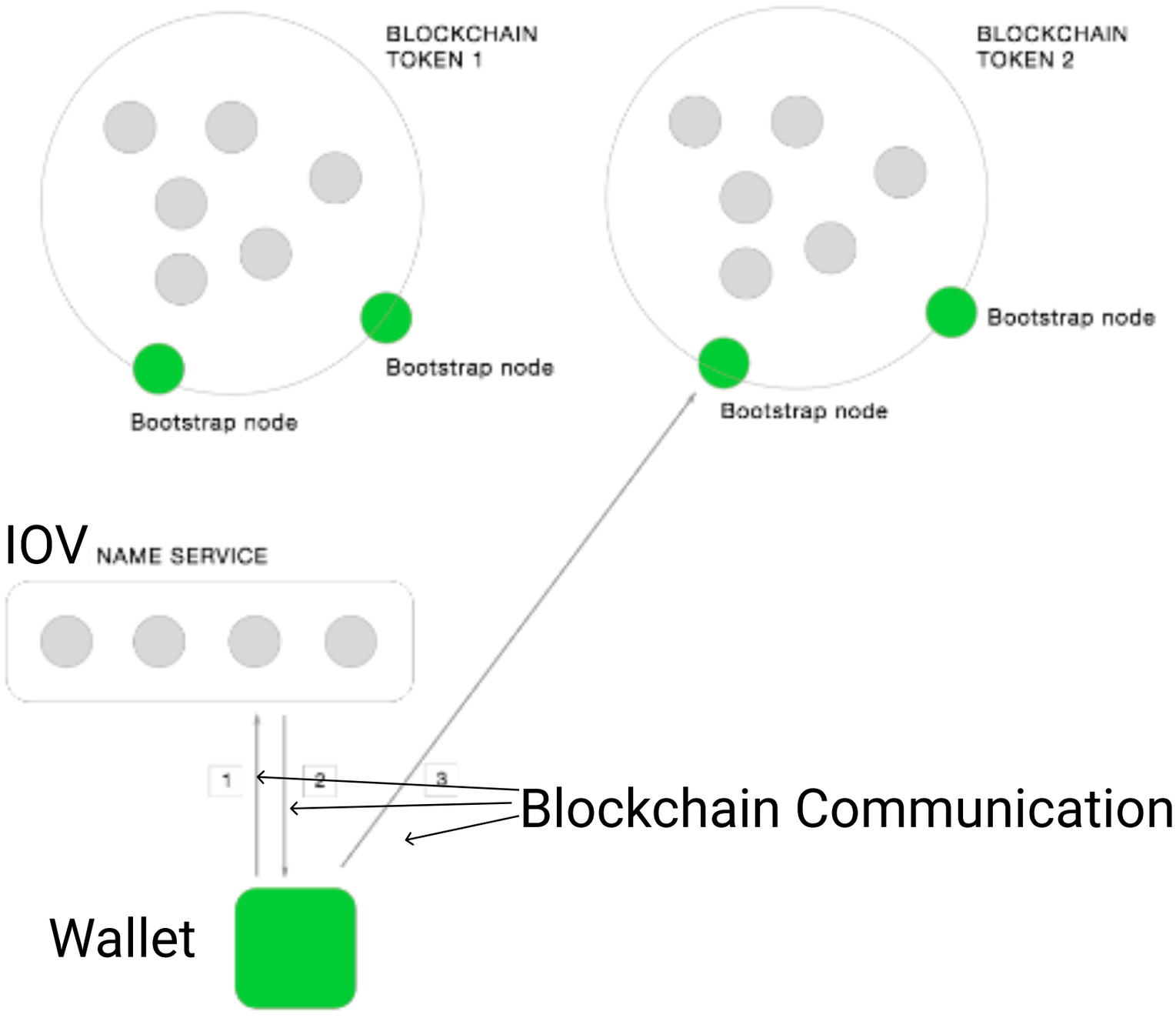
- Google Chrome Extension

- Weave SDK (Tendermint Golang Blockchain)

Economic Model of the IOV Name Service



Blockchain Communication Protocol



What is the Blockchain Communication Protocol

Set of agnostic standards to communicate between a wallet and a blockchain

IOV-Core

1st client implementation of the Blockchain Communication Protocol

iov-one / iov-core

Watch 47 | Unstar 187 | Fork 10

Code | Issues 34 | Pull requests 4 | Projects 0 | Wiki | Security | Insights | Settings

