# Storing data in the Blockchain

## Walkthrough and Use Cases

Jose Aguinaga
Flynt.io

DIGICOMP

canoo [delivering end-user happiness]

{ DEVDAY } by DIGICOMP

# Agenda

Introduction

Blockchain General Concepts

Bitcoin Blockchain

Interacting with the Bitcoin Blockchain

Use Cases

# Introduction

@jjperezaguinaga

Web Engineer

+5 Years Startup experience FinTech

Zürich, México, San Francisco, Bali

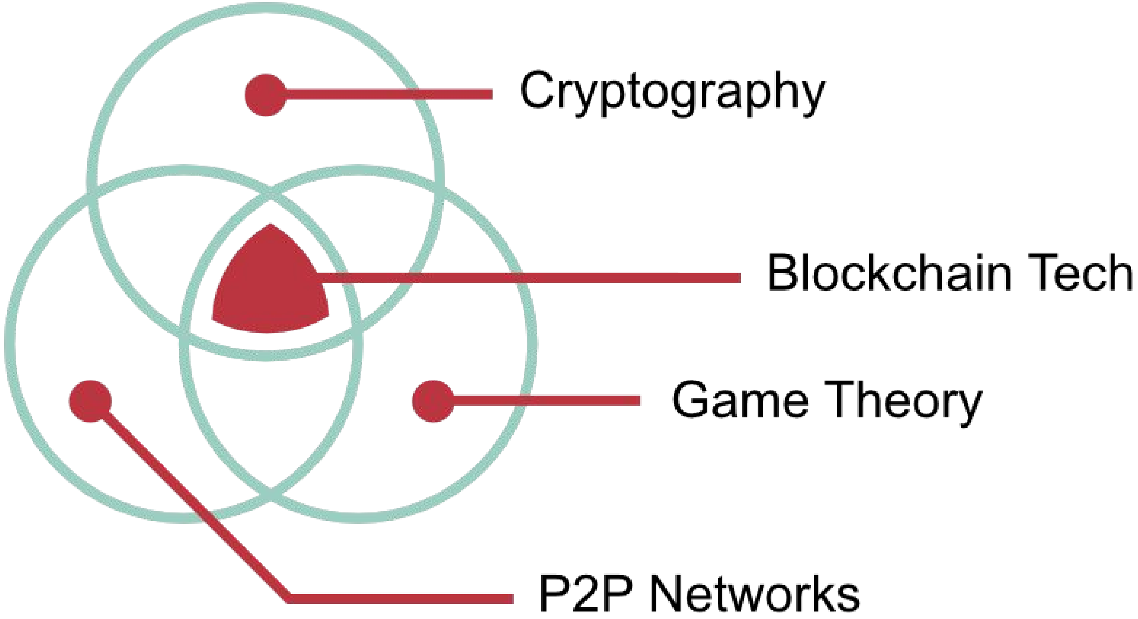
Applied Cryptography

Crypto Valley Active Member / Engineer

Web3 Application Developer

Photo by William Bout on Unsplash

# Blockchain General Concepts



Cryptography

Blockchain Tech

Game Theory

P2P Networks

# Blockchain General Concepts

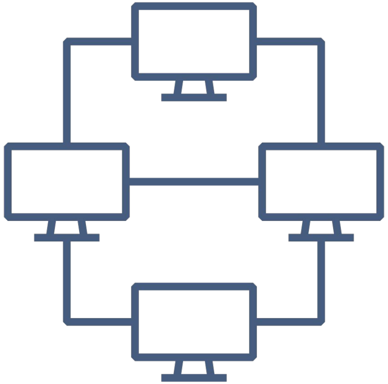
Decentralized

Shared

Public

Transparent

Verifiable



# Blockchain General Concepts

**Decentralized**

Shared

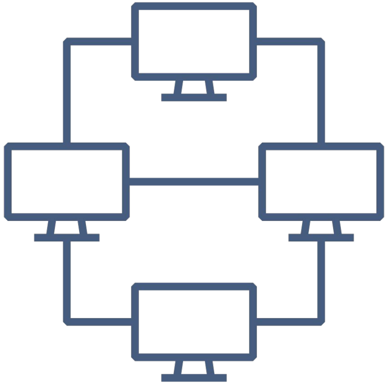
Public

Transparent

Verifiable

**No single point of failure**

**No unique entity controlling network**



# Blockchain General Concepts

Decentralized

**Shared**

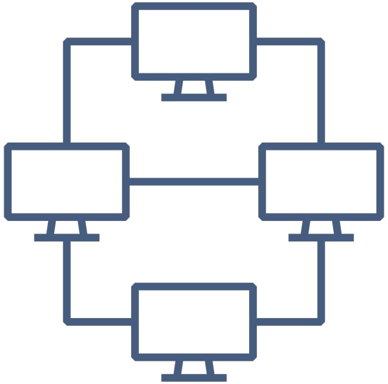
Public

Transparent

Verifiable

**Every node in network shares multiple tasks**

**Computer processing in general is used to reach consensus within network**



# Blockchain General Concepts

Decentralized

