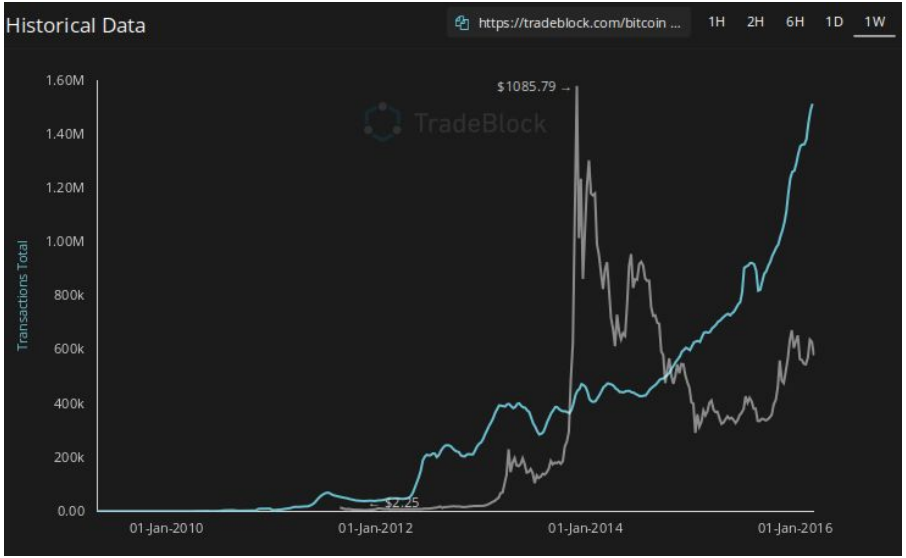
Blockstream

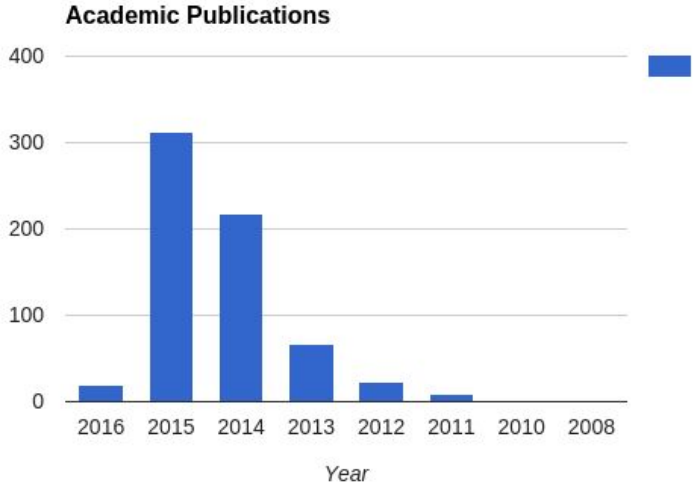
Building the blockchain ecosystem

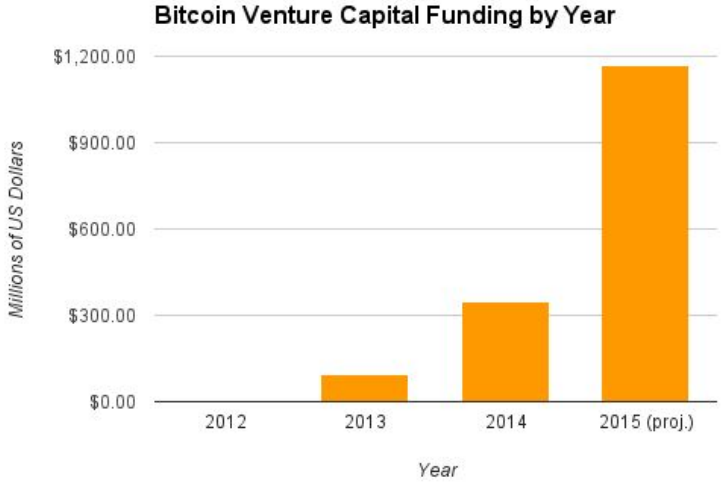
2016-03-11 Jonas Nick jonas@blockstream.com

Bitcoin: A Peer-to-Peer Electronic Cash System

- Solves double spending problem without a trusted third party
- Blockchain: public database of transactions
- Secured by miners
- Controlled inflation via mining reward

