Straight Talk on Bitcoin and Blockchain

Cutting through the BS to get to the tech and stuff you need to know.

Jarret Dyrbye

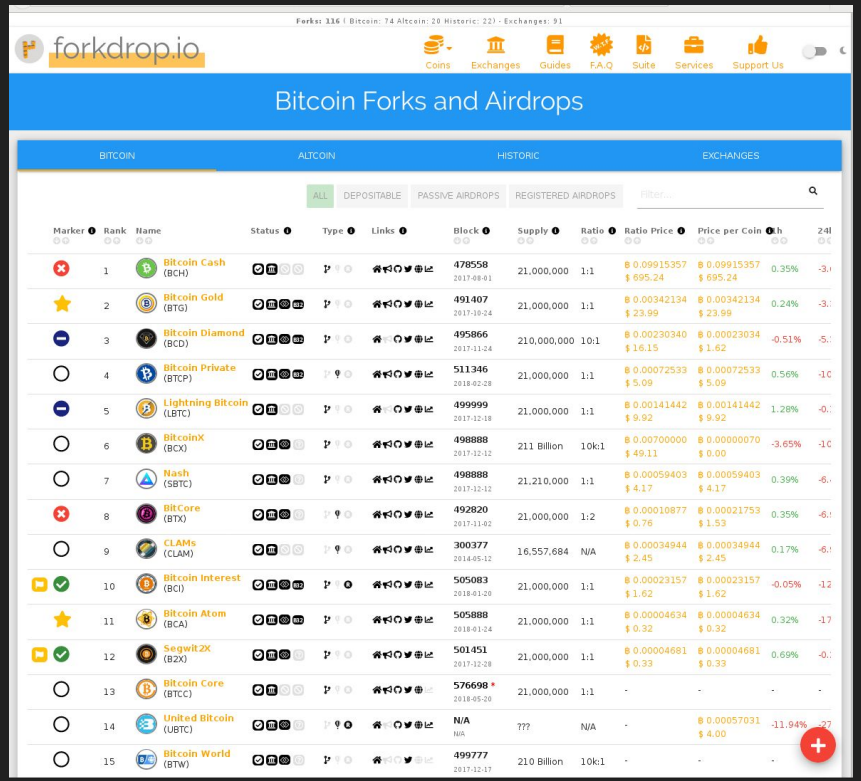
- UofA BSc. Computer Engineering 2005
- UofA MSc. Electrical and Computer Engineering 2008
- formerly YottaYotta, EMC, Dell EMC (9 year run as dev on VPLEX product)
- co-Founder PrimeVR
- co-Founder forkdrop.io

- Doing Bitcoin-related stuff full-time-ish since Jan 2017
- Some Bitcoin open source work
- Edmonton Bitcoin Meetup co-organizer
- email: jarret.dyrbye@gmail.com
- @jarret on YEGSEC slack

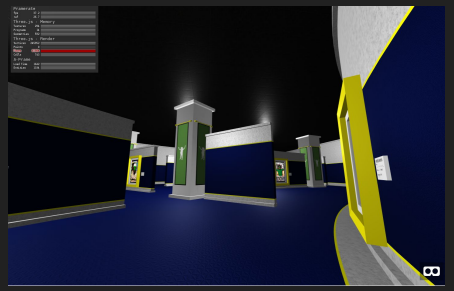
Disclosure: I own a long investment position in Bitcoin (BTC)

PrimeVR

Dash Dash Run!
VR running game (2017)
HTC Vive & Oculus
Available on Steam & Oculus Store



Forkdrop.io
Directory of Bitcoin Forks & Private Key Security Education & Open Source Tools (2018)



Unreleased WebVR/Blockchain Project (2017)

WIP Lightning Network Application project (2018)

My Goals:

1. Grow engagement in this topic
2. Create critical mass of reasonable people
3. Help seed an industry in Edmonton

Why Bitcoin Literacy for InfoSec People?

Negative trends in:

- Ransomware/Cons
- Botnet Mining
- Spam
- Spearphishing
- Scam ‘Investments’

Positive trends in:

- Distributed systems tech
- Economic Sciences
- Computer Literacy
- Entrepreneurship
- Energy Development
- Internet freedom activism

New Challenges in:

- Private Key Security
- Host Security
- Internet Privacy/Anonymity
- Cryptography
- Internet Message Routing

This is a gigantic topic! We can only scratch the surface.