Shared

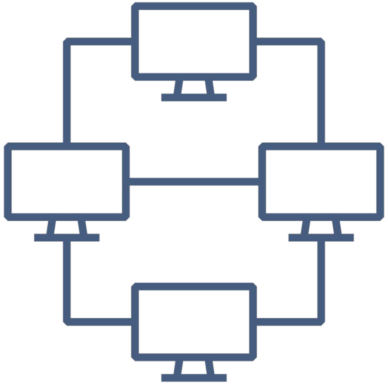
**Public**

Transparent

Verifiable

**Public ledger of transactions for easy audit**

**Every information about each transaction is available to the public**



# Blockchain General Concepts

Decentralized

Shared

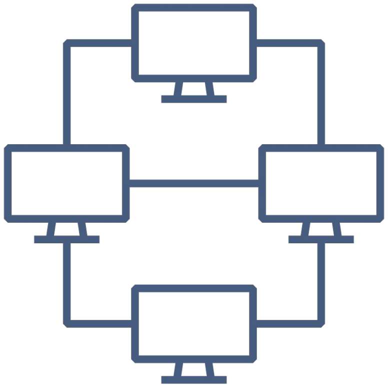
Public

**Transparent**

Verifiable

**No requirements are needed to inspect / audit**

**All protocols had been agreed upon**



# Blockchain General Concepts

Decentralized

Shared

Public

Transparent

**Verifiable**

**Transactions can be verified up to the root block (genesis block)**

**Cryptographic operations ensure integrity**

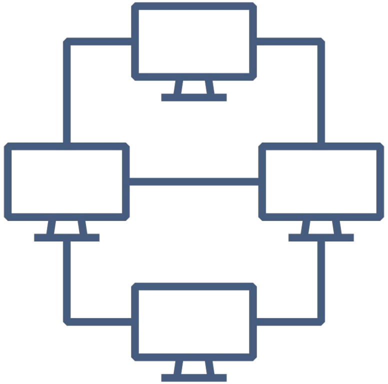


Photo by Tim Evans on Unsplash

# Bitcoin Blockchain

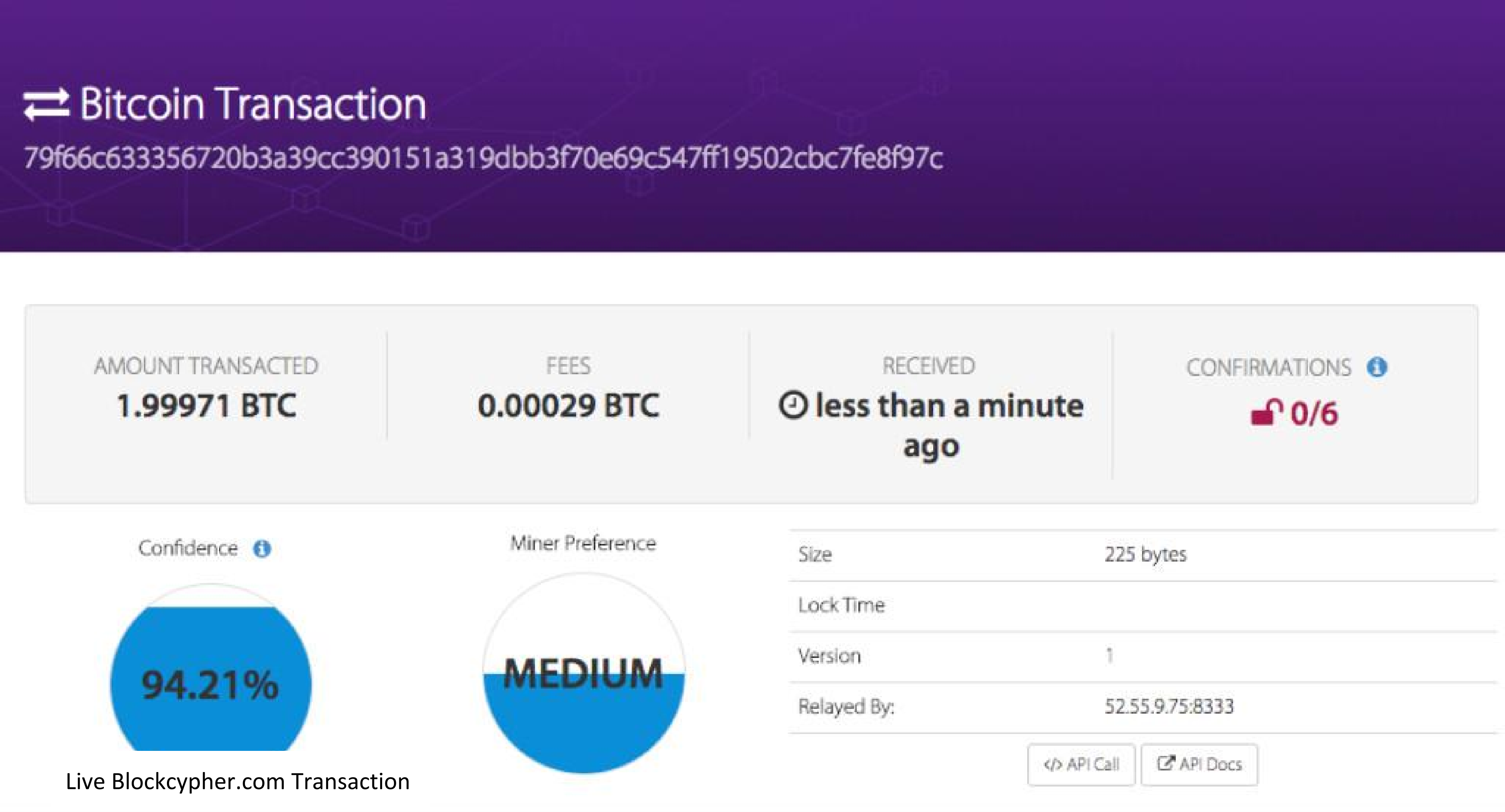
Most popular blockchain

Public and permissionless

Economic incentive

Metadata embeddable

High value, slow, unpredictable



# ⇄ Bitcoin Transaction

79f66c633356720b3a39cc390151a319dbb3f70e69c547ff19502cbc7fe8f97c

| AMOUNT TRANSACTED | FEES | RECEIVED | CONFIRMATIONS |
|---|---|---|---|
| **1.99971 BTC** | **0.00029 BTC** | **less than a minute ago** | **0/6** |