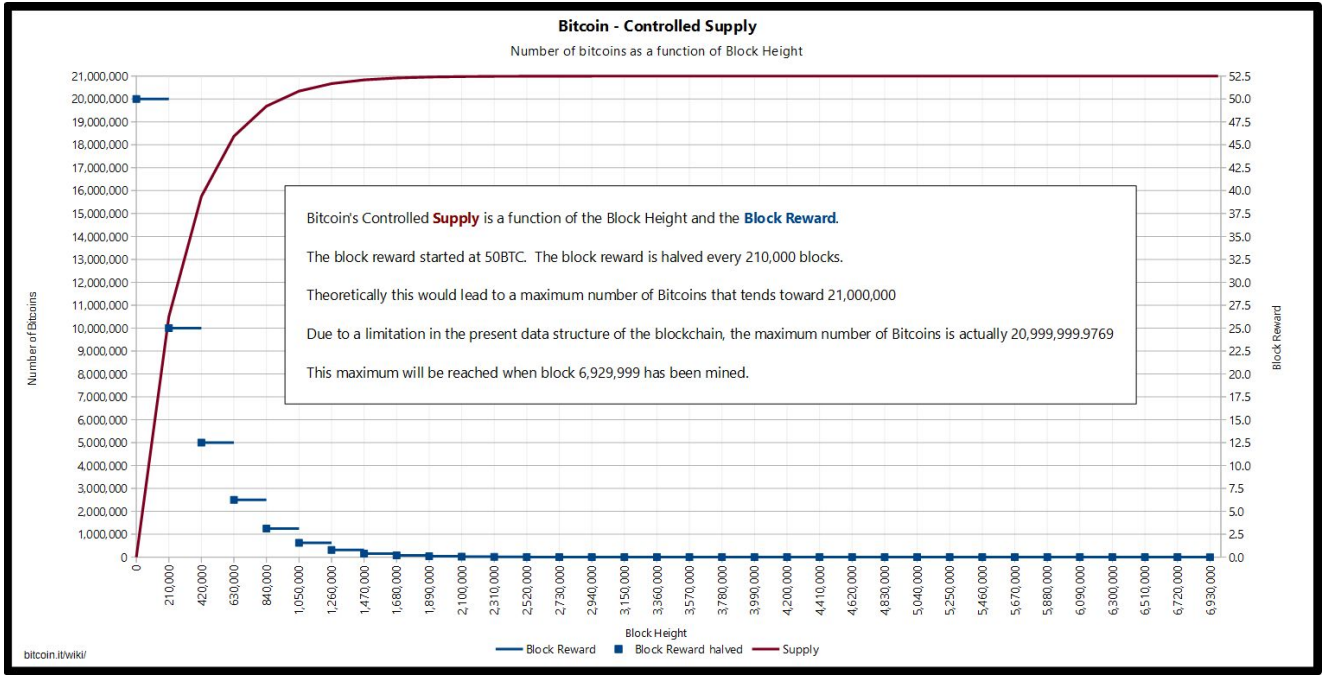

Historical Data
https://tradeblock.com/bitcoin ...
1H
2H
6H
1D
1W
TradeBlock
$1085.79
$2.45
Transactions Total
1.60M
1.40M
1.20M
1.00M
800k
600k
400k
200k
0.00
01-Jan-2010
01-Jan-2012
01-Jan-2014
01-Jan-2016


Academic Publications
400
300
200
100
0
2016
2015
2014
2013
2012
2011
2010
2008
Year

