



Blockstream

Building the blockchain ecosystem

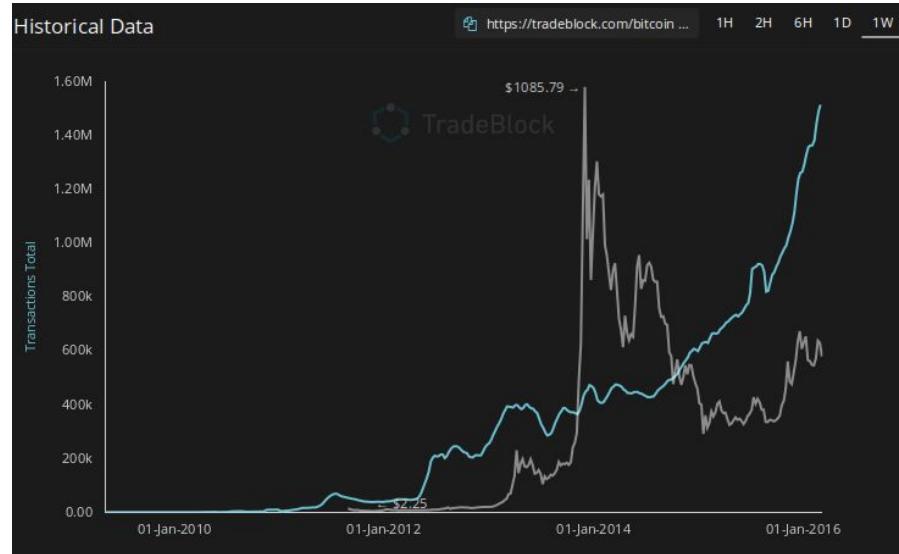
2016-03-11

Jonas Nick

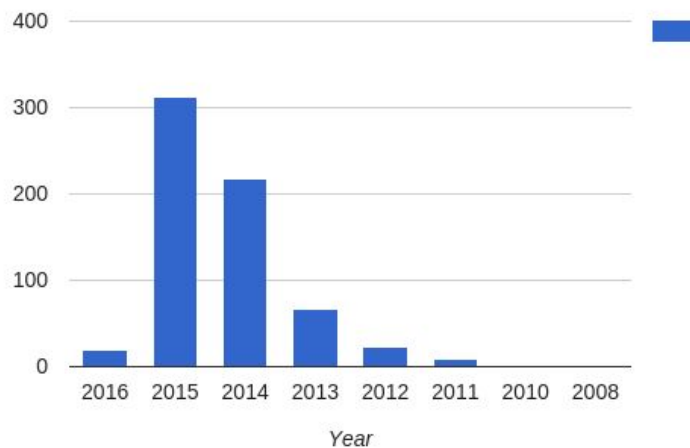
jonas@blockstream.com

Bitcoin: A Peer-to-Peer Electronic Cash System

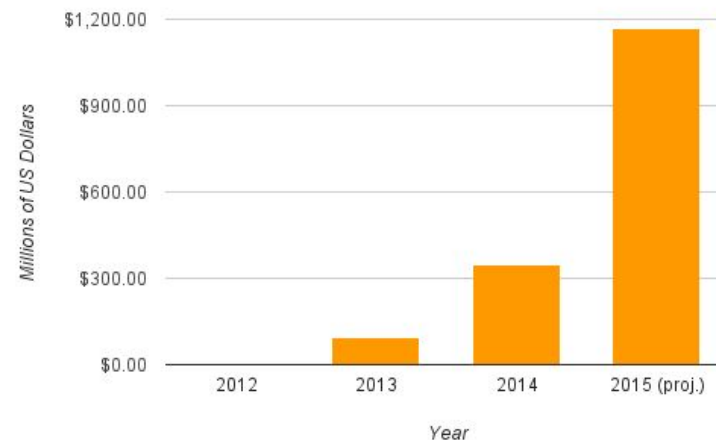
- Solves double spending problem without a trusted third party
- Blockchain: public database of transactions
- Secured by miners
- Controlled inflation via mining reward