Confidence

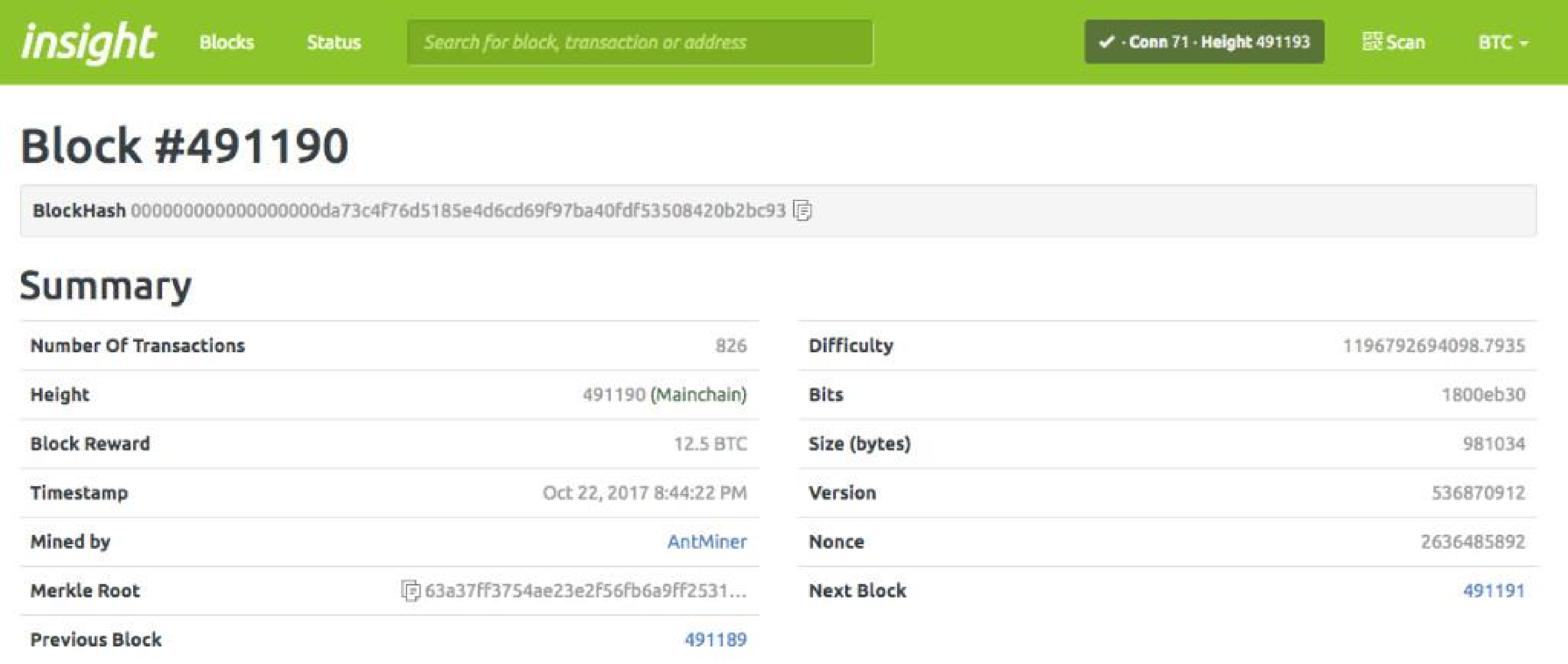
94.21%

Miner Preference

MEDIUM

| | |
|---|---|
| Size | 225 bytes |
| Lock Time | |
| Version | 1 |
| Relayed By: | 52.55.9.75:8333 |

Live Blockcypher.com Transaction



insight
Blocks
Status
Search for block, transaction or address
✓ · Conn 71 · Height 491193
Scan
BTC

