Class 21: Scaling Bitcoin & ~~Web~~ ~~Bitcoin~~ Blockchain 2.0

Nick Skelsey & Alex Kuck – Cofounders @ Soapbox Systems

Why are we here?

UVA is great

We TA’d this class

Dave asked us

No VC funding

We are hiring

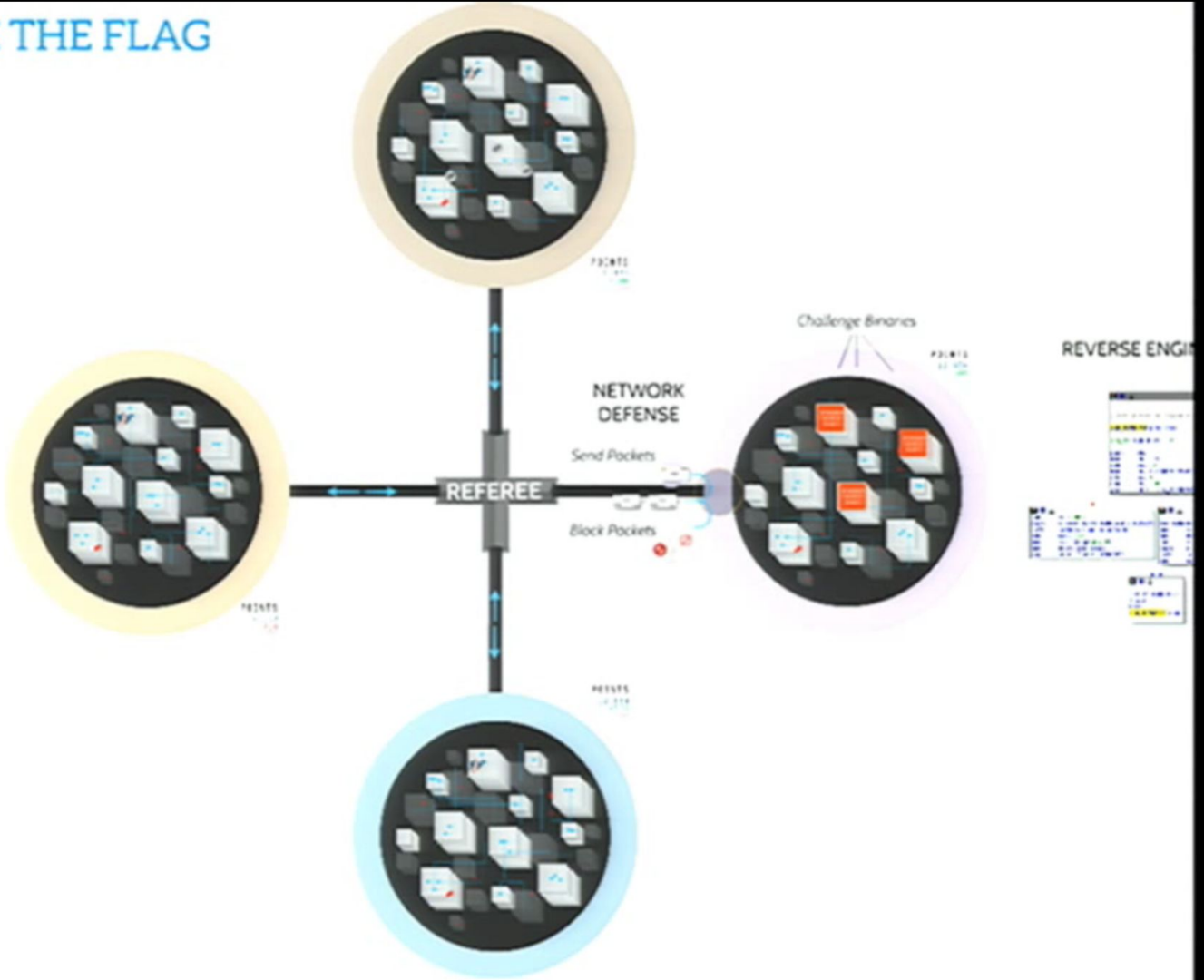
Who are we?

University of Virginia Engineering — Department of Computer Science

The TECHx team consists of leading software analysis experts from GrammaTech, Inc. and the University of Virginia. The team is led by Dr. David Melski (PI) and Professors Jack Davidson and John Knight (co-PIs). GrammaTech and UVA are co-developers of an automatic software-hardening technology called PEASOUP ("Preventing Exploits of Software Of Uncertain Provenance"). PEASOUP uses a combination of automatic binary analysis, repair, confinement and diversification to prevent exploits of important classes of vulnerabilities, including those based on memory-safety, command-injection, and number-handling weaknesses.