Client library for secure key management and multi-blockchain communication https://iov-one.github.io/iov-core-docs/ Edit

blockchain crypto Manage topics

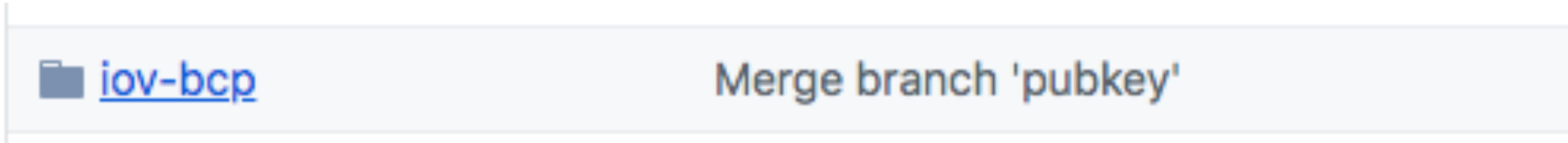
4,489 commits | 17 branches | 63 releases | 13 contributors | Apache-2.0

Branch: master | New pull request | Create new file | Upload files | Find File | Clone or download

webmaster128 Merge pull request #1060 from iov-one/229-rpc-queue ... Latest commit f472101 20 hours ago

custom_types	Migrate from jasmine2-custom-message to native withContext()	last month
docs	Reduce chain ID length from 128 to 32	7 days ago
packages	Merge pull request #1060 from iov-one/229-rpc-queue	20 hours ago
scripts	Merge branch 'pubkey'	22 hours ago
.editorconfig	Use simple socket server instead of Tendermint for @iov/socket	5 months ago
.eslintignore	Add .eslintignore to root package	22 days ago
.eslintrc.json	Update no-use-before-define eslint setting and fix	14 days ago
.gitignore	Exclude docs/ folder from npm package	10 months ago
.prettierrc.json	Default printWidth: 110, override for crypto spec tests	last year
.travis.yml	Add Linux/Firefox to allowed failures on Travis	last month

In IOV-core, we define an abstract interface called the Blockchain Communication Protocol to access a blockchain



What is IOV-core

Branch: master ▾ **iov-core** / **packages** /

Create new file | Upload files | Find file | History

webmaster128 Merge pull request #1060 from iov-one/229-rpc-queue ··· Latest commit `f472101` 20 hours ago

..

iov-bcp	Merge branch 'pubkey'	22 hours ago
iov-bns	Rename BnsUsernamesByOwnerAddressQuery to BnsUsernamesByOwnerQuery	21 hours ago
iov-cli	Merge branch 'pubkey'	22 hours ago
iov-core	Merge branch 'pubkey'	22 hours ago
iov-crypto	Merge branch '0.14'	23 hours ago
iov-dpos	Merge branch 'pubkey'	22 hours ago
iov-encoding	Merge branch '0.14'	23 hours ago
iov-ethereum	Merge branch 'pubkey'	22 hours ago
iov-faucets	Merge branch 'pubkey'	22 hours ago
iov-jsonrpc	Merge branch '0.14'	23 hours ago
iov-keycontrol	Merge branch 'pubkey'	22 hours ago
iov-lisk	Merge branch 'pubkey'	22 hours ago
iov-rise	Merge branch 'pubkey'	22 hours ago
iov-socket	Address QueueingStreamingSocket review comments	21 hours ago
iov-stream	Merge branch '0.14'	23 hours ago
iov-tendermint-rpc	Merge branch '0.14'	23 hours ago

What the Blockchain Communication Protocol looks like

```
// connection
  readonly disconnect: () => void;
  readonly chainId: () => ChainId;
  readonly height: () => Promise<number>;
  readonly getToken: (ticker: TokenTicker) => Promise
  readonly getAllTokens: () => Promise<readonly Toke
```

What the Blockchain Communication Protocol looks like

```
// accounts
readonly getAccount: (query: AccountQuery) => Pro
readonly watchAccount: (account: AccountQuery) =
readonly getNonce: (query: AddressQuery | Pubkey(
readonly getNonces: (query: AddressQuery | Pubkey
```