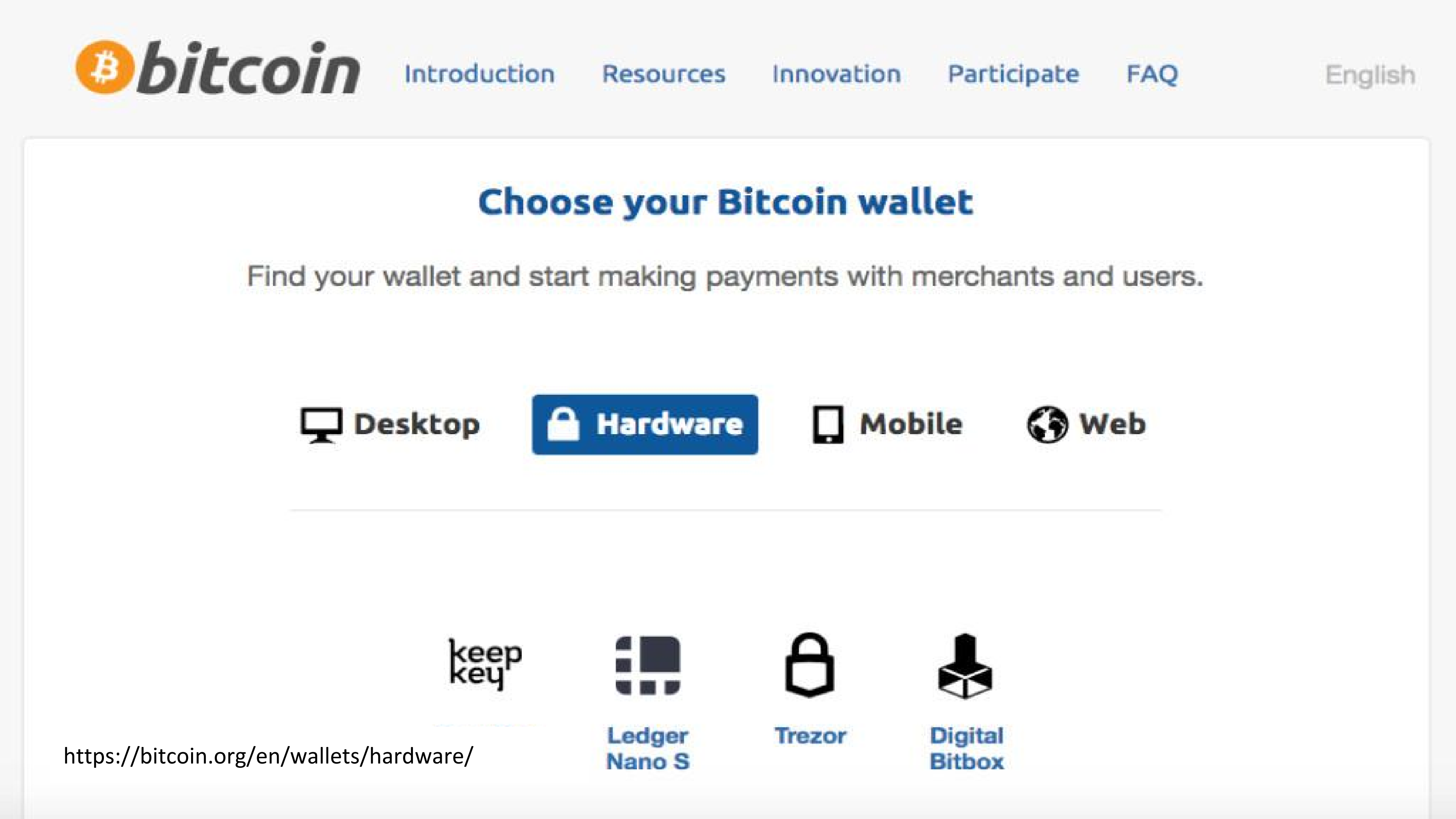
# Block #491190

**BlockHash** 000000000000000000da73c4f76d5185e4d6cd69f97ba40fdf53508420b2bc93

## Summary

| | | | |
|---|---|---|---|
| **Number Of Transactions** | 826 | **Difficulty** | 1196792694098.7935 |
| **Height** | 491190 (Mainchain) | **Bits** | 1800eb30 |
| **Block Reward** | 12.5 BTC | **Size (bytes)** | 981034 |
| **Timestamp** | Oct 22, 2017 8:44:22 PM | **Version** | 536870912 |
| **Mined by** | AntMiner | **Nonce** | 2636485892 |
| **Merkle Root** | 63a37ff3754ae23e2f56fb6a9ff2531... | **Next Block** | 491191 |
| **Previous Block** | 491189 | | |

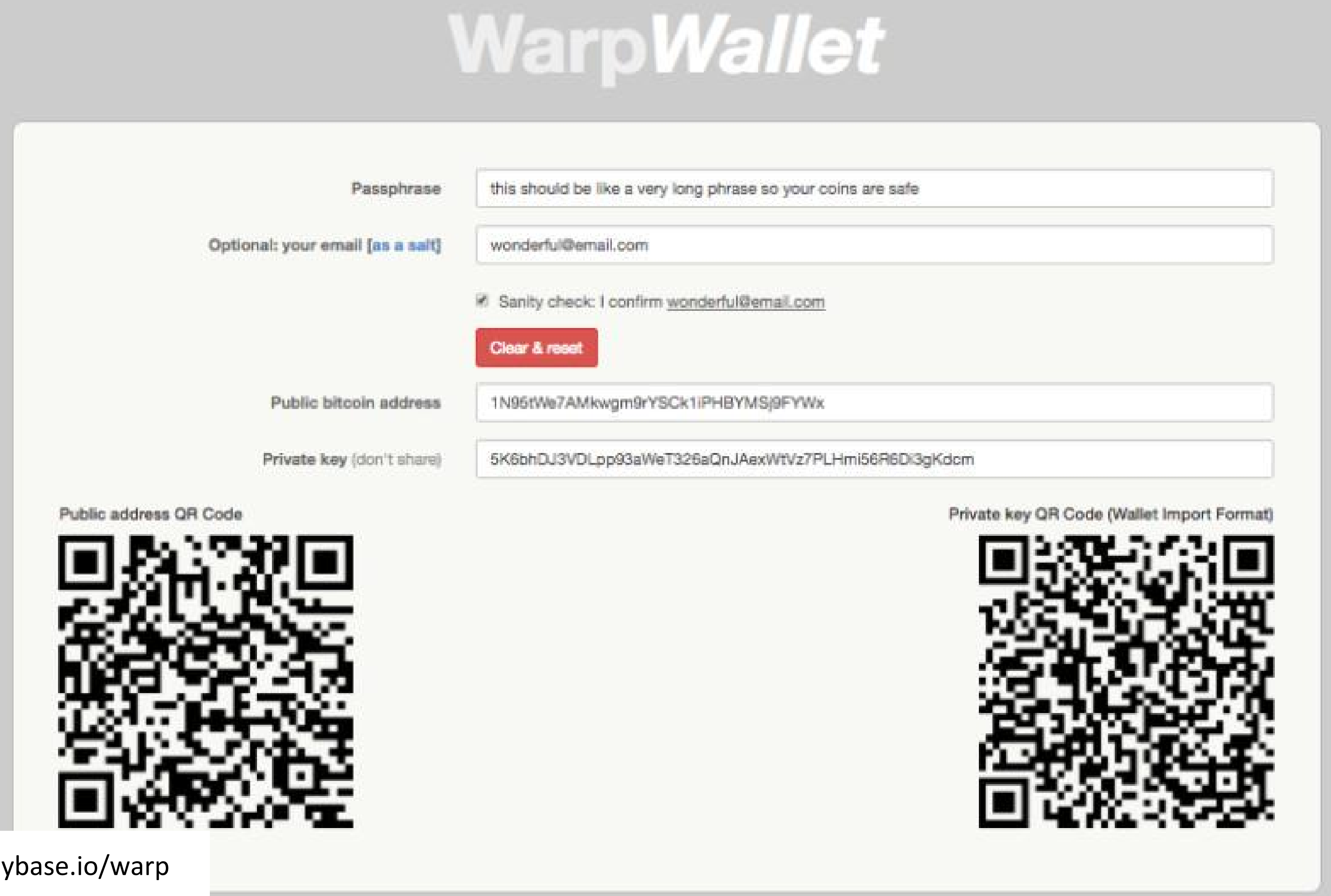
Live Insight.bitpay.com Block



## Choose your Bitcoin wallet

Find your wallet and start making payments with merchants and users.