CGC CYBER GRAND_CHALLENGE

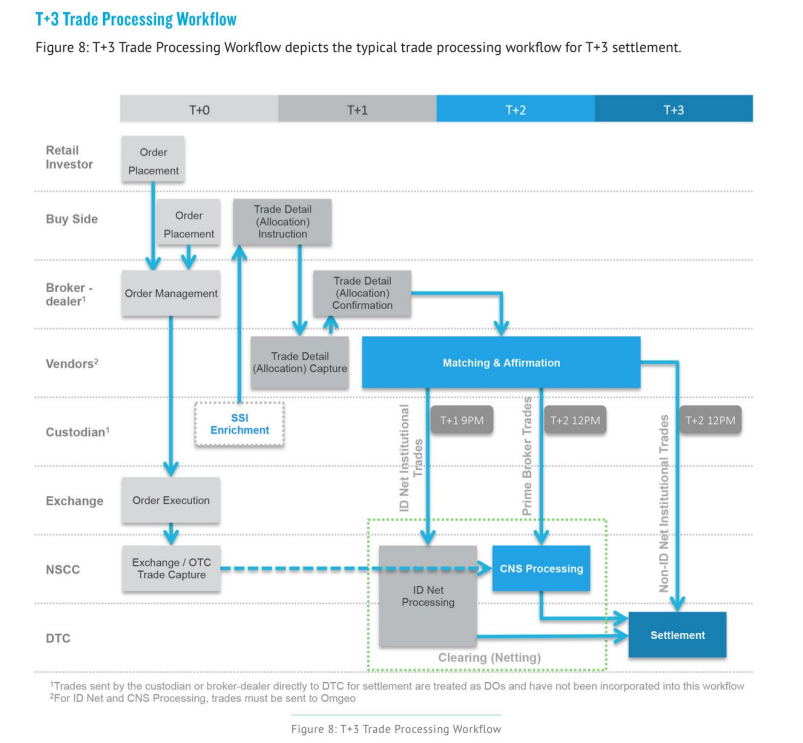
CAPTURE THE FLAG



CTF is way cooler than Bitcoin

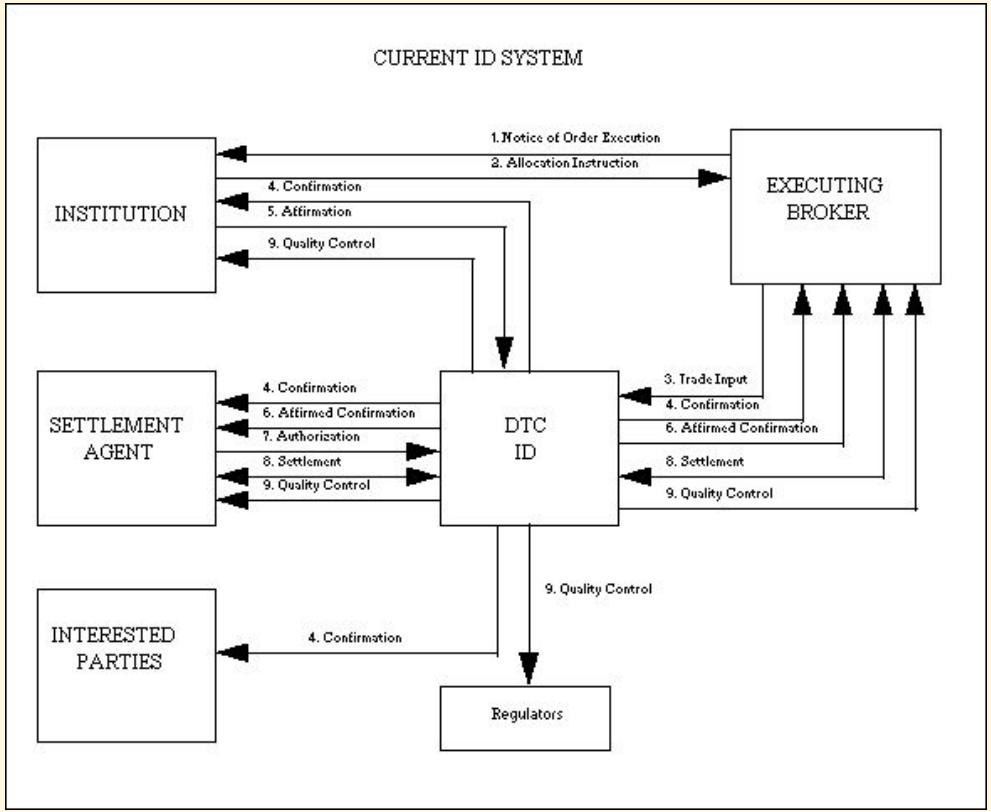
Scaling Bitcoin as an inter-bank inter-national settlement system

Selling a stock takes three days



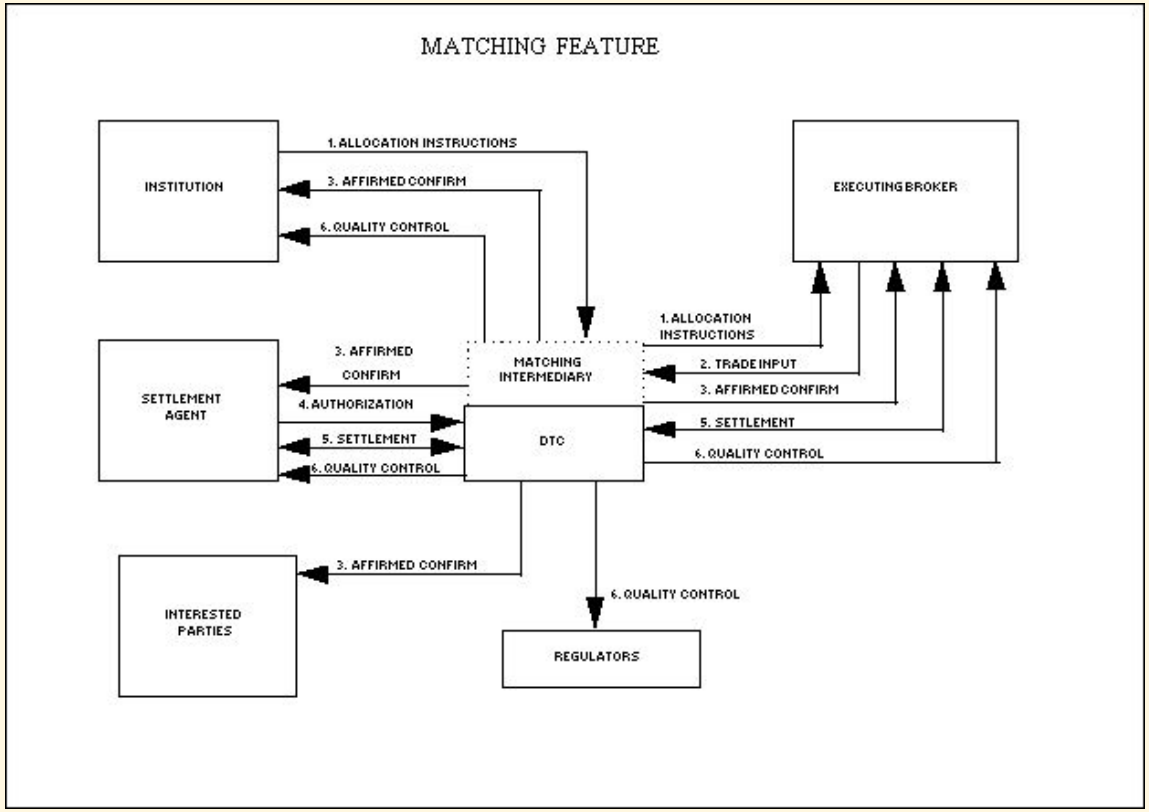
From ust2.com

Settling ownership of stocks today (T+3)