Academic Publications

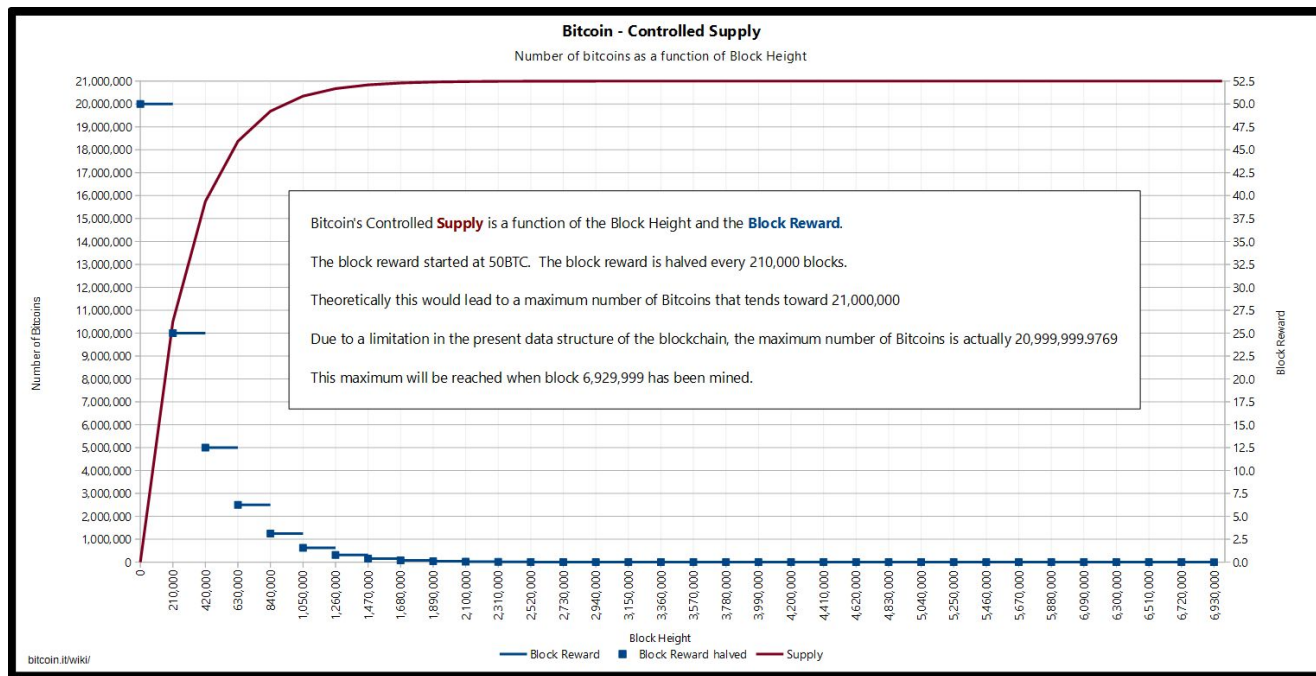


Bitcoin Venture Capital Funding by Year



Store of value

- properties of a currency: scarce, durable, transferable



A Payment System

INTERNET ARCHIVE
Wayback Machine

138 captures
1 May 12 - 3 Feb 16

http://satoshidice.com/

Go

MAY JUL AUG
2011 12 2012 2013

SatoshiDice is the world's most popular Bitcoin betting game. Win up to 64,000x your bet, instantly. All rolls are verifiable using the blockchain.

How To Play

Step 1 Send BTC to an address below to place a bet (must be between the max and min).

Step 2 The Ghost of Satoshi will roll the dice and pick a Lucky Number!

Step 3 You win if Lucky Number is less than the number you chose.

You should see a new transaction back within seconds with your prize or .005x your bet if you lose. Note: payout addresses can be [customized](#). Best Bitcoin game ever!

Need to buy Bitcoins? Use [BitInstant.com](#)

This site is a scam. Go to satoshidice.com

Like

Follow us

Learn More

- [How it Works](#)
- [Secret Keys and Numbers](#)
- [Advanced Tips & Tricks](#)
- [Progressive Games](#)

WARNING: Only use wallets that allow you to receive Bitcoin from the same address you sent from. If you're not sure, test with .001 Bitcoins. If you get nothing back, then your wallet is not compatible.