https://bitcoin.org/en/wallets/hardware/



WarpWallet

Passphrase: this should be like a very long phrase so your coins are safe

Optional: your email [as a salt]: wonderful@email.com

☑ Sanity check: I confirm wonderful@email.com

Public bitcoin address: 1N95tWe7AMkwgm9rYSCk1iPHBYMSj9FYWx

Private key (don't share): 5K6bhDJ3VDLpp93aWeT326aQnJAexWtVz7PLHmi56R6Di3gKdcm

https://keybase.io/warp

# Interacting w/the Bitcoin Blockchain

## Bitcoin APIs / Services

blockcypher, blockchain.info, coinbase, chain.com

## JavaScript Client Libraries

bitpay/bitcore-lib, bitcoinjs/bitcoinjs-lib

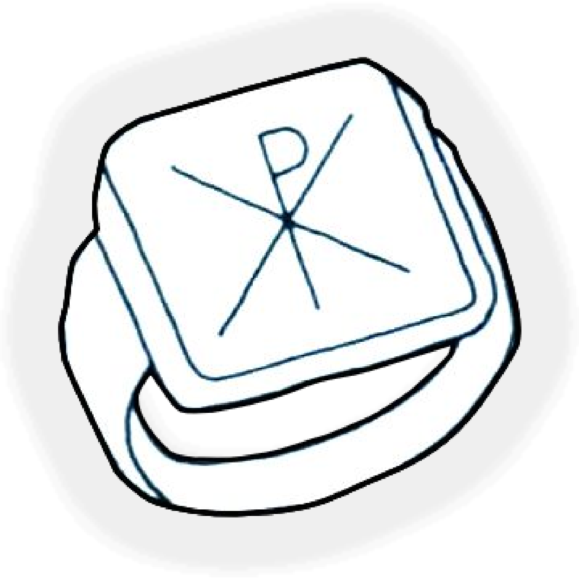
## Blockchain Analysis

live.blockcypher, blockchain.info, insights.bitpay.com

# Interacting w/the Bitcoin Blockchain

**Sealed.website**

Website integrity proof of concept



# Interacting w/the Bitcoin Blockchain

```
const bitcoin = require("bitcoinjs-lib")
// generate random keyPair
const keyPair = bitcoin.ECPair.makeRandom()
// obtain public and private key
const publicAddress = keyPair.getAddress()
const privateKeyWIF = keyPair.toWIF()
```

# Interacting w/the Bitcoin Blockchain

```
const bitcoin = require("bitcoinjs-lib")
// generate random keyPair
const keyPair = bitcoin.ECPair.makeRandom()
// obtain public and private key
const publicAddress = keyPair.getAddress()
const privateKeyWIF = keyPair.toWIF()
```

# Interacting w/the Bitcoin Blockchain

```
const bitcoin = require("bitcoinjs-lib")
// generate random keyPair
const keyPair = bitcoin.ECPair.makeRandom()
// obtain public and private key
const publicAddress = keyPair.getAddress()
const privateKeyWIF = keyPair.toWIF()
```

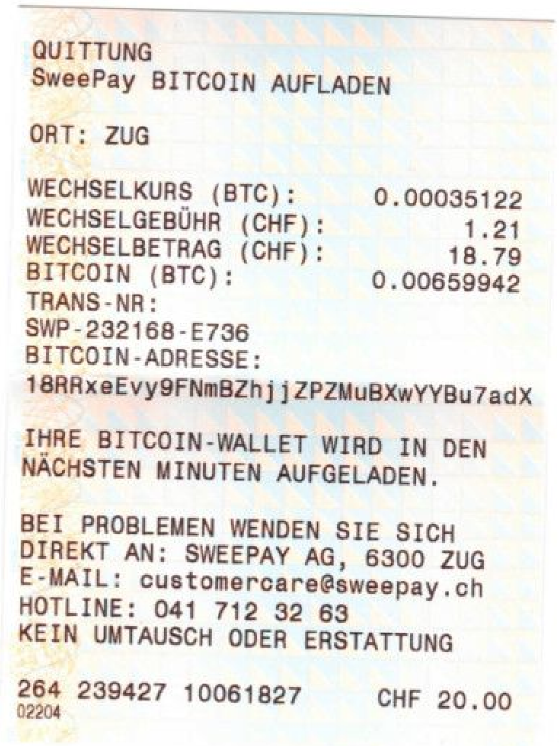
# Interacting w/the Bitcoin Blockchain

```
const bitcoin = require("bitcoinjs-lib")
// generate random keyPair
const keyPair = bitcoin.ECPair.makeRandom()
// obtain public and private key
const publicAddress = keyPair.getAddress()
const privateKeyWIF = keyPair.toWIF()
```

# Interacting w/the Bitcoin Blockchain

**Buy BTC using Public Address**

SBB allows prepaid load through cash or card in train stations



```
QUITTUNG
SweePay BITCOIN AUFLADEN

ORT: ZUG

WECHSELKURS (BTC):          0.00035122
WECHSELGEBÜHR (CHF):              1.21
WECHSELBETRAG (CHF):             18.79
BITCOIN (BTC):              0.00659942
TRANS-NR:
SWP-232168-E736
BITCOIN-ADRESSE:
18RRxeEvy9FNmBZhjjZPZMuBXwYYBu7adX

IHRE BITCOIN-WALLET WIRD IN DEN
NÄCHSTEN MINUTEN AUFGELADEN.

BEI PROBLEMEN WENDEN SIE SICH
DIREKT AN: SWEEPAY AG, 6300 ZUG
E-MAIL: customercare@sweepay.ch
HOTLINE: 041 712 32 63
KEIN UMTAUSCH ODER ERSTATTUNG

264 239427 10061827         CHF 20.00
02204
```

# Interacting w/the Bitcoin Blockchain

```
const blockchainAnchor = require('blockchain-anchor');
const privateKeyWIF = '<YOUR_WIF>';
// setup anchor options to communicate with blockcyper
const anchorOptions = {
  blockchainServiceName: 'blockcypher',
  blockcypherToken: '<YOUR_BLOCKCYPHERTOKEN>'
};
```