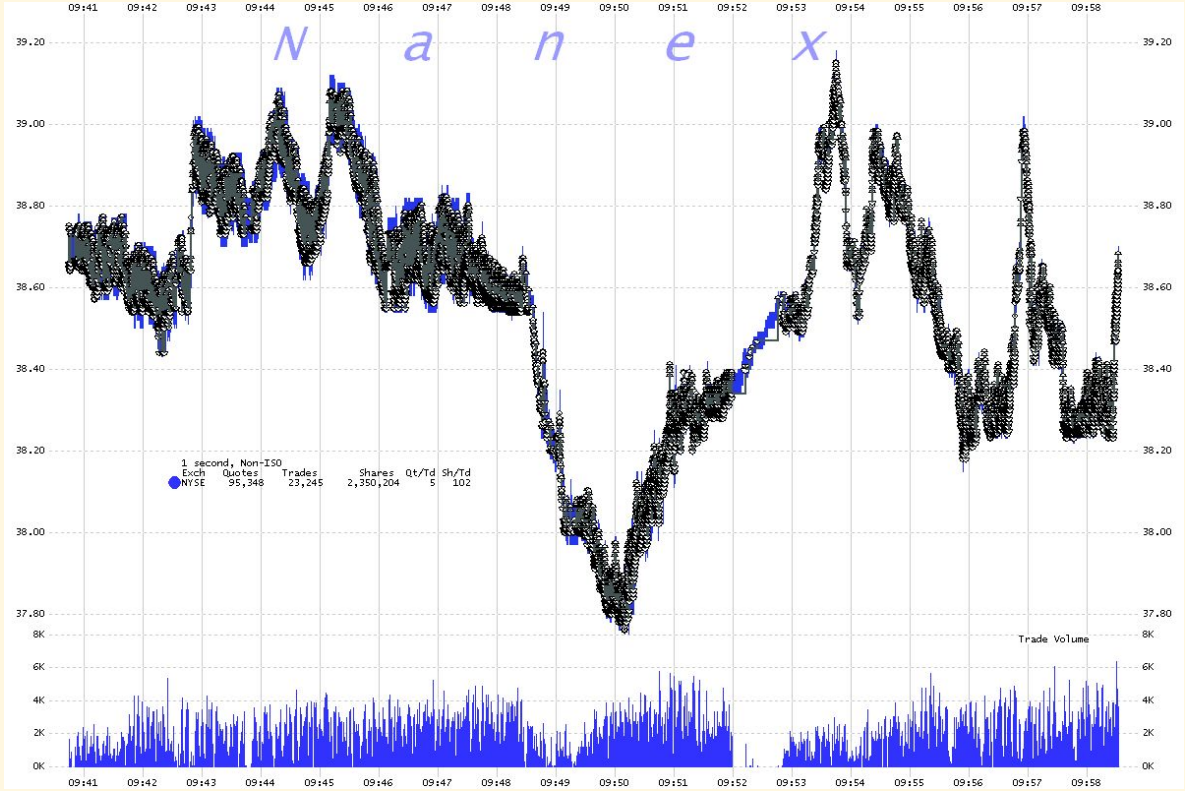
From SECURITIES AND EXCHANGE COMMISSION
17 CFR PART 241

Settling ownership of stocks tomorrow (T+2)

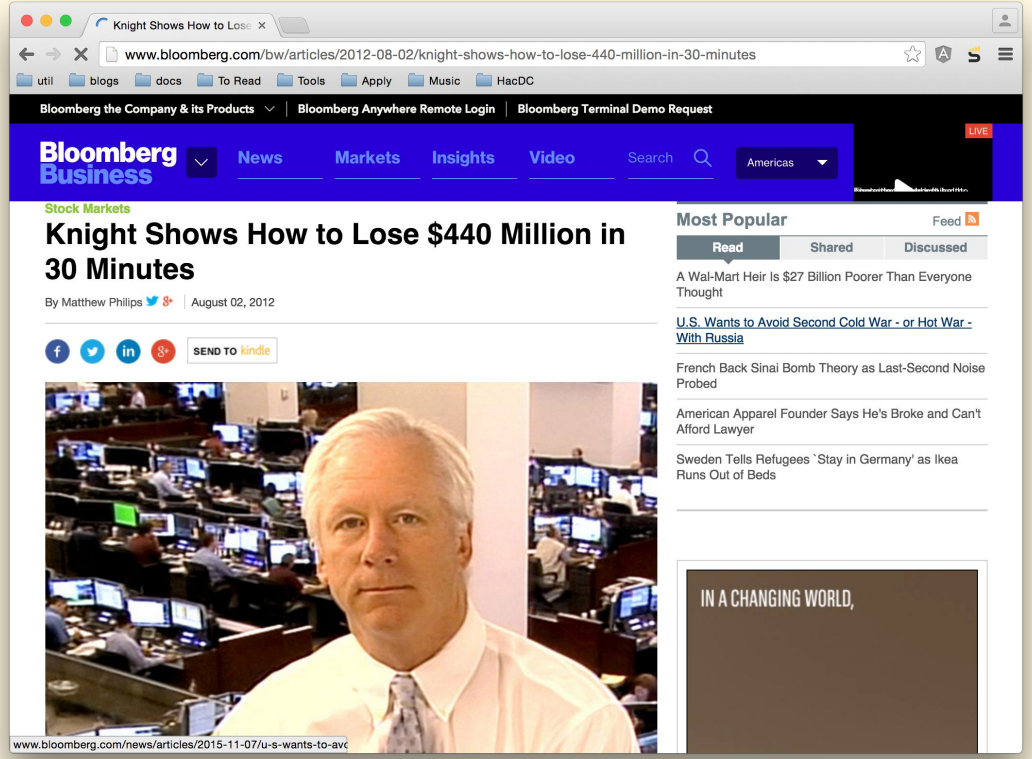


From SECURITIES AND EXCHANGE COMMISSION
17 CFR PART 241

This is a big industry

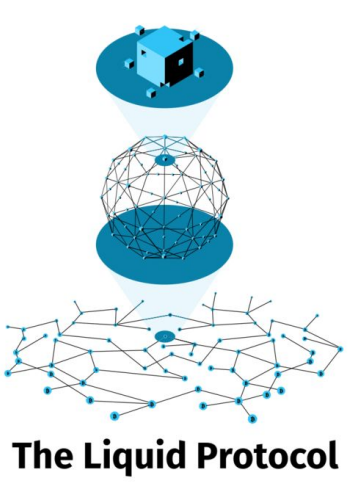


Mistakes happen



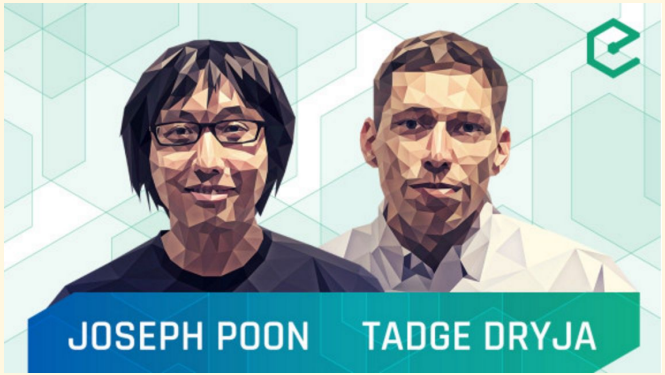
A Cryptocurrency might solve this

In 2011, DTCC settled the vast majority of securities transactions in the United States and close to $1.7 quadrillion in value worldwide. DTCC operates facilities in the New York metropolitan area, and at multiple locations in and outside the United States.