Presentation Overview

1) Reminder about responsible investing

2) What is a Bitcoin/blockchain good/bad - discussion

3) Interesting challenges going forward

4) Brief Lightning Network Demo

5) Observations on Blockchain Snake Oil

6) Q & A

1) Responsible Investing

This presentation is not an investment recommendation!

Smart personal finance starts with the simple stuff:

Employer's DPSP or RRSP Contribution Matching

- literally free money from your employer
- This is an amazing deal, only 1/3 of employees opt-in

RRSP = get a large tax return by contributing

TFSA = tax-free investment gains!

RESP = tax-free discount on your children's education

Manage Debt:

- pay off credit cards for a guaranteed 20% return on investment
- Average Albertan carries $28,155 in consumer debt - not good!

Do this expertly and you will be set for life.

All paths to wealth require **discipline** as a common element

Bitcoin Is Not Easy Money

Bitcoin is **volatile AF**

- ruins finances
- ruins marriages/relationships
- scrambles your brain with chemical signals
- high suicide rate (seriously!)
- puts you close contact with The Dark Side

Bitcoin **may not actually work long-term**

- relies on miner subsidies that expire eventually
- fee pressure needs to develop to sustain

Chart goes up AND down - how disciplined are you?

The incentive structure might be flawed.

There could be cryptographic flaws discovered

There could be heavy government action

Government money is digital and can be improved

100s more reasons not to invest. Be careful!

2) What is Bitcoin/Blockchain good/bad for?

What Is Bitcoin?

(plenty of Bitcoin 101 material out there)

- Uses Proof of Work (PoW) to filter insincere packets from sincere
- PoW is unforgeable and lying has a cost
- Max 2,100,000,000,000,000 (2.1 quadrillion) satoshis in existence
- everyone validates a copy of the ledger
- Open Source protocol

What a Blockchain?

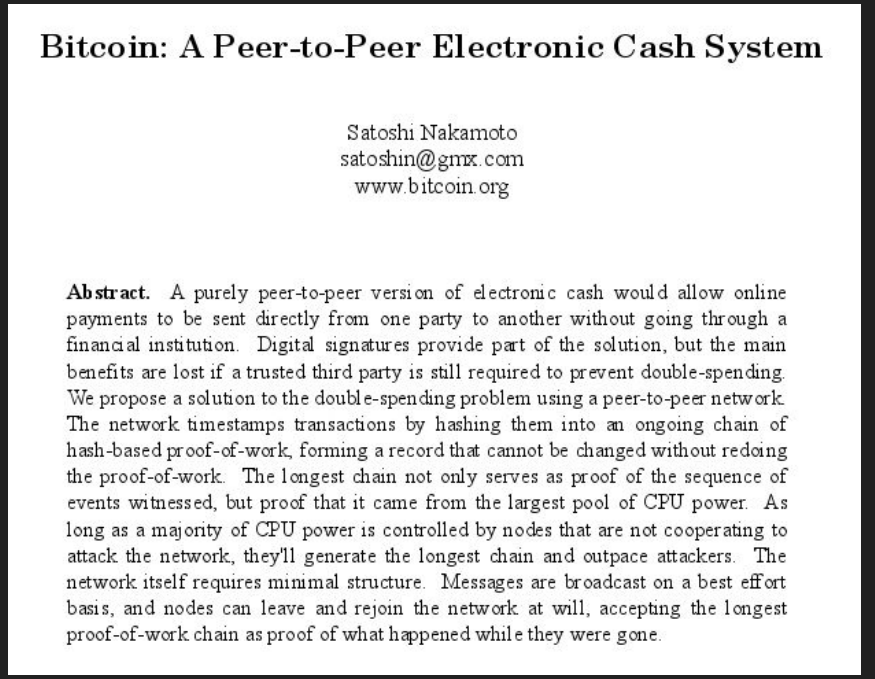
- used to have a specific meaning (chain of blocks with most PoW)
- now used as a (largely-meaningless) buzzword
- Does all the things databases do (only better????!!!)

What is Bitcoin's Blockchain good for?