# Interacting w/the Bitcoin Blockchain

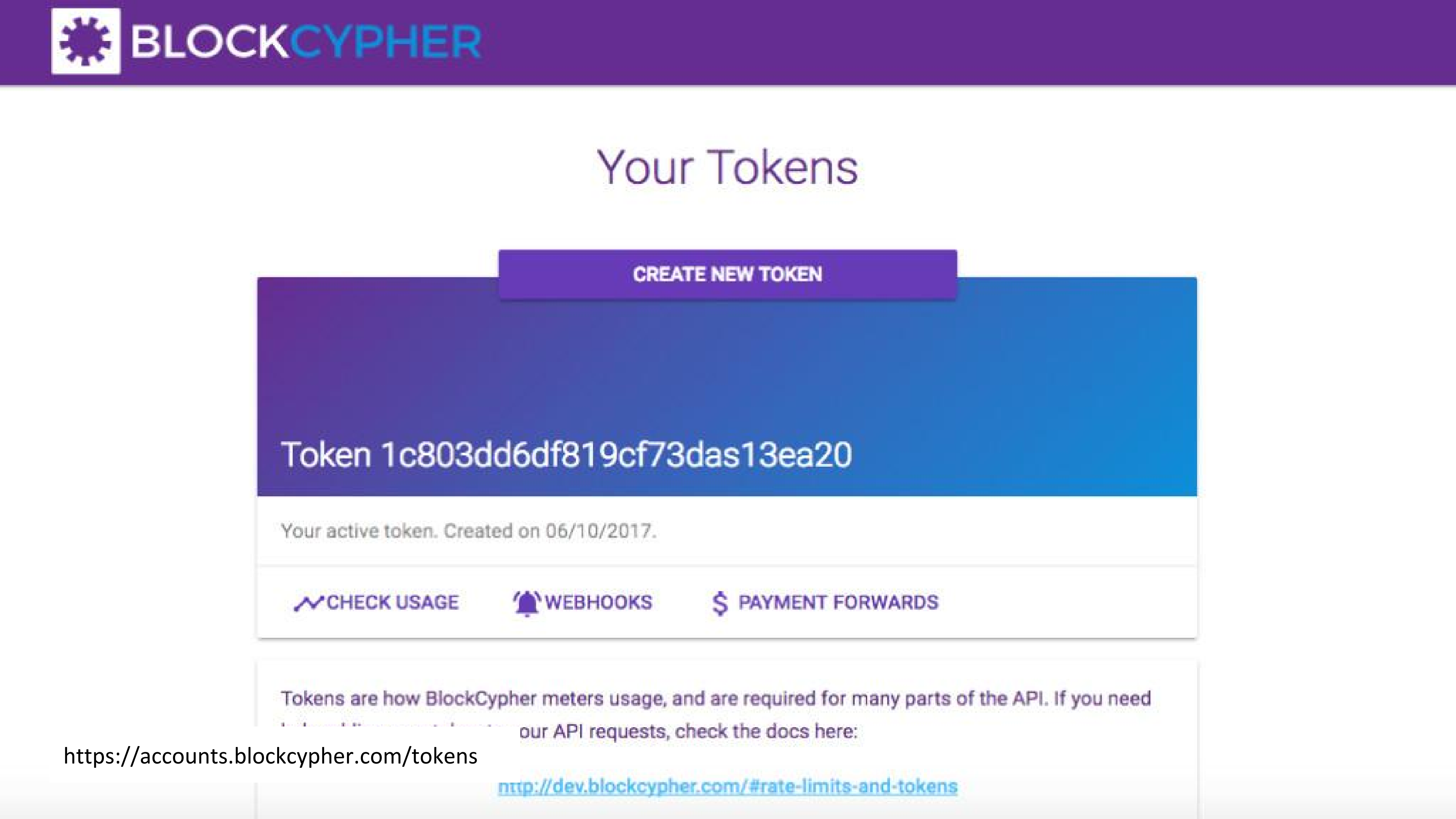
```
const blockchainAnchor = require('blockchain-anchor');
const privateKeyWIF = '<YOUR_WIF>';
// setup anchor options to communicate with blockcyper
const anchorOptions = {
  blockchainServiceName: 'blockcypher',
  blockcypherToken: '<YOUR_BLOCKCYPHERTOKEN>'
};
```

# Interacting w/the Bitcoin Blockchain

```
const blockchainAnchor = require('blockchain-anchor');
const privateKeyWIF = '<YOUR_WIF>';
// setup anchor options to communicate with blockcyper
const anchorOptions = {
  blockchainServiceName: 'blockcypher',
  blockcypherToken: '<YOUR_BLOCKCYPHERTOKEN>'
};
```

# Interacting w/the Bitcoin Blockchain

```
const blockchainAnchor = require('blockchain-anchor');
const privateKeyWIF = '<YOUR_WIF>';
// setup anchor options to communicate with blockcyper
const anchorOptions = {
  blockchainServiceName: 'blockcypher',
  blockcypherToken: '<YOUR_BLOCKCYPHERTOKEN>'
};
```



# Your Tokens

Token 1c803dd6df819cf73das13ea20

Your active token. Created on 06/10/2017.

Tokens are how BlockCypher meters usage, and are required for many parts of the API. If you need

our API requests, check the docs here:

http://dev.blockcypher.com/#rate-limits-and-tokens

https://accounts.blockcypher.com/tokens

# Interacting w/the Bitcoin Blockchain

```
$ curl https://jjperezaguinaga.com \
> | openssl dgst -sha512

d257206f08808bd0bc2a2e6320e47de3d5e...
```

# Interacting w/the Bitcoin Blockchain

```
const anchor = new blockchainAnchor(
    privateKeyWIF,
    anchorOptions
);
const hexData =
"d257206f08808bd0bc2a2e6320e47de3d5e..."
```

# Interacting w/the Bitcoin Blockchain

```
const anchor = new blockchainAnchor(
    privateKeyWIF,
    anchorOptions
);
const hexData =
"d257206f08808bd0bc2a2e6320e47de3d5e..."
```

# Interacting w/the Bitcoin Blockchain

```
const anchor = new blockchainAnchor(
    privateKeyWIF,
    anchorOptions
);
const hexData =
"d257206f08808bd0bc2a2e6320e47de3d5e..."
```

# Interacting w/the Bitcoin Blockchain

```
const anchor = new blockchainAnchor(
    privateKeyWIF,
    anchorOptions
);
const hexData =
"d257206f08808bd0bc2a2e6320e47de3d5e..."
```

# Interacting w/the Bitcoin Blockchain

```
anchor.embed(hexData, function (err, txId, rawTx) {
  if(err) {  console.log('Err', err) } else {
    console.log('New transaction Id = ' + txId);
    console.log('Raw tx = ' + rawTx);
  }
});
```