Counterparty

State-Sponsored Cryptocurrency: Adapting the best of Bitcoin's Innovation to the Payments Ecosystem



ripple

Bitcoin has a speed limit as of Nov 8, 2015

```
20  // MaxBlocksPerMsg is the maximum number of blocks allowed per message.
21  const MaxBlocksPerMsg = 500
22
23  // MaxBlockPayload is the maximum bytes a block message can be in bytes.
24  const MaxBlockPayload = 1000000 // Not actually 1MB which would be 1024 * 1024
25
26  // maxTxPerBlock is the maximum number of transactions that could
27  // possibly fit into a block.
28  const maxTxPerBlock = (MaxBlockPayload / minTxPayload) + 1
```

From github.com/btcsuite/btcd/master/wire/msgblock.go

A Bitcoin Block

type MsgBlock

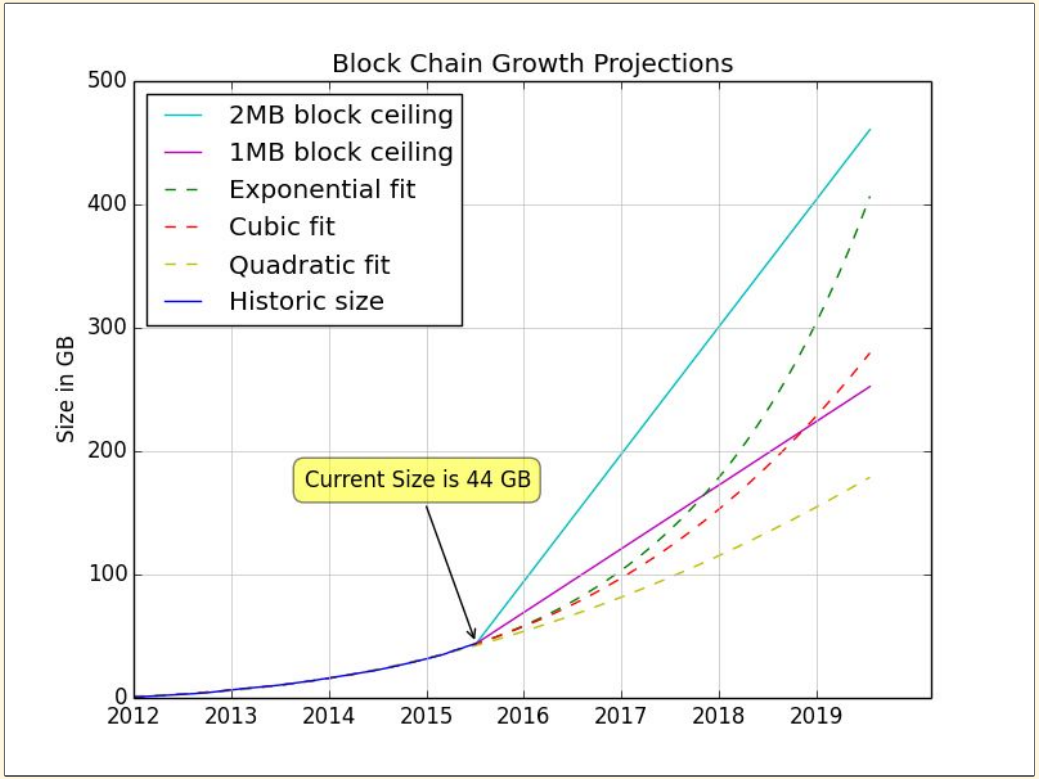
```
type MsgBlock struct {
    Header       BlockHeader
    Transactions []*MsgTx
}
```

MsgBlock implements the Message interface and represents a bitcoin block message. It is used to deliver block and transaction information in response to a getdata message (MsgGetData) for a given block hash.