1) Solves the Double-Spend problem
2) Irreversible, uncensorable payment of native currency

...and with the inbuilt scripting language:

3) Automated "Court-of-Law" settlement for cryptography-bound agreements



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

The Double-Spend Problem

Alice pays Bob; Alice cannot pay Carol with the same money.

In order to double-spend attack, Alice must provide more SHA256 work than 50% of the network, sustained over time.

The cost of attack is immense and continues to accumulate

Therefore **Bob can be increasingly probabilistically certain** of the received payment.

That is All.

Irreversible, Uncensorable Money Implies:

Ugly: Black market activity

- nasty stuff
- where banks definitely won't touch
- Good actors must ‘pick up the trash’

Bad?: Grey market activity

- "Pharmaceuticals"
- "adult entertainment”
- "great investment opportunity"
- where banks won't touch

Good: Cross-border economic activity

- Remittance
- shipping/receiving
- where banks do poorly
- the worse the country/banks, the more appealing

Amazing: Programmable money

- can trust the state of the ledger like it is an extension of RAM/Disk
- host A negotiates with host B for service and price - micropayments supported!
- paradigm shift! - banks can't do this!

What is a Blockchain bad for?

Key point: they are bad at **Nearly Everything**

Terrible databases!

- "everybody knows everything" is a bad architecture
- “Everybody validates everything” is only as fast as the **slowest** computer on the P2P network

T**errible** app platforms!

- end users don't know how to handle cryptography
- everything **costs money**
- Blockchains **don’t scale**. Sorry. Laws of the universe.

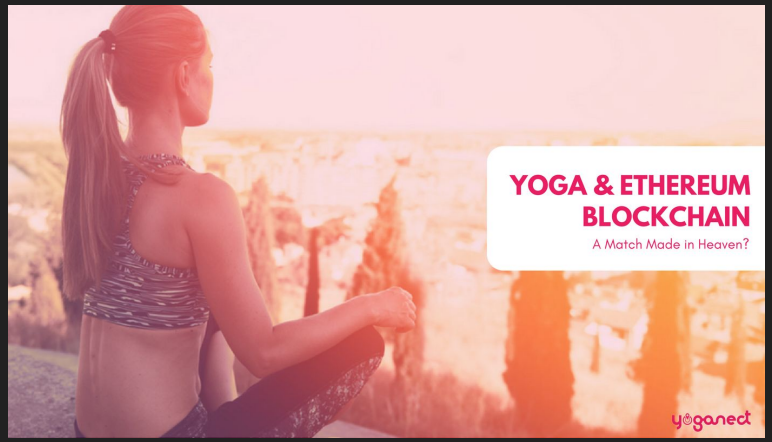
Always remember:

- Cryptography is math to **prevent** you from doing things.
- blockchains are for preventing double-spends
- "Do one thing" architecture

'decentralized' systems already exist, and work great without a blockchain. What gives?

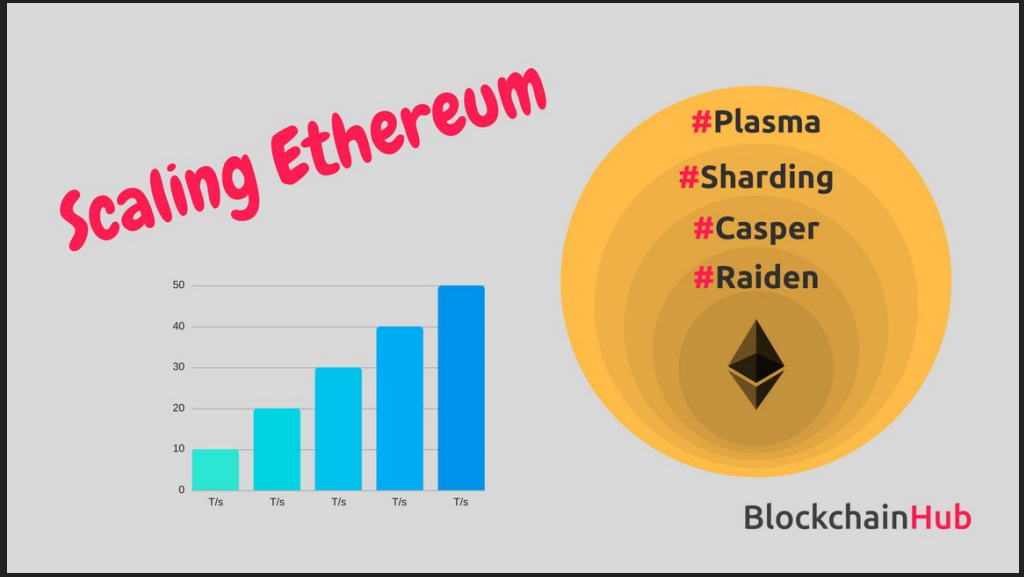
- In particular: git, DNS, certificate authorities
- Also: email, www, ip, internet routing tables, bittorrent, PGP
- Uh, database can be distributed and trust-minimized too