[Bets](#) | [Recent](#) | [Unconfirmed](#) | [Big Wins](#) | [Big Losses](#) | [Rare Wins](#)

Also visit our partner
BitLotto
To enter the next BitLotto drawing, send any multiple of 0.25 BTC to (warning above applies):
• August 3 2012: 1JreG7hy49u71qUkwsYvxNCEu8NFe7LsVY
• Current Jackpot: 26.00 BTC


House edge temporarily raised to 3%

Simple Games


| Name | Bet Address | Win Odds | Price | Multiplier | House Percent | Expected Return | Min | Bet | Max | Bet |
|--------------|-----------------------------------|----------|------------|------------|---------------|-----------------|--------|-----|-----|-----|
| less than 1 | 1dice1e6pdhLzzWQq7yMidf6j8eAg7pkY | 0.0015% | 64000.000x | 1.844% | 98.156% | 0.0010 | 0.0125 | | | |
| less than 2 | 1dice1Qf4Br5EYjj9rnHWqgMVYnQWehYG | 0.0031% | 31621.125x | 3.000% | 97.000% | 0.0010 | 0.0253 | | | |
| less than 4 | 1dice2pxmRZrtqBVzixvWnxsMa7wN2GCK | 0.0061% | 15810.565x | 3.000% | 97.000% | 0.0010 | 0.0506 | | | |
| less than 8 | 1dice2vQoUkQwDMbfDACM1xz6svEXdhYb | 0.0122% | 7905.285x | 3.000% | 97.000% | 0.0010 | 0.1012 | | | |
| less than 16 | 1dice2WmRTLf1dEk4HH3Xs8LDuXzaHEQU | 0.0244% | 3952.645x | 3.000% | 97.000% | 0.0010 | 0.2024 | | | |

Permissionless Innovation


Welcome! | Silk Road


 **Silk Road**
anonymous marketplace


Welcome [redacted]
messages(0) | orders(0) | account(#0) | settings | log out

search |  (0)

Shop by category:
[Cannabis\(178\)](#)
[Ecstasy\(26\)](#)
[Psychedelics\(63\)](#)
[Opioids\(29\)](#)
[Stimulants\(35\)](#)
[Dissociatives\(7\)](#)
[Other\(66\)](#)
[Benzos\(38\)](#)


1 hit of LSD (blotter)
฿1.39


1/8 oz high quality cannabis
฿4.04


1 g pure MDMA (white)
฿5.83

Step-by-step:
1. Get **anonymous money**
2. Buy something here
3. Enjoy it when it arrives!

- New feature: **escrow hedging**.
- Change your Mt. Gox **password**.

recent feedback:


| seller | rating | feedback | item |
|---|--------|--|----------------------|
| hybridmike(99) | 5 of 5 | Good vendor. Would use again. | item |
| acidfriedmybrain(100) | 5 of 5 | Three hits and one of my friends pissed his pants. I'm pretty sure it's good. | item |
| jjj17(99) | 5 of 5 | Fast delivery, a+ | item |
| 0000ff42(99) | 5 of 5 | Leave feedback here | item |
| undrdwg(98) | 5 of 5 | Got it, creative packaging :) | item |
| PuffBuddy(99) | 5 of 5 | Extremely quick shipping- ordered Thursday morn and received Saturday. Double sealed. | item |
| MrDdroMcGillacutty(100) | 5 of 5 | Excellent packaging. Fast shipping. Legit product. Great accommodating seller. | item |
| 1stdegree(93) | 5 of 5 | Package never arrived but I don't think it was the seller's fault. 50% refund was offered. Would like to try this vendor again. I have a good reason to believe that the package was simply stolen by someone I'm living with (that have admitted to stealing other packages). | item |
| scooterfan | 5 of 5 | | item |
| legionx | 5 of 5 | Leave feedback here | item |

฿1 = \$14.88


[list an item](#) | [how does it work?](#) | [community forums](#) | [contact us](#)

(don't do that!)

A protocol layer

 **coinprism**


Wallet Explorer


0.00 BTC  3wwmfz ▾


Issue Coins

Home Send coins Addresses & Colors Transactions Settings


Send coins


 Quick send

 Advanced send


 Refund


Colored coin management

 Issue colored coins


 Uncolor coins


Advanced

 Crowd sale

 Send dividends

Issue colored coins

 You are about to create a transaction taking uncolored Bitcoins as Input and creating colored coins as output.
Colored coins can be uncolored at any time to recover their weight in Bitcoin.

 This address has no Bitcoin available for coloring. Fund this address by transferring uncolored Bitcoins into it before you can issue colored coins.