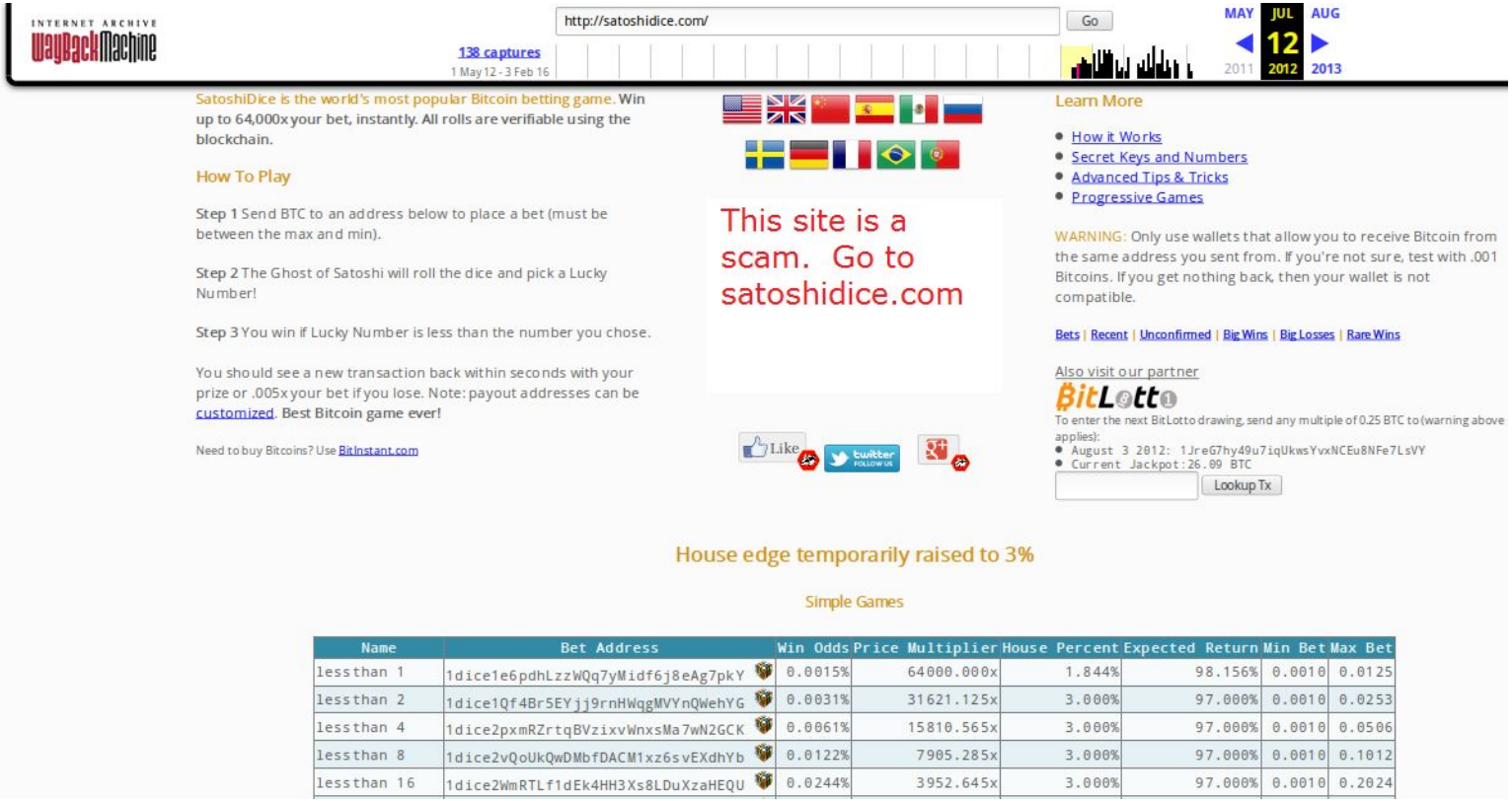

Bitcoin Venture Capital Funding by Year
$1,200.00
$900.00
$600.00
$300.00
$0.00
Millions of US Dollars
2012
2013
2014
2015 (proj.)
Year