People disagree with my perspective on Blockchain



ESLCoin
ENGLISH AS A SECOND LANGUAGE

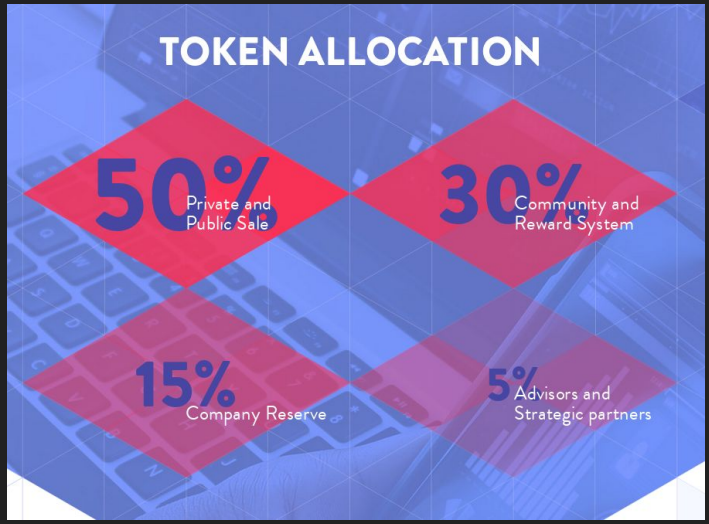
Scaling?



Linear scaling?
What do those words mean?

Jolyy - Beauty services on the Blockchain!

JOLYY is an online beauty booking platform which will be upgraded using blockchain technology. Our mission is to disrupt the existing market for on-line beauty booking by providing an innovative and highly effective beauty booking platform. We will provide the beauty market with a secure, trustworthy and efficient platform, which will be beneficial for all parties – from the industry representatives to their clients.



What's the token for?
Would Paypal work for this?
What's wrong with a LAMP stack?

Atonomi - IoT on the Blockchain

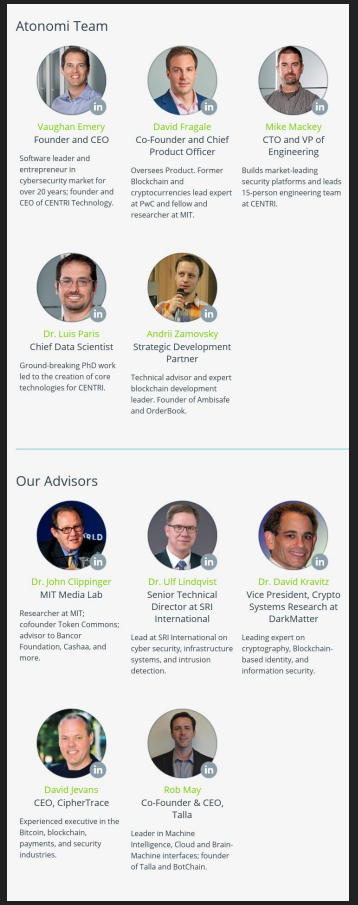
The Secure Ledger of Things

Security Protocol for the Internet of Things

Atonomi:

Atonomi provides a new security protocol and infrastructure to enable billions of IoT devices to have trusted interoperability for both data and commerce.

The key innovation of Atonomi is to root the identity and reputation of devices on a blockchain-based immutable ledger. We accomplish this by building and incentivizing an ecosystem of participants to maintain decentralized consensus for device transactions on the Atonomi Network.



Is this a lean start up?
Do they have a working product?
What are the advisors for?