From github.com/btcsuite/btcd/master/wire/msgblock.go

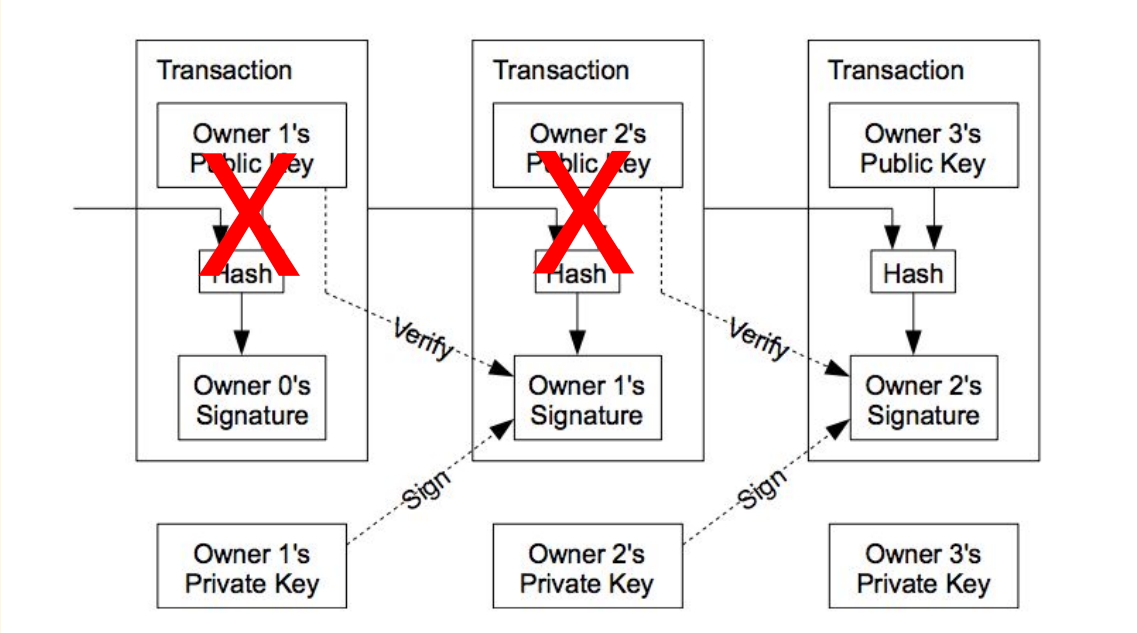
This is the challenge

Oct 28, 2015



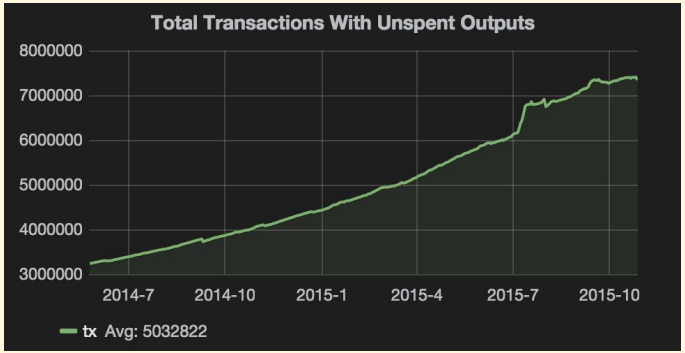
github.com/NSkelsey/uva-eng-thesis

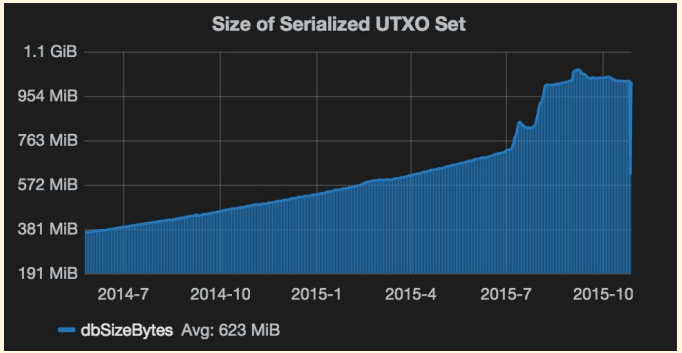
The Unspent Transaction Set

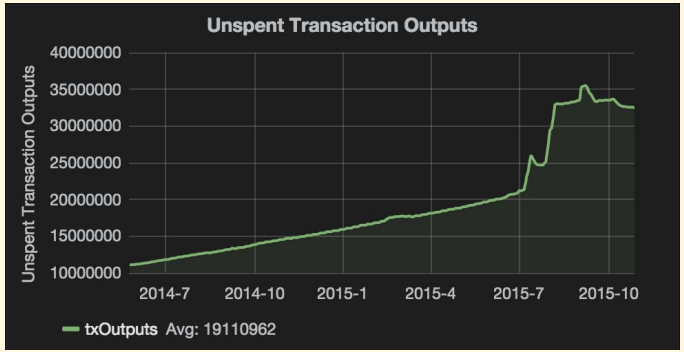


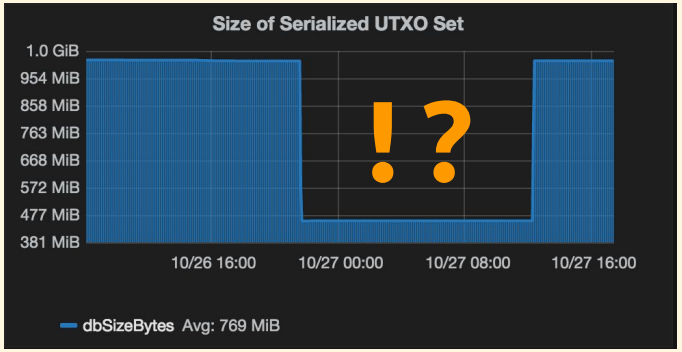
sizeOf(Unspent Transaction Set)

Satoshi Info Oct 27, 2015









Some requirements for ~~a new settlement system~~ a scaled bitcoin:

a fungible currency

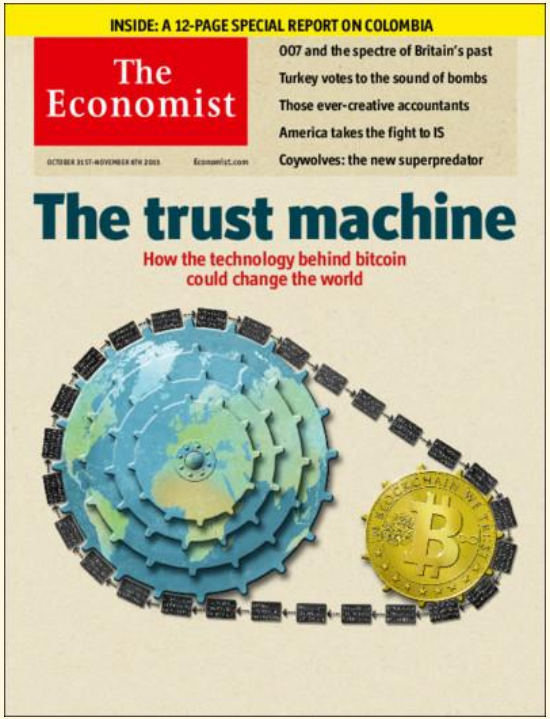
handle transaction volume

be regulatable

not run by crypto-anarchists

Scaling Bitcoin as a ~~state machine~~ public ledger

The world has some trust issues



TRANSITION TRANSITION TRANSITION

What is Bitcoin trying to accomplish?

NASDAQ

soapbox
systems
Counterparty

Scale bitcoin?