Store of value

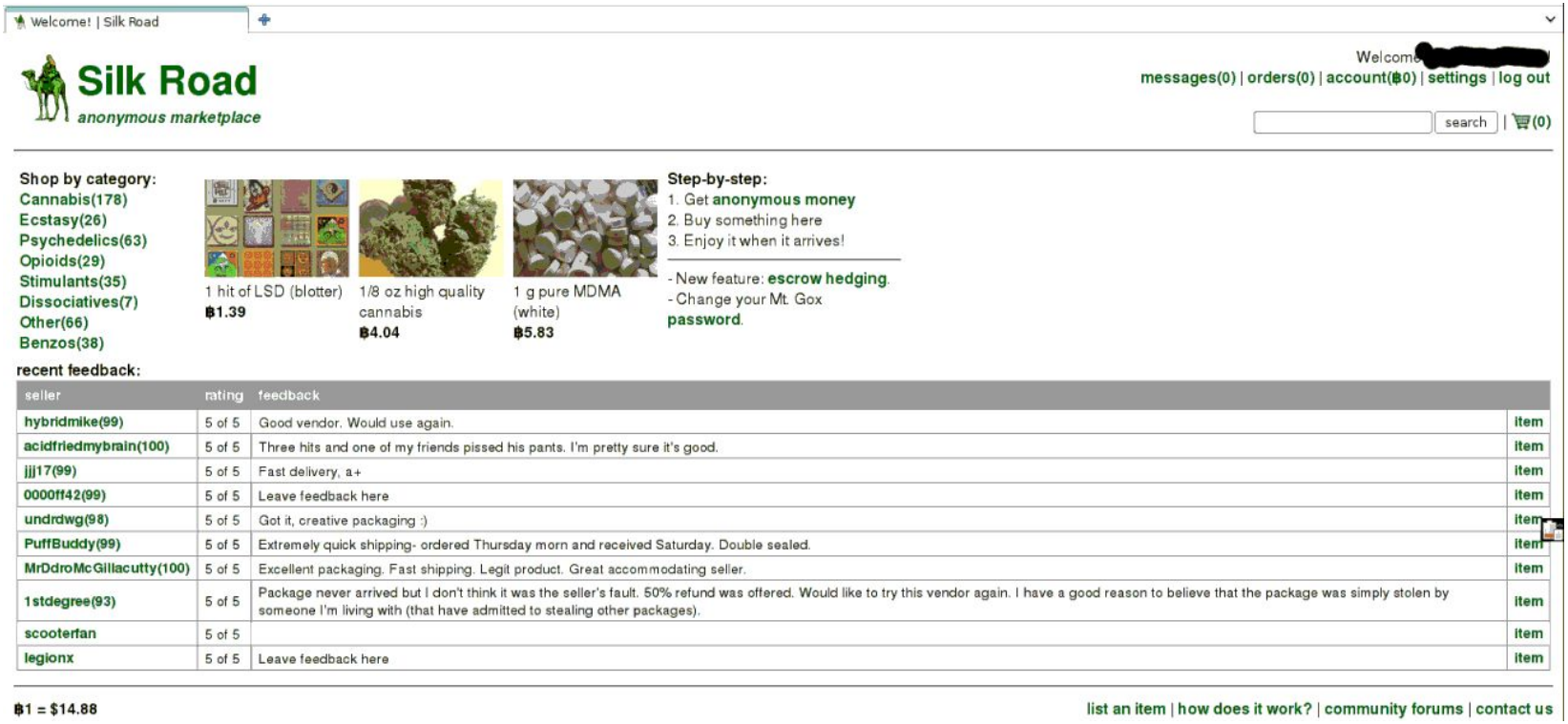
- properties of a currency: scarce, durable, transferable