# Interacting w/the Bitcoin Blockchain

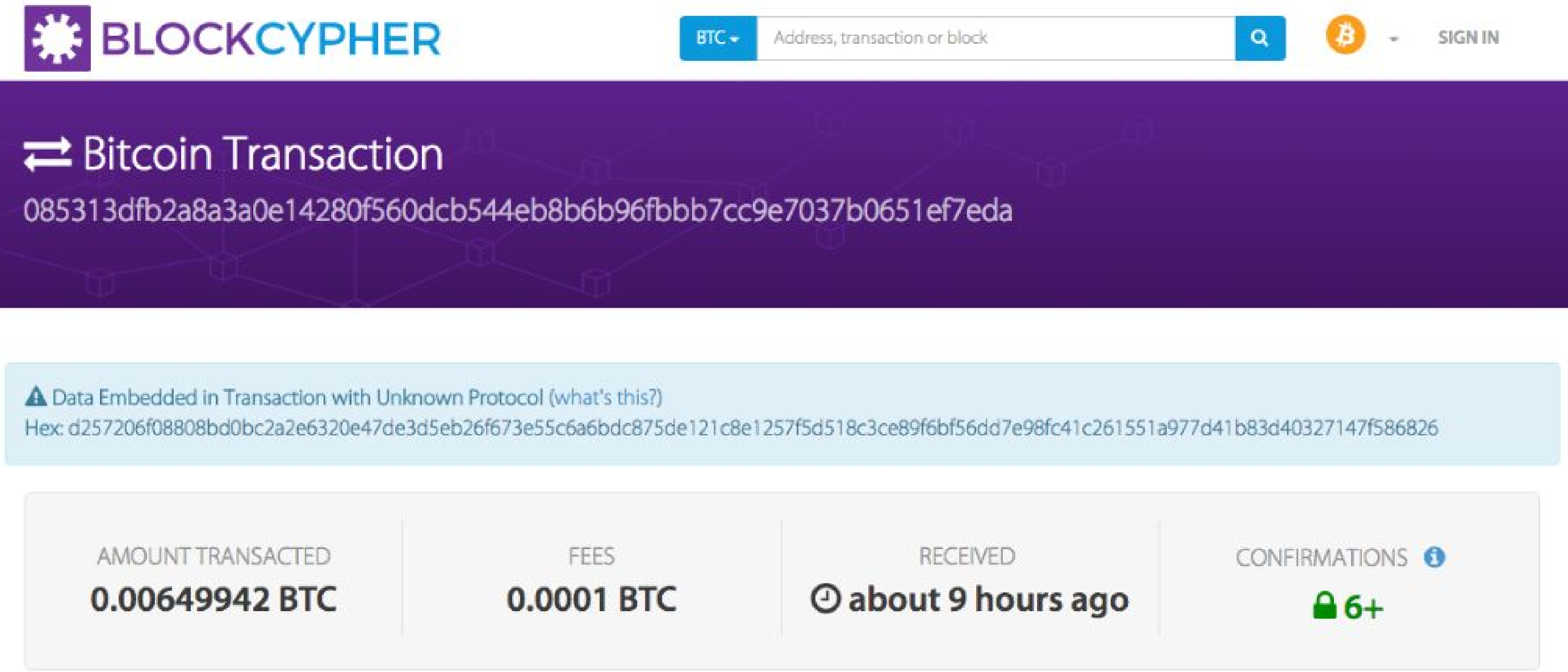
```
anchor.embed(hexData, function (err, txId, rawTx) {
  if(err) {  console.log('Err', err) } else {
    console.log('New transaction Id = ' + txId);
    console.log('Raw tx = ' + rawTx);
  }
});
```

# Interacting w/the Bitcoin Blockchain

```
anchor.embed(hexData, function (err, txId, rawTx) {
  if(err) {  console.log('Err', err) } else {
    console.log('New transaction Id = ' + txId);
    console.log('Raw tx = ' + rawTx);
  }
});
```

# Interacting w/the Bitcoin Blockchain

```
anchor.embed(hexData, function (err, txId, rawTx) {
  if(err) {  console.log('Err', err) } else {
    console.log('New transaction Id = ' + txId);
    console.log('Raw tx = ' + rawTx);
  }
});
```



## Bitcoin Transaction

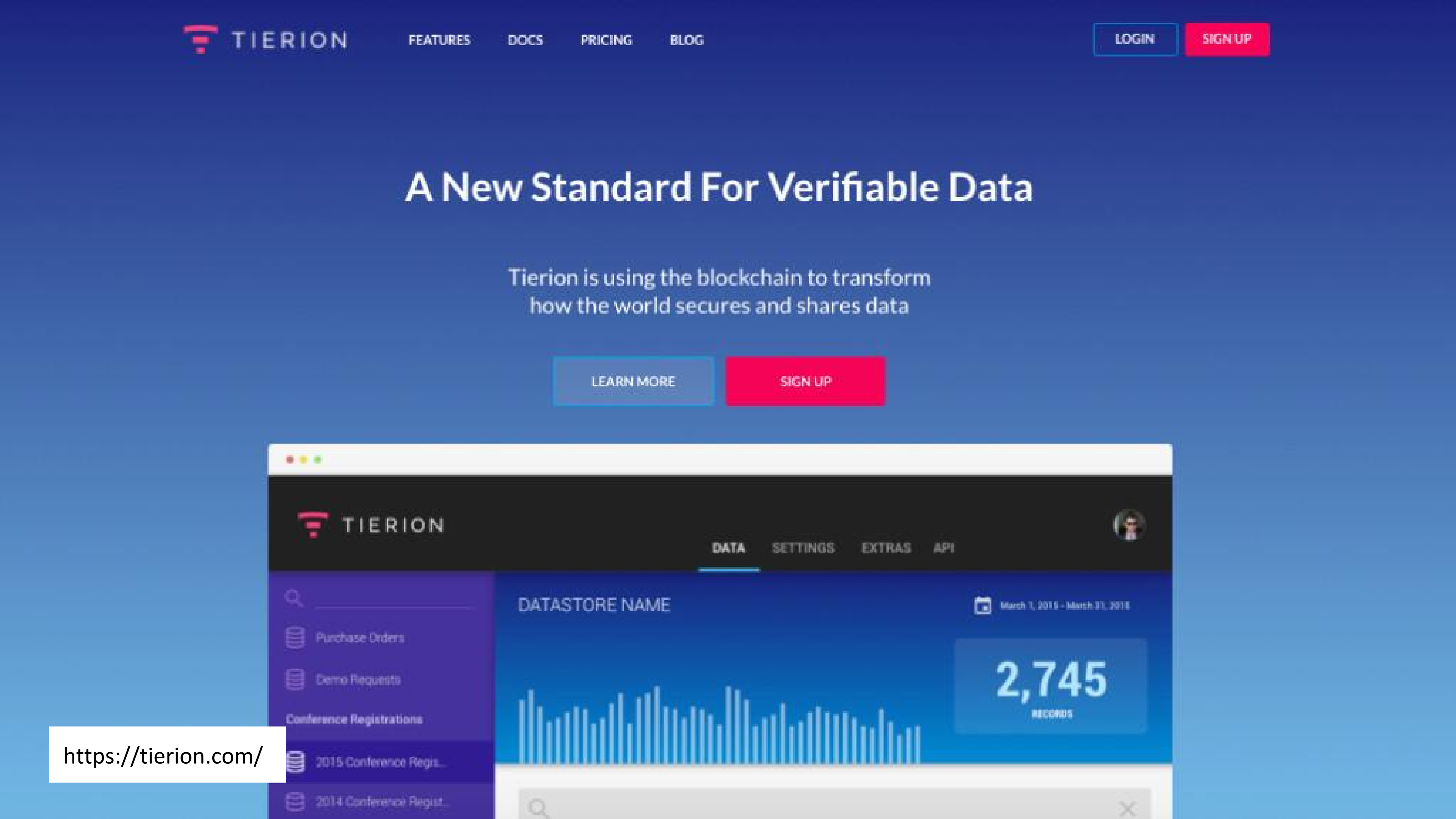
085313dfb2a8a3a0e14280f560dcb544eb8b6b96fbbb7cc9e7037b0651ef7eda