From address

hacks

To address

akMA9inh4hhW6jGPqBLKFNe6Fj4GsU4pV

hacks ▾

Amount

100

hax

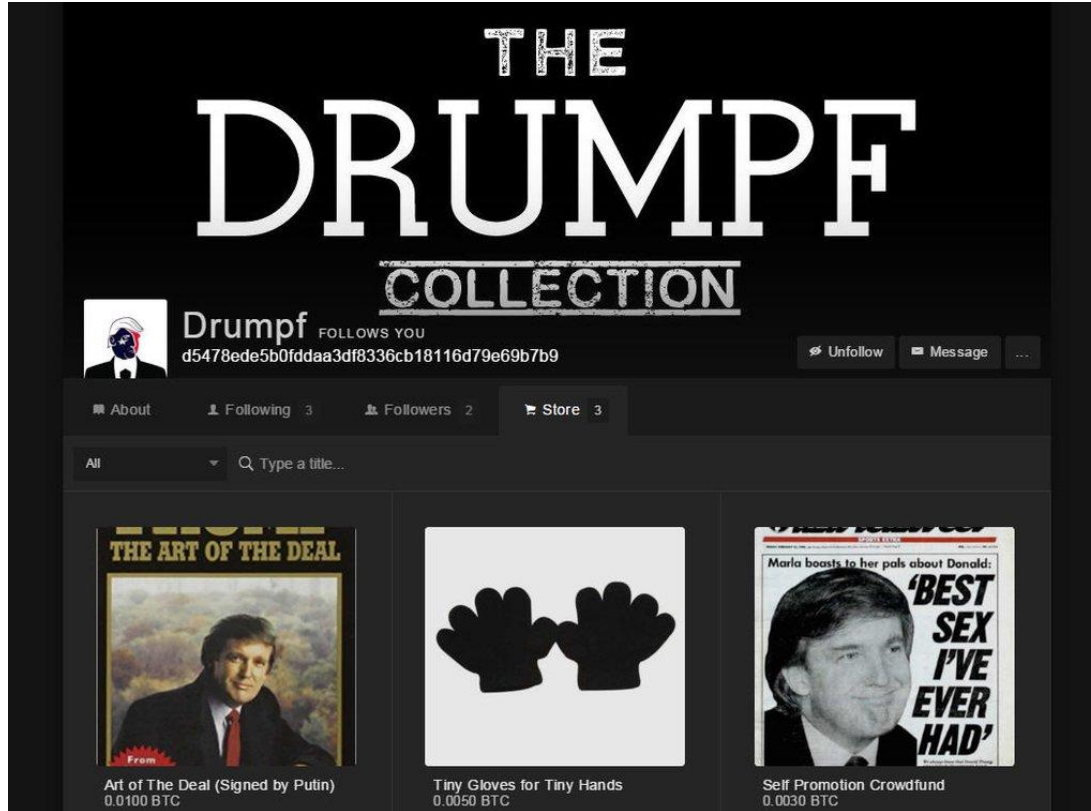
This asset is indivisible

Fees

0.0001

BTC

A Smart Contract Platform

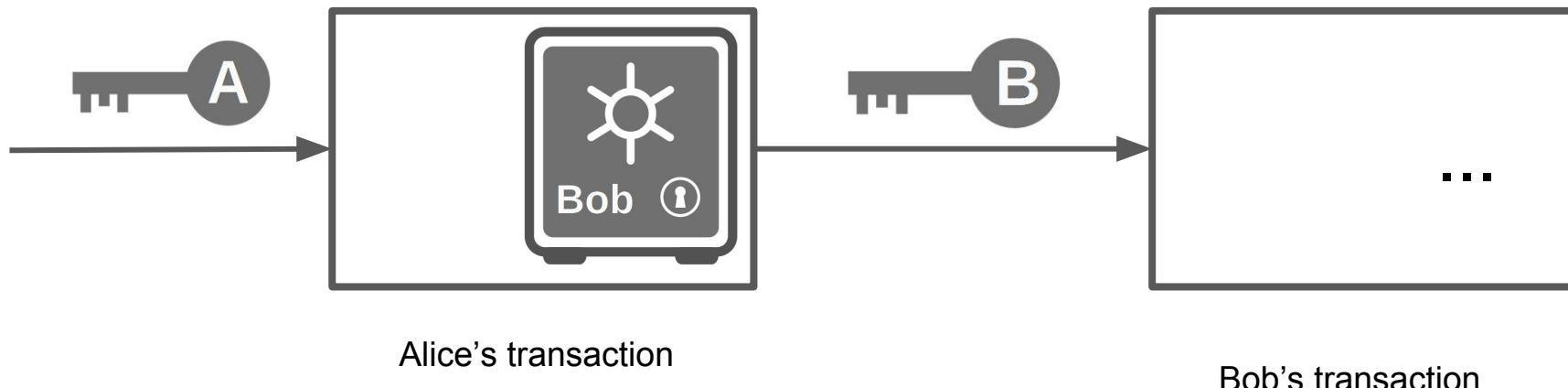


Cryptography Basics