A Payment System

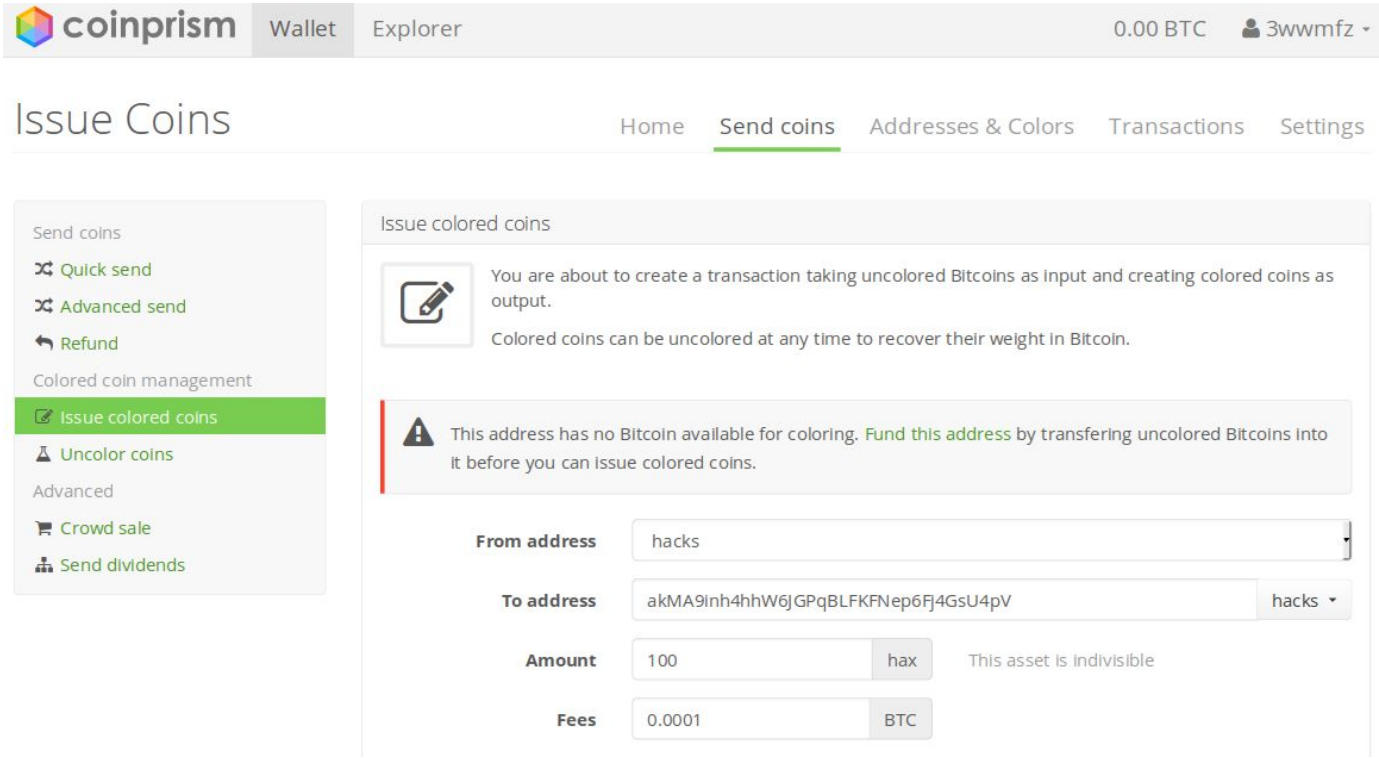


Permissionless Innovation

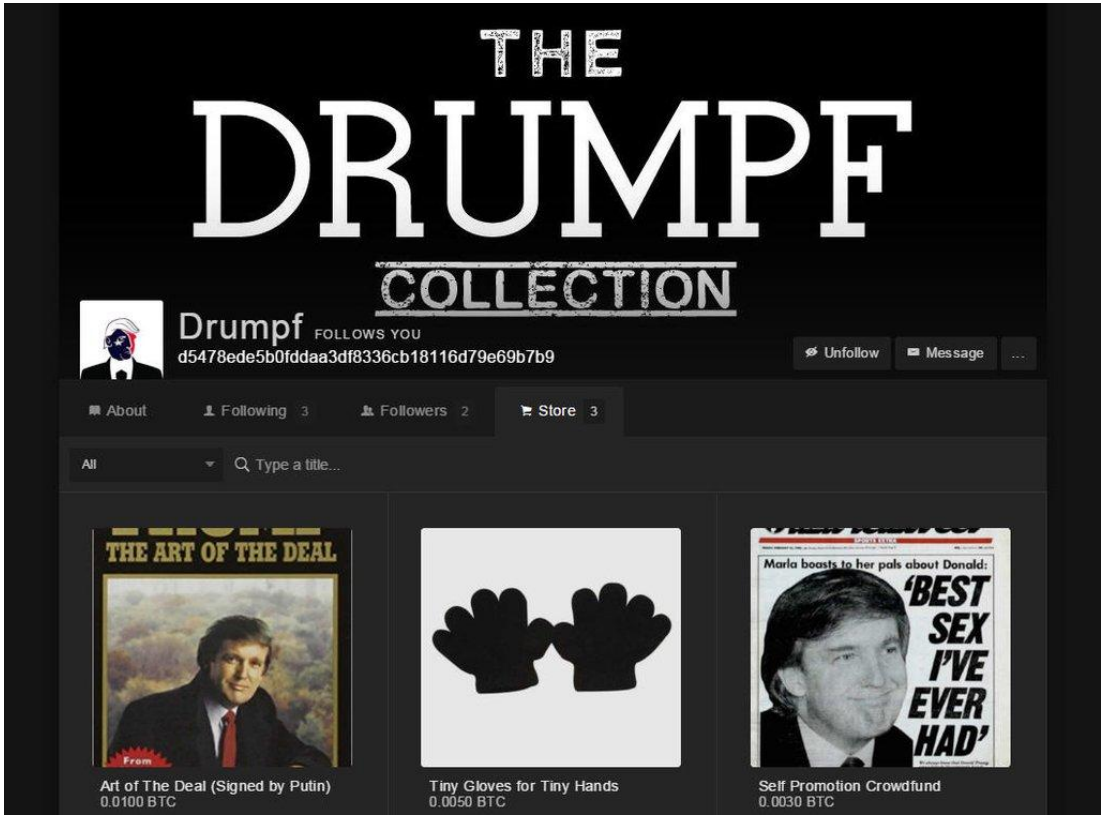


(don’t do that!)

A protocol layer



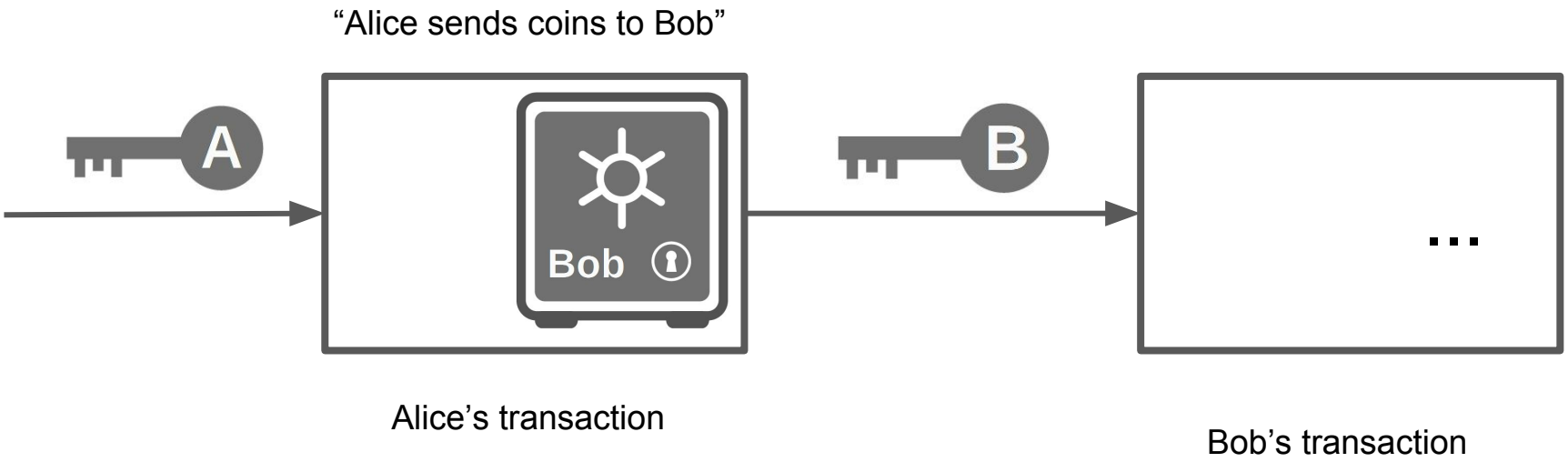
A Smart Contract Platform



Cryptography Basics

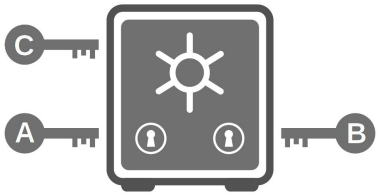
- cryptographic hash functions
  - hash: `{0,1}* -> {0,1}^n`
  - collision resistant
- public key cryptography
  - keypair: secret key `sk` and public key `pk`
  - cryptographic signature over message m
    - `sign(message, sk) -> sig`
    - `verify(message, pk, sig) -> {0, 1}`