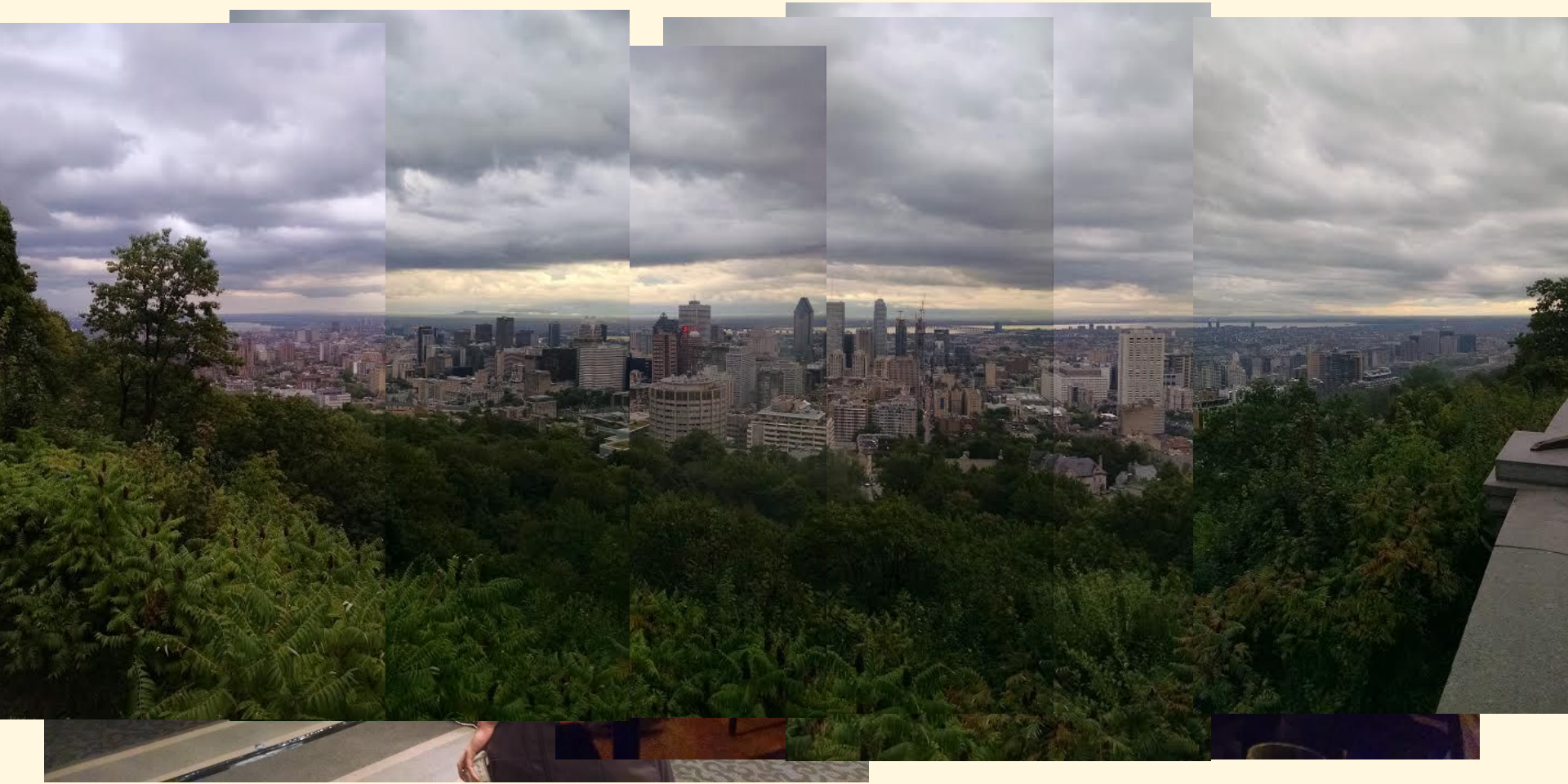
“How do we *scale* bitcoin?”

=

“Towards what *end* should we grow bitcoin?”

=

bitcoin is something now,
but what should bitcoin become?



Single consensus

“ We don’t care what happens, we just want a decision. ”

- Chinese and Scandinavian Miners @ Scaling Bitcoin, Montreal 2015

But, politics

Four Categories

(1) Short term
(2) Deterministic growth
(3) Market decision
(4) External

(1) Short term

BIP: 102
Title: Block size increase to 2MB
Author: Jeff Garzik <jgarzik@gmail.com>
Created: 2015-06-23

Abstract
Simple, one-time increase in total amount of transaction data permitted in a block from 1MB to 2MB.

https://github.com/jgarzik/bips/blob/2015_2mb_blocksize/bip-0102.mediawiki

Why?

Attack July 8 - July 10

“The average fee went up 3x, while the minimum fee went up a staggering 25x”
- Josh Cincinnati

200 t/s | height of attack
1-2 t/s | normal bitcoin
7 t/s | max 1mb
14 t/s | max 2mb

(2) Deterministic Growth

BitcoinXT
- hard fork
- 8 megabyte blocks after January 2016 once 75%+ of mined blocks are voting for the change
- After the switch the max block size limit smoothly increases, doubling every two years

BIP: 101
Title: Increase maximum block size
Author: Gavin Andresen <gavinandresen@gmail.com>
Created: 2015-06-22

Abstract: This BIP proposes replacing the fixed one megabyte maximum block size with a maximum size that grows over time at a predictable rate.

initial 8mb cap, cap doubles every 2 years for 20 years

(2) Deterministic Growth

Gavin, explaining motivation behind BIP 101:

(1) Transaction confirmation times for transactions with a given fee will rise; very-low-fee transactions will fail to get confirmed at all.
(2) Average transaction fee paid will rise
(3) People or applications unwilling or unable to pay the rising fees will stop submitting transa
(4) People and businesses will shelve plans stunting growth and adoption

(3) Market Decision

Making Decentralized Economic Policy
BIP 100 - Theory and Discussion, v0.8.1 - draft
Jeff Garzik

Protocol changes proposed:

1. Hard fork, to
2. Remove static 1MB block size limit.
3. Simultaneously, add a new floating block size limit, set to 1MB.
4. The historical 32MB limit remains.
5. Schedule the hard fork on testnet for September 1, 2015.
6. Schedule the hard fork on bitcoin main chain for January 11, 2016.
7. Changing the 1MB limit is accomplished in a manner similar to BIP 34, a one-way lock-in upgrade with a 12,000 block (3 month) threshold by 90% of the blocks.
8. Limit increase or decrease may not exceed 2x in any one step.
9. Miners vote by encoding 'BV'+BlockSizeRequestValue into coinbase scriptSig, e.g. "/BV8000000/" to vote for 8M. Votes are evaluated by dropping bottom 20% and top 20%, and then the most common floor (minimum) is chosen.

tldr; floating cap, let miner's decide themselves

What does the rational miner do? (Nick's got some opinions on this)

(4) External

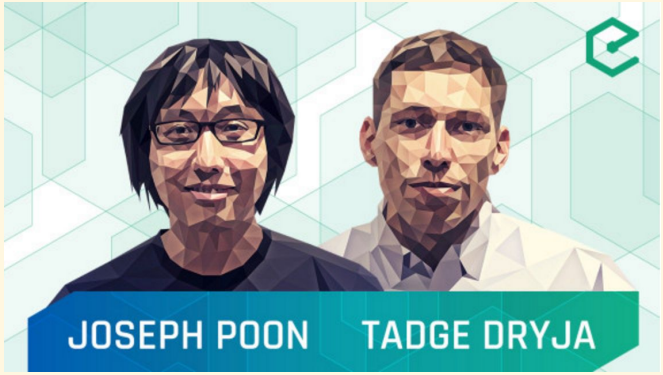
“ In the end, I believe the production quota would fail. The thing is that we can only really enforce rules that most of us agree with anyways. **Bitcoin will break down dams erected by special interest groups attempting to block the stream of transactions.** That's all I have to say about the transaction fee market.”