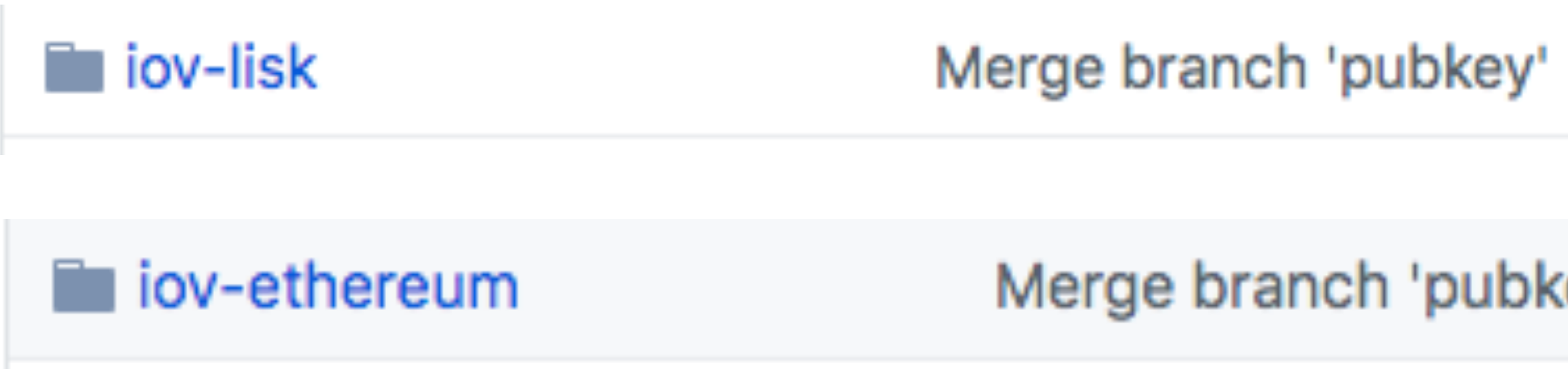
What the Blockchain Communication Protocol looks like

```
 // blocks
  readonly getBlockHeader: (height: number) => Prom
  readonly watchBlockHeaders: () => Stream<BlockH
```

What the Blockchain Communication Protocol looks like

```
// transactions
readonly getTx: (
  id: TransactionId,
) => Promise<ConfirmedTransaction<UnsignedTransaction> | FailedTransaction>;
readonly postTx: (tx: PostableBytes) => Promise<PostTxResponse>;
  readonly searchTx: (
    query: TransactionQuery,
  ) => Promise<readonly (ConfirmedTransaction<LightTransaction> | FailedTransaction)[]>;
  readonly listenTx: (
    query: TransactionQuery,
  ) => Stream<ConfirmedTransaction<LightTransaction> | FailedTransaction>;
  readonly liveTx: (
    query: TransactionQuery,
  ) => Stream<ConfirmedTransaction<LightTransaction> | FailedTransaction>;
  readonly getFeeQuote: (tx: UnsignedTransaction) => Promise<Fee>;
  readonly withDefaultFee: <T extends UnsignedTransaction>(tx: T) => Promise<T>;
}
```

So far we implement the BCP for two blockchains Ethereum and Lisk



Overview of the Package.json of the iov-lisk package

```
  "dependencies": {
    "@iov/bcp": "^0.14.4",
    "@iov/crypto": "^0.14.4",
    "@iov/dpos": "^0.14.4",
    "@iov/encoding": "^0.14.4",
    "@iov/keycontrol": "^0.14.4",
    "@iov/stream": "^0.14.4",
    "@types/long": "^4.0.0",
    "axios": "^0.19.0",
    "fast-deep-equal": "^2.0.1",
    "long": "^4.0.0",
    "readonly-date": "^1.0.0",
    "xstream": "^11.10.0"
  }
```

Sneak Pick of the iov-lisk of the BCP implementation

Sneak Pick of the iov-lisk of the BCP implementation

```
public async getNonces(_: AddressQuery | PubkeyQuery, count: number): Promise<readonly Nonce[]> {
  const checkedCount = new Uint53(count).toNumber();
  // use unique nonces to ensure the same transaction content leads to a different transaction ID
  // [now-3, now-2, now-1, now] for 4 nonces
  const lastNonce = generateNonce();
  return Array.from({ length: checkedCount }).map((_1, index) => {
    return (lastNonce - (checkedCount - 1 - index)) as Nonce;
  });
}
```

```
export function generateNonce(): Nonce {
  const now = new ReadonlyDate(ReadonlyDate.now());
  return Parse.timeToNonce(now);
}
```

BCP is not only an interface to connect to a blockchain but also to transactions

- send token

- atomic swap transactions

```
/** A swap offer or a counter offer */
export interface SwapOfferTransaction extends LightTransaction {
readonly kind: "bcp/swap_offer";
/**
 * The ID of the swap to aid coordination between the two parties.
 *
 * If required, the data should be generated randomly by the client to avoid
 * collisions.
 *
 * The type of this may be extended with additional properties depending on
 * the requirements of the individual chain.
 */
readonly swapId?: SwapId;
readonly amounts: readonly Amount[];
readonly recipient: Address;
```

BCP atomic swap is fully specifed and implemented in

- Tendermint with the Weave SDK
- Ethereum

What next

- Cosmos integration
- Bitcoin integretion

Thank you!

IOV-core is open-source.

Feel free to try it!

https://github.com/iov-one/iov-core