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

Transactions

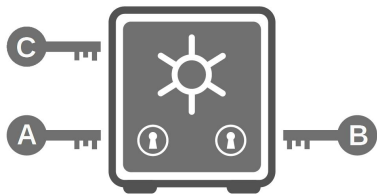
“Alice sends coins to Bob”



Smart Contract platform

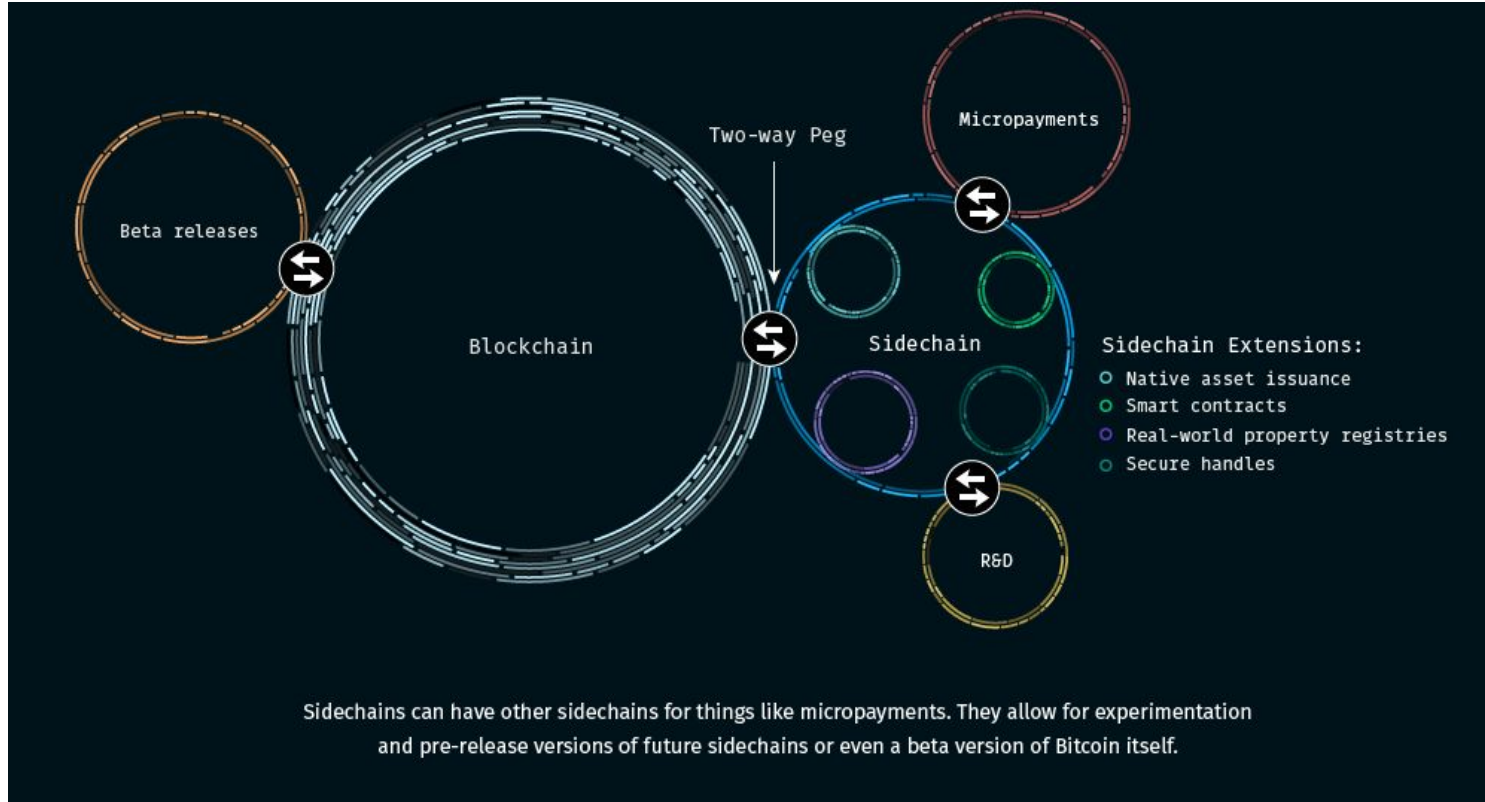
- Transactions contain Bitcoin Script
 - Key: <Signature>
 - Safe: <Public Key> OP_CHECKSIGVERIFY