- Peter R
  http://diyhpl.us/wiki/transcripts/scalingbitcoin/peter-r/

(4) External

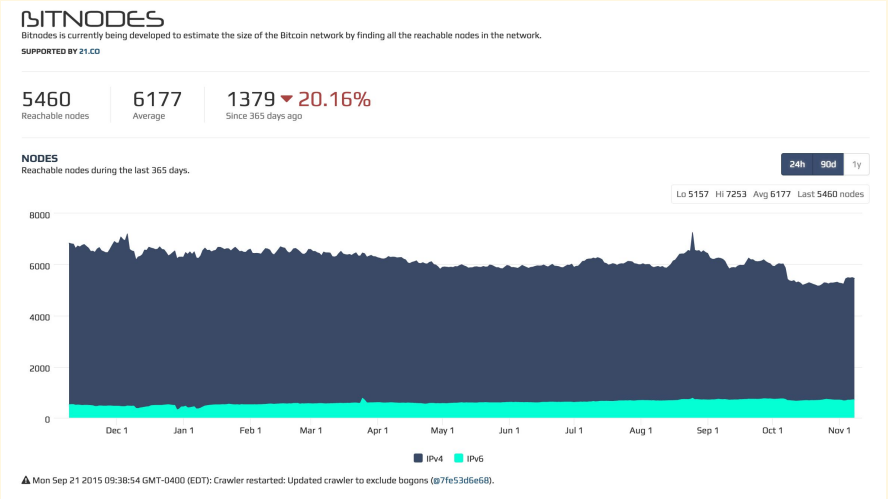
- Lightning Network
  “Bitcoin *doesn’t* scale”

  tldr; **transfer tx out of network.**
  if conflict, settle on chain.



TRANSITION TRANSITION TRANSITION

Bitcoin blocks have a replication factor of 100%



Sharding the block chain is complicated

Re: [Bitcoin-development] Tree-chains preliminary summary

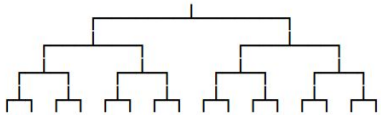
http://diyhpl.us/~bryan/papers2/bitcoin/tree-chains-preliminary.pdf

DATE: 2014-03-23

AUTHORS: Peter Todd

Blocks and the TXO set as a binary radix tree
==========

So how can we do better? Start with the "big picture" idea and take the linear blockchain and turn it into a tree:



Obviously if we could somehow split up the UTXO set such that individual miners/full nodes only had to deal with subsets of this tree we could significantly reduce the bandwidth that any one miner would need to process. Every transaction output would get a unique identifier, say txoutid=H(txout) and we put those outputs in blocks appropriately.

We can't just wave a magic wand and say that every block has the above structure and all miners co-ordinate to generate all blocks in one go. Instead we'll do something akin to merge mining. Start with a linear blockchain with ten blocks. Arrows indicate hashing:

Some requirements for ~~a new public ledger~~ a scaled bitcoin:

anonymous data storage tokens

replication guarantees

availability guarantees

immutability guarantees

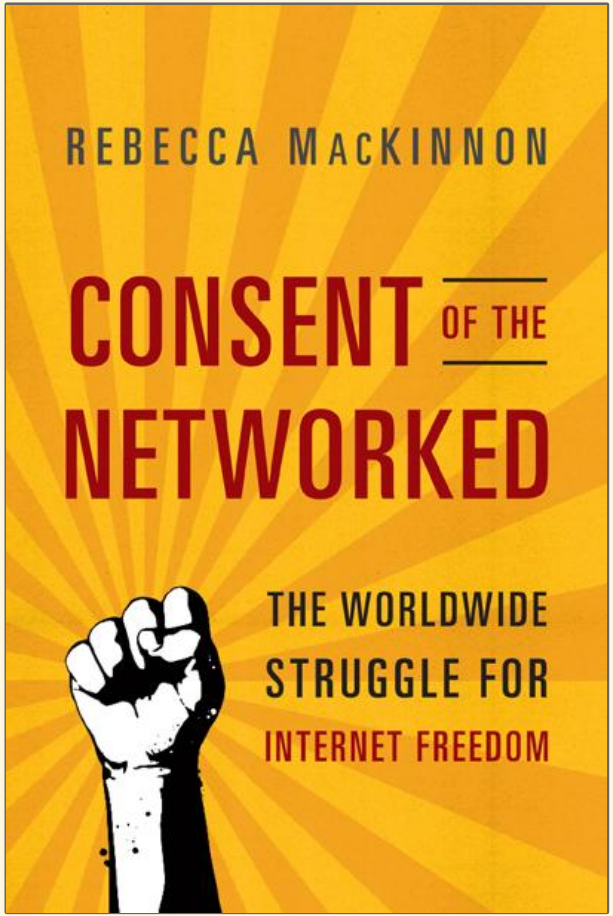
Ombuds

Block chain microblogs

“Authorities also use extra-legal measures to forcibly remove online content. Through the use of arrests, detentions, and torture, security forces coerced many online forum moderators into permanently shutting down their sites following the 2011 crackdown. This resulted in the loss of a large amount of information on _____’s history that had been documented by online users and made available only through local forums and websites.”

Freedom House report “Freedom on the Net in _____ 2014.”

Marks on the back of Nabeel Rajab after allegedly being beaten by police at a 15 July 2005 protest. From Wikipedia.