Singularity NET - AI on the Blockchain

The Global AI Network

SingularityNET lets anyone create, share, and monetize AI services at scale. The world's decentralized AI network has arrived.

Open AI For All

SingularityNET is a full-stack AI solution powered by a decentralized protocol.

We gathered the leading minds in machine learning and blockchain to democratize access to AI technology. Now anyone can take advantage of a global network of AI algorithms, services, and agents.

Executive Team

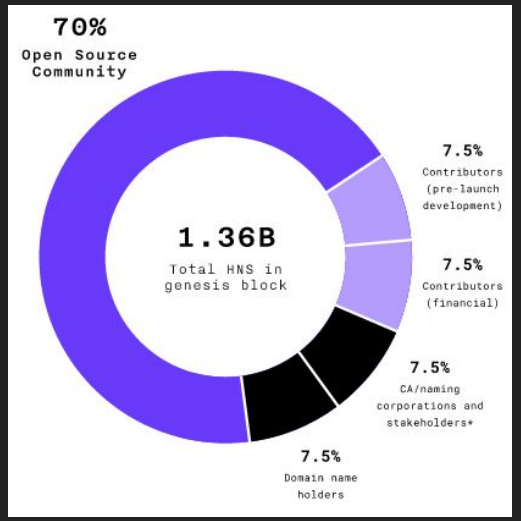
Ben Goertzel
CEO & Chief Scientist

Simone Giacomelli
Head of Business Development

Cassio Pennachin
Chief AI Officer

Handshake.org - DNS and CA on a blockchain

Handshake is a decentralized, permissionless naming protocol compatible with DNS where every peer is validating and in charge of managing the root zone with the goal of creating an alternative to existing Certificate Authorities. Its purpose is not to replace the DNS protocol, but to replace the root zone file and the root servers with a public commons.



Funds

a16z crypto

Draper Associates

Greylock Partners

IDEO Colab

Kilowatt Capital

Strong VC

DCG

Collaborative Fund

SV Angel

DCM Ventures

Ausum Ventures

Founders Fund

Sequoia Capital

Polychain Capital

DHVC

FBG

Hashed

Pantera Capital

Boost VC

Nima Capital

Craft Ventures

The Handshake project has received 10.2MM USD from Project Sponsors. The net proceeds are pledged to be distributed to Free and Open Source Software communities (projects, non-profits, hackerspaces).

OK, What is going on here?!!!!

Handshake.org (Part 2)

- Accuses existing CA and DNS providers of **rent seeking** on fees and being tyrants.
- Plans to solve with Open Source and PoW blockchain governed by hashrate
- Handshake assigns 100% of the coins to themselves and distributes how they see fit
- CA and DNS reduces to Key-Value store, do blockchains add something to the problem of key-value store?
- What happens when you lose/leak a private key? Is dispute resolution a needed feature?
- Switching cost from existing systems?
- 51% hashrate attacks?
- Are there **rent seekers** in this system?

- Why are Silicon Valley Venture Capitalists **pitching to YOU**?
- Are SV VCs offloading their downside risk onto the general public?
- Can they exit position onto the general public based on their insider knowledge?
- What prevents them from market manipulation? (Wash trading, etc.)
- What are insider trading laws and regulation for?

Handshake.org (Part 3)

What about Namecoin?
DNS + Key-value on a blockchain
was already tried in 2012
This was a well-known and well-studied project

Namecoin is an experimental open-source technology which improves decentralization, security, censorship resistance, privacy, and speed of certain components of the Internet infrastructure such as DNS and identities.

(For the technically minded, Namecoin is a key/value pair registration and transfer system based on the Bitcoin technology.)

From Handshake.org whitepaper:

```
Namecoin's model requires a user to run a fully validating node in order to
securely resolve domain names. Although Namecoin was the first cryptocurrency
project to attempt to implement a DNS bridge[namecoin-2] for a cryptocurrency
naming protocol, the protocol itself is lacking in the area of SPV.
```

Handshake.org Fine Print:

We also have a SPV client, hnsd, which is written in C. It acts as a light client to the blockchain, as well as a recursive name server. It can serve provable resource records and verify payments without having the resource requirements of a full node.