- 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:
{
    ...
}

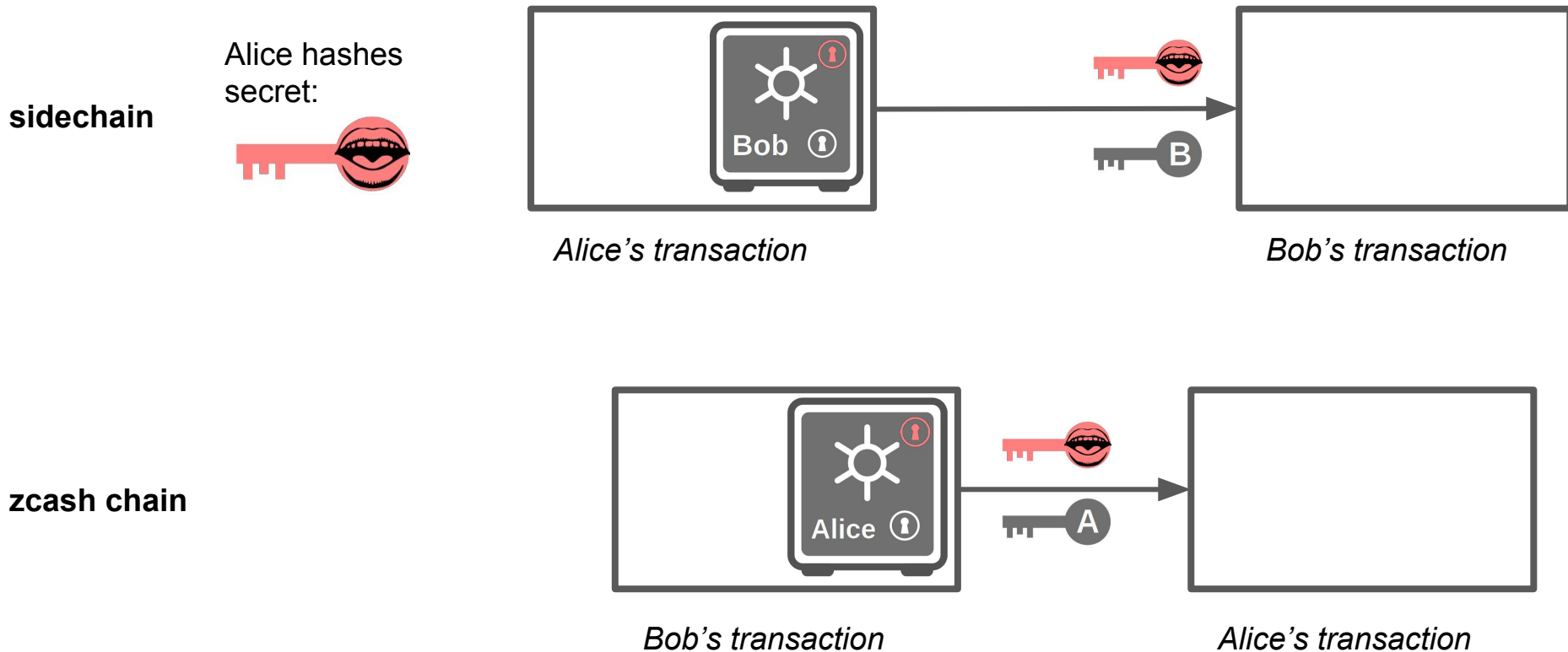
case OP_PYTHON:
{
    if (stack.size() < 1)
        return set_error(error, SCRIPT_ERR_INVALID_STACK_OPERATION);
    valtype& code = stacktop(-1);
    popstack(stack);
    valtype output = eval(sprintf("python -c %s", code));
    stack.push_back(output);
}
```

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



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