Transactions



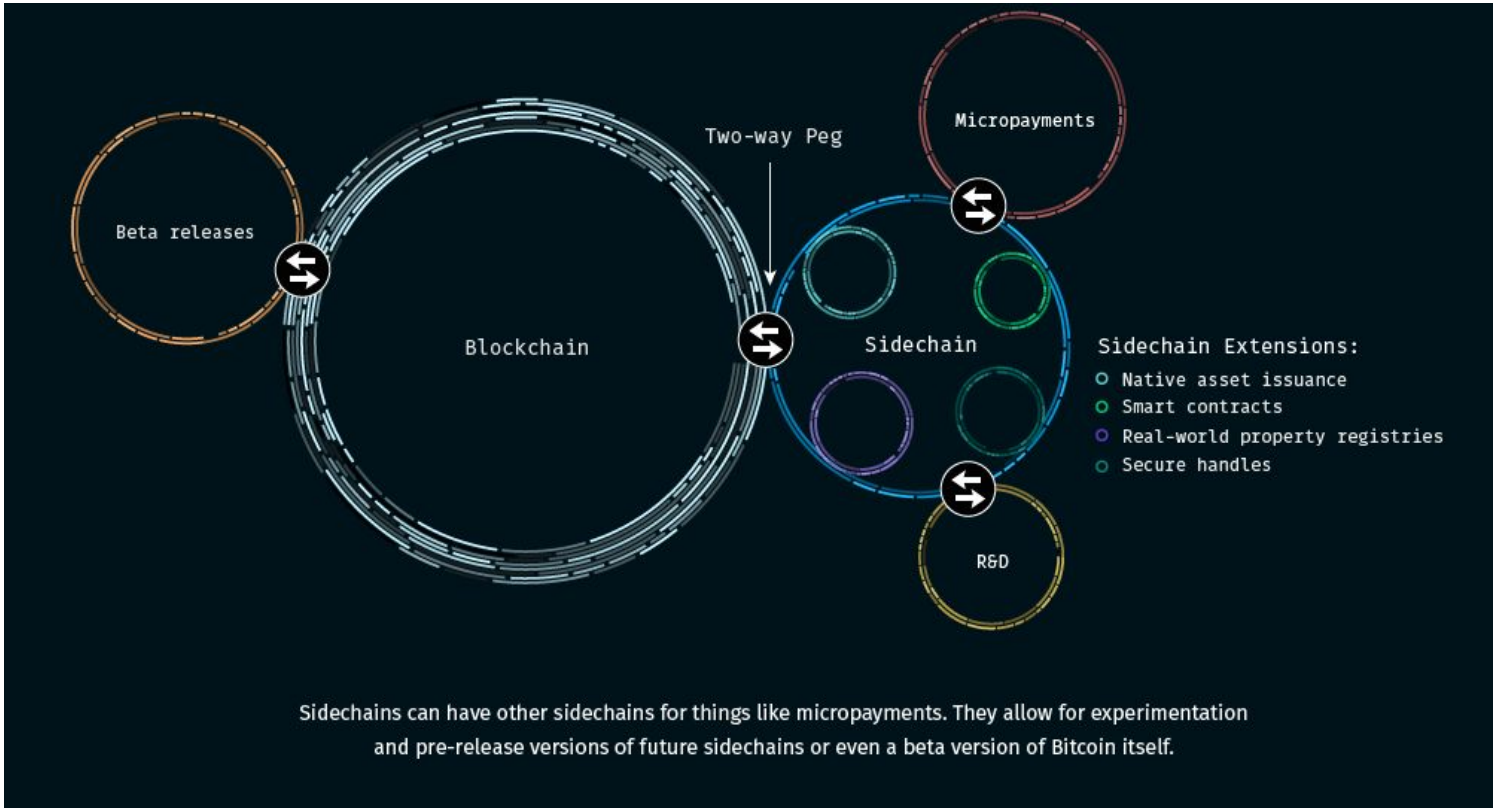
Smart Contract platform

- Transactions contain Bitcoin Script
  - Key: `<Signature>`
  - Safe: `<Public Key> OP_CHECKSIGVERIFY`
- multisig



  - multisig wallets
  - escrow
- sidechains

Interoperable Blockchains



Sidechains

- Use case: Create blockchain with new features
- Altcoins not ideal
  - Network effect
  - Security
- Pegged Sidechains
  - transfer Bitcoins to sidechain and back without trusted third party
  - no separate token, uses Bitcoin mining power
  - federated peg
  - Elements Alpha

Project Inspiration: Build your own blockchain

- Features
  - opcodes for specific protocols, covenants
  - Turing Complete Script Language