Data Embedded in Transaction with Unknown Protocol (what's this?)

Hex: d257206f08808bd0bc2a2e6320e47de3d5eb26f673e55c6a6bdc875de121c8e1257f5d518c3ce89f6bf56dd7e98fc41c261551a977d41b83d40327147f586826

| AMOUNT TRANSACTED | FEES | RECEIVED | CONFIRMATIONS |
|---|---|---|---|
| 0.00649942 BTC | 0.0001 BTC | about 9 hours ago | 6+ |

https://live.blockcypher.com/btc/tx/085313dfb2a8a3a0e14280f560dcb544eb8b6b96fbbb7cc9e7037b0651ef7eda/



# A New Standard For Verifiable Data

Tierion is using the blockchain to transform how the world secures and shares data

https://tierion.com/

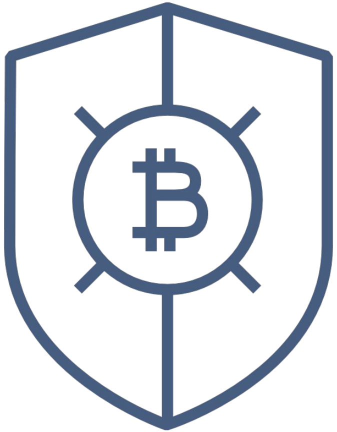
# Use Cases

**Insurance**

Register detailed information about insured item, fill form and register it within the Bitcoin Blockchain. Time of creation can be used to avoid fraud.

# Use Cases: Insurance

```
cat client_1_FordFiesta_2017.pdf \
> | openssl dgst -sha512


eb4917a0944731ca85634c1c17a59b16320...
```



# Use Cases: Insurance

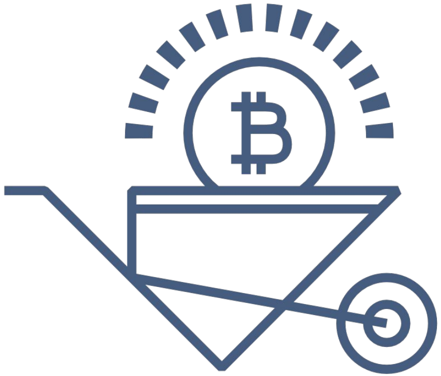
**Existing Project - POEX.IO**

Upload a document and have it certified in the Bitcoin blockchain

# Use Cases

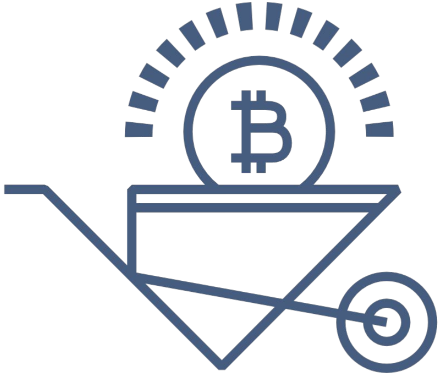
**Provenance / Supply Chain**

Tracks and assets throughout the supply chain by collecting assets defining characteristics, details, and ownership to create a permanent record on the Bitcoin Blockchain



# Use Cases: Provenance / Supply Chain

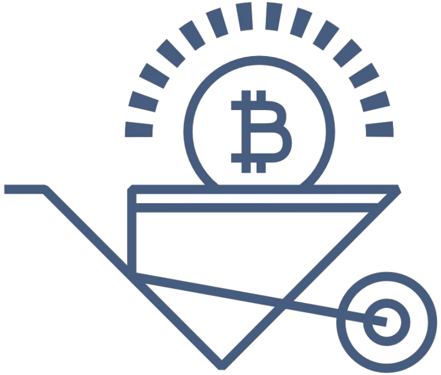
```
cat asset_1_DetailedInfo.pdf \
> | openssl dgst -sha512

c14731ca7a59b1638563c1a094420eb4917...
```



# Use Cases: Provenance / Supply Chain

**Existing Project - Everledger.io**

Track diamonds and other valuable instruments throughout their history in order to certify their value



# Thank you!

Questions and Answers to follow.

Jose Aguinaga
Flynt.io

DIGICOMP

canoo [delivering end-user happiness]

{ DEVDAY } by DIGICOMP