SPV = “simple payment verification”
Blockchain speak for thin/mobile client

Handshake.org’s blockchain innovation
Is a client-server architecture!

(also, Namecoin is open source. Why not add SPV functionality?)

(deep breath)

Reminder:

1. Solves the Double-Spend problem
2. Irreversible, uncensorable payment of native currency
3. Automated “Court-of-Law” settlement for cryptography-bound agreements

Very. Cool. Programmable. Money.

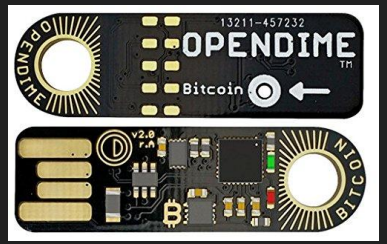
3) Interesting Challenges Going Forward

On Private Key Security

- Your private key is your money. Potentially a lot of money.
- How much do you trust your computer? a million dollars worth? A billion?
- What kind of a computer handles a billion dollars?

Solutions:

- Paper Key Storage
- Physical Security for Key Storage (vaults, guns etc.)
- Hardware Wallet
- OpenDime
- Pseudo-airgap signers
- Airgap



Open Problems:

- Scaling to the needs of large organizations
- will/estate planning
- Loss from mistakes due to bad UI?
- Rooted hardware? Silicon poisoning?

On Host Security

- Hosts now have money on them that the bad guys want to steal
- Digital bank robberies

Solutions:

- rich history of good OS security products
- Linux/BSD
- Encrypted drives
- robust crypto libraries/tools
- You can still host your own web server on today's internet

Open Problems:

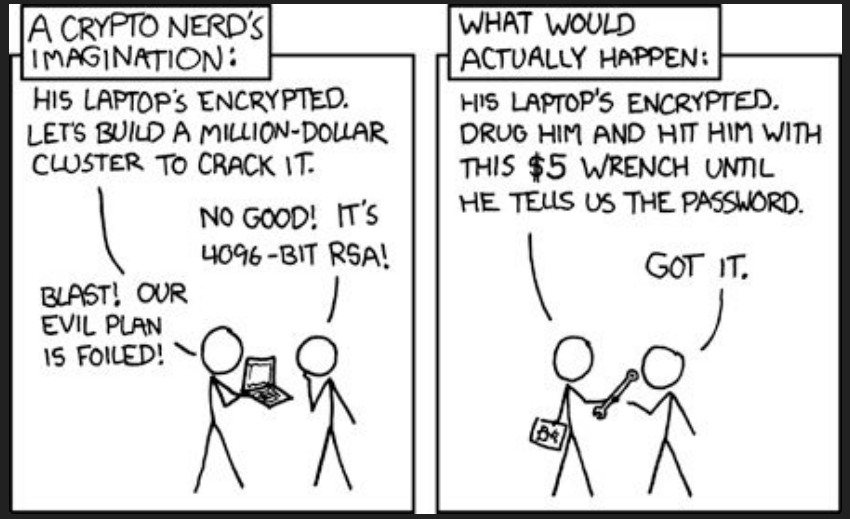
- how secure is our stuff really (Intel ME, etc.)?
- Copy-paste UI metaphor really sucks for cryptocurrency - error prone and easy malware target
- Cell phone security really sucks
- cloud hosting is very convenient and cheap
- move fast and break things innovation culture
- Companies aren't run by the most competent

Internet privacy/anonymity

- People walking around with digital bearer asset fortunes
- is it smart to have $1M worth of gold stored in your basement?
- $5 wrench attack
- people want financial privacy

Solutions:

- Tor is very important
- Coin mixing / cash trading
- Protonmail and other private email for private communication
- Catalyst for PGP adoption?



Open Problems:

- dealing with spearphishing
- Know Your Customer Regulation
- Anonymous 2FA devices?

On Advanced Cryptography

- Crypto is still a new, obscure science.
- Brightest minds in Mathematics are just getting interested in this now.

Solutions:

- amazing applications of ECDSA, and hash algorithms
- libsecp256k1 is amazing. (TLS applications can learn from it!)
- Schnorr signatures soon
- Chaumian coin-join

Open Problems:

- blind signatures + homomorphic zero-knowledge tech
- advanced cryptographic assumptions good for handling money?
- how much do we really know about cryptography?
- is quantum computing a problem?