(WARNING: insecure and stupid)

```
case OP_ADD:
case OP_SUB:
case OP_BOOLAND:
case OP_BOOLOR:
{
    ...
}

case OP_PYTHON:
{
    if (stack.size() < 1)
        return set_error(serror, SCRIPT_ERR_INVALID_STACK_OPERATION);
    valtype& code = stacktop(-1);
    popstack(stack);
    valtype output = eval(sprintf("python -c %s", code));
    stack.push_back(output);
}
```

src/script/interpreter.cpp

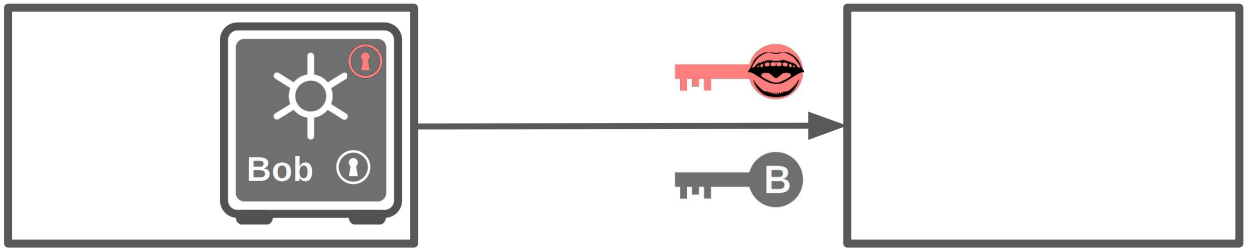
Project Inspiration: Atomic Cross Chain Swap (ACCS)

- Problem: transfer between chains is either centralized or slow
  - implement ACCS protocol to allow trustless transfer between blockchains
  - decentralized exchange
- Coordination layer: “Alice wants exchange Bitcoins on a sidechain with Bob’s zcash coins”

Atomic Cross Chain Swap

sidechain

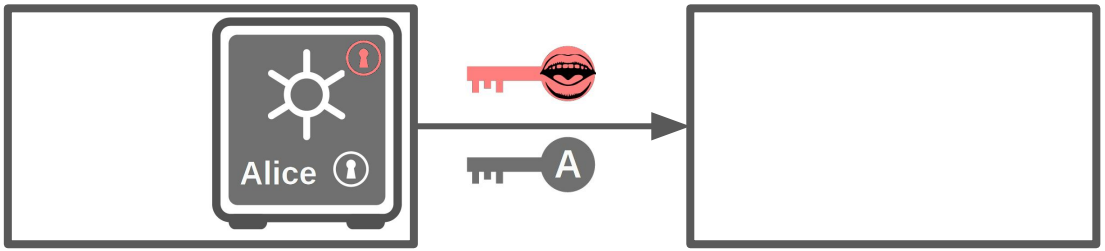
Alice hashes secret:



Alice's transaction

Bob's transaction

zcash chain



Bob's transaction

Alice's transaction

Project Inspiration: Leverage Elements Alpha features

- CT coinjoin
  - coinjoin is mechanism to merge transactions of multiple users into a single one to improve privacy
  - Elements Alpha has Confidential Transactions (CT) which means that transaction values are encrypted
  - CT makes coinjoin much more practical
- Sidechain-aware blockchain analytics
  - visualize peg-specific smart contracts
  - represent chain specific features (Confidential transactions, …)

Resources

- Bitcoin Developer Documentation (RPC API etc.)
  - https://bitcoin.org/en/developer-documentation
- Elements Alpha
  - https://github.com/ElementsProject/elements
  - https://elementsproject.org/
  - Guide http://blog.cryptoiq.ca/?p=395
  - Create new sidechain https://github.com/bitcoin-s/elements#building-a-new-sidechain-with-elements

Resources

- Covenants
  - http://hackingdistributed.com/2016/02/26/how-to-implement-secure-bitcoin-vaults/
- ACCS
  - https://en.bitcoin.it/wiki/Atomic_cross-chain_trading
  - https://bitcointalk.org/index.php?topic=946174.0
- Coinjoin
  - https://bitcointalk.org/index.php?topic=279249.0
  - https://github.com/JoinMarket-Org/joinmarket
- existing block explorers
  - blockchain.info, insight.bitpay.com, tradeblock.com/bitcoin, kaiko.com, blockbin.com, blockseer.com

Contact

- start-hack.slack.com
  - Channel: #blockchain
  - User: jonas
- #sidechains-dev irc channel (user nickler)
- jonas@blockstream.com

- We’re hiring, visit blockstream.com/jobs