The Kingdom of Bahrain

2014 SCORES

FREEDOM ON THE NET STATUS

Not Free

FREEDOM ON THE NET TOTAL
(0 = BEST, 100 = WORST)

74

OBSTACLES TO ACCESS
(0 = BEST, 25 = WORST)

12

LIMITS ON CONTENT
(0 = BEST, 35 = WORST)

27

VIOLATIONS OF USER RIGHTS
(0 = BEST, 40 = WORST)

35

The 2014 Freedom House net freedom report card for Bahrain.

Use Bitcoin’s block chain as a permanent storage device for public statements and blog posts.

Use the public ledger as a public record.

This is not an original idea.

(Ab)using Bitcoin for an Anti-Censorship Tool

On the feasibility of a censorship resistant decentralized name system

Maybe not a good one.

Majority is not enough: Bitcoin mining is vulnerable

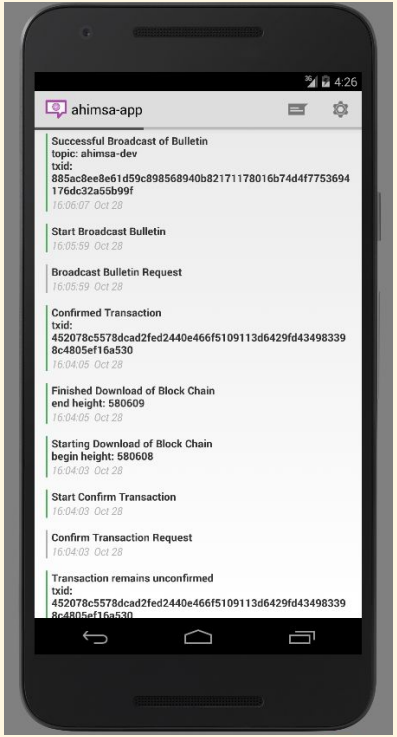
The Economics of Bitcoin mining, or Bitcoin in the presence of adversaries

To blog you need:

1. The equipment and software
2. An external connection out
3. At least ¢12 in bitcoin

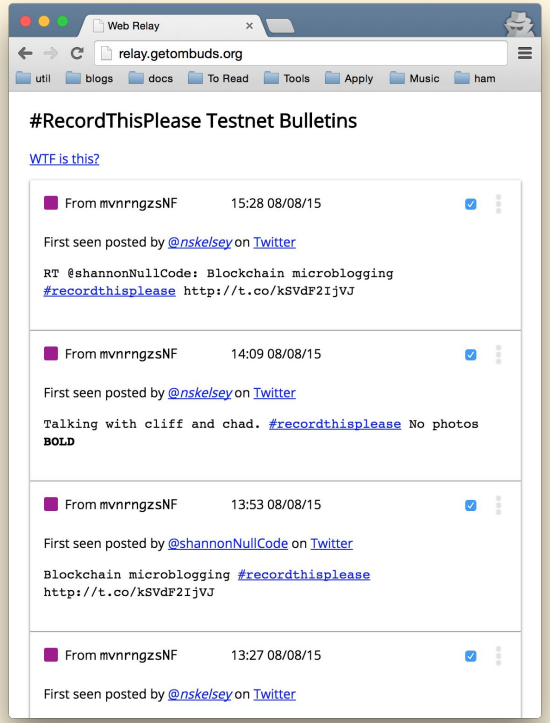
To blog you need:

ombuds-app is an Android app



- An SPV Bitcoin Client.
- Rely on external API server for more data.
- Connects via TOR.

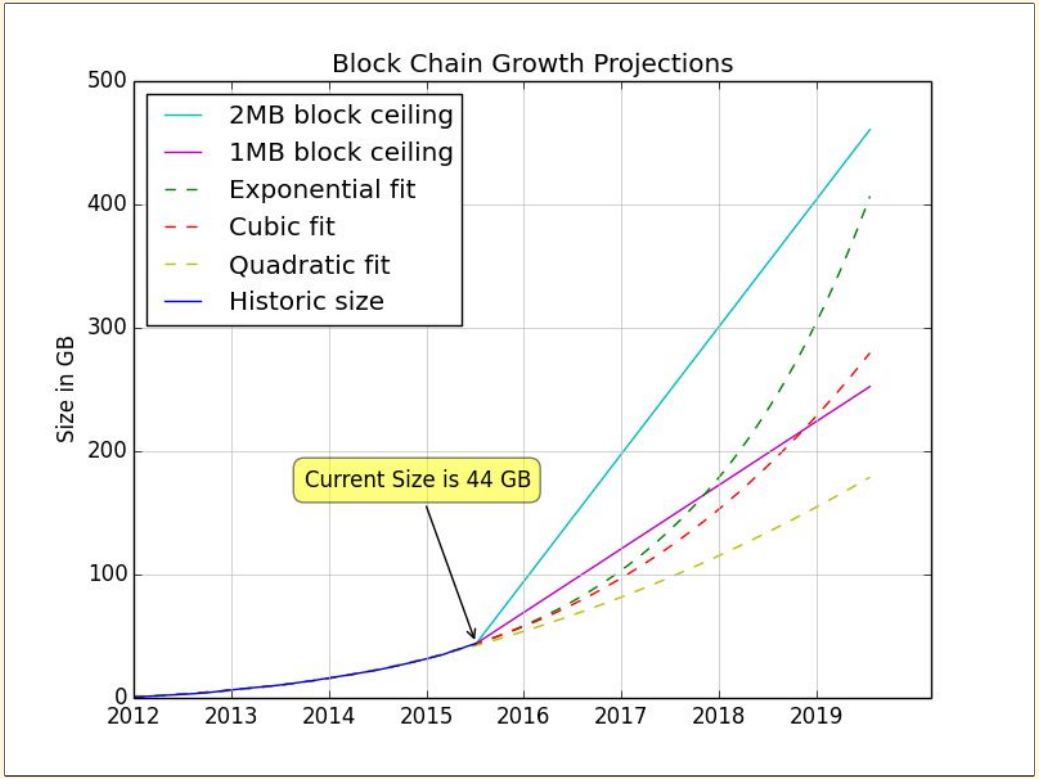
ombfullrelay is a full node and a web server.



- Responsible only for displaying content
- Run on the Web and as TOR hidden service
- Multiple Organizations can host records

This is a (solvable) challenge

Oct 28, 2015



github.com/NSkelsey/uva-eng-thesis

People make public statements on the Web

We are hiring a frontend dev

On the Web

https://getombuds.org

Special thanks to these folks!

Knight Foundation

hack.cville

batten institute
DARDEN SCHOOL OF BUSINESS