On Message Routing

- Blockchains don’t scale
- We need to **coordinate** with cryptography **off-chain**
- We need custom-built networking infrastructure for this

Solutions:

- Bitcoin Peer-To-Peer networking has become very robust
- Tor is a fantastic starting point

Open Problems:

- Mining decentralization improvements
- onion routing
- rendezvous networking for P2P paradigms
- value-centric routing
- "ant routing" vs "mail routing"

4) Brief Lightning Network Demo

5) Observations on Blockchain Snake Oil

General Observations

- Understanding software architecture tradeoffs is a highly-specialized skill
- Even most programmers don't have a very good grasp of cryptography, databases, git, RAFT, PAXOS, etc.
- Average person with money to invest not into Comp Sci - just how it is
- Average people get caught up in Ponzis, Pyramids, MLMs, scams, gambling, lotto, etc.
- Marketing a coin is a low-knowledge occupation with a high payoff (at present)
- Not every scammer thinks they are a scammer.
- Securities regulators (SEC, CSA, ASC) are catching up to these fraudsters.
- ... but fraudsters continue to innovate in this space
- ICOs go by different names and have different spins to dodge regulators
- An ICO is not a ponzi scheme, pyramid scheme or, MLM, but damn close
- It is a the next iteration of a rich history of internet scams. Usenet spam, email spam, Viagra pills, nigerian princes, “one weird trick”, etc.
- Shouldn’t be surprising.

Architecture of the ICO scam (yes, all ICOs)

1) "Great idea guys!"
   - lots of technobabble in marketing material
   - Highly Credible team (marketing people in suits, no developers)
   - "look, we are regulated" or "look, we don't need regulation"

2) Coin distribution: actual cronies get coins

3) "pre-pre sale": first round of idiots that think they are cronies get sold on the pump

4) "pre sale": second round of idiots that think they are cronies get sold on the pump

5) "sale" - sell to the general public on the pump

6) get on exchanges

   - requires bribe to exchanges
   - e.g. $2-3 Million USD to get listed on Binance

7) trading on exchanges

   - Insider cronies have lots of BTC
   - wash trading to set price anywhere they want
   - traders buy in to trade patterns

8) Initial croneys exit their holdings

   - price bleeds out
   - may have rounds of pump-n-dumps
   - may have lingering victims in denial continuing on

Internet Comments Considered Harmful (1)

"decentralize all the things"

"decentralized is better"

"Automate the government"

"(cult messiah figure) is a blockchain genius"

"Rothbard/Mises/Friedman is an economic genius and predicted this"

"Proof of Stake is cleaner than Proof of Work"

"Satoshi's vision"

"Democratize investing”

"Trading makes you easy money"

"<random scamcoin> is the new Bitcoin"

"Utility/security token"

"Blockchain + <buzzword>"

"Blockchain and not Bitcoin"

"Bitcoin is old technology"

"Bitcoin mining is dirty"

“Masternodes make you easy money”

Internet Comments Considered Harmful (2)

“Bitcoin is dead”

“Bitcoin has no intrinsic value”

“Bitcoin is Beanie Babies all over again”

“Bitcoin is for heroin”

“Bitcoin is obviously dumb”

“Economists agree deflation is bad”

“Money has value because it is backed by the government”

“Bitcoin is legacy technology”

“Bitcoin is not backed by anything”

“Blockchains can never work because the don’t scale”

“This is a passing fad”

“Bitcoin is a Ponzi scheme”

“Bitcoin is too volatile to be useful”

“Transaction fees are too high”

Common Sense

Dunning-Kruger effect:

- "a cognitive bias in which people of low ability have illusory superiority and mistakenly assess their cognitive ability as greater than it is"
- Admitting you don’t understand stuff is hard. BSing is easy.
- when people make money, they think they are **sooooo smart**

- There always an investment product hiding behind these people somewhere
- (Bitcoin is often one of those products being shilled)
- People argue according to the bag of coins they hold (this is human nature and incentives)
- Tech is still early - give it a decade or two before judging anything.
- Beware Ideology and Ideologues - these are proto-cults.
- The universe owes you nothing
- Any great tech has FUD

Thanks!
Q & A
AMA