Crypto-currency: Status and Future Perspectives

R. R. Brooks – rrb@acm.org
Clemson University, Electrical and Computer Engineering

June 19th, 2017

A Propos PowerPoint Slides

Boston Sunday Globe

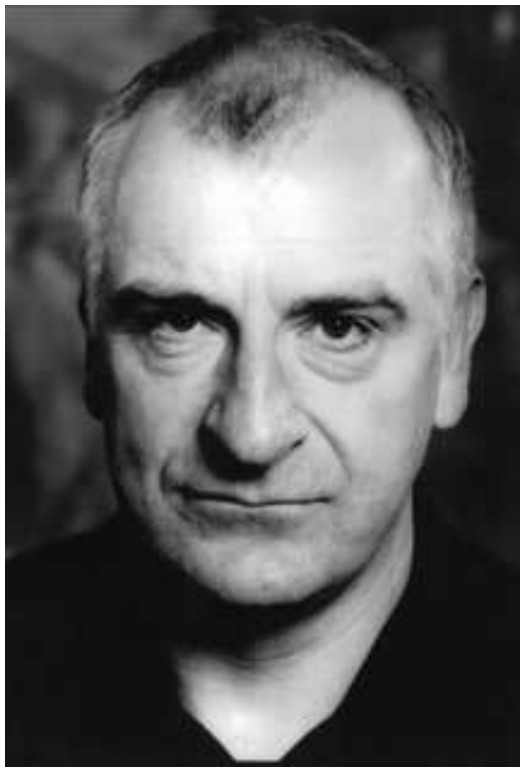
FEBRUARY 2, 2003

Space shuttle Columbia lost on reentry; 7 astronauts dead

A fiery trail streaked across the sky as the space shuttle Columbia broke apart yesterday over Texas. An amateur photographer captured this image from his backyard in Tyler.

- Slide decks bad medium for imparting information.
- Edward Tufte attributes loss of Columbia space shuttle to PowerPoint use by NASA.

A Propos Money



- "This planet has - or rather had - a problem, which was this: most of the people living on it were unhappy for pretty much of the time. Many solutions were suggested for this problem, but most of these were largely concerned with the movement of small green pieces of paper, which was odd because on the whole it wasn't the small green pieces of paper that were unhappy." - Douglas Adams *H2G2*

History of money

Barter to Commodity

- First agrarian settlements use barter and gift economies,
- 9000 to 6000 BC – Items of value (cattle, goats),
- 1200 BC – Cowrie shells in China,
- 1000 BC – Metal cowrie imitations in China.

Yapese currency

- Yap island in Pacific uses limestone blocks as currency.
- No limestone on Yap. Imported from other islands by canoe.
- Rare and valuable. Almost impossible to move.
- Currency ownership established by oral tradition.
- Public ledger of ownership and transactions.

Commodity to Fiat

- 1816 Gold standard established by England. Best known commodity.
- Problems due to great depression.
- Keynes – currency availability controls economy.
- 1930 Gold standard ends.
- 1944 Bretton Woods conference established World Bank and IMF.
- Central banks establish money supply. IMF mediates.

Money summary

- ☐ 100,000,000,000,000 Zimbabwe Dollars = USD 0.40
- ☐ Money is a widely accepted medium of exchange.
- ☐ Must be a limited supply.
- ☐ Should be hard to counterfeit.
- ☐ Danger of hyper-inflation and deflation.
- ☐ Money supply regulated by a central bank.
- ☐ International exchanges regulated by IMF.

Virtual currency

Current state

- Starting with Rothschild, international banking system.
- Your bank account is an entry on a computer disk.
- What if EMP destroys all computer records?
- Banking system is a regulated universal ledger of accounts.

First virtual currencies

- Online currencies start with trusted intermediary.
- Credit card companies, eBay, PayPal, E-Gold, etc.
- Needed for on-line transactions.
- Risks taken by middle man, in exchange for fees.
- Some markets use escrow accounts.
- Lawyers are the real computer and network security mechanism.

Video game currencies

- ☐ Video games create complex worlds with complex societies.
- ☐ Hire economist to avoid hyperinflation and chaos in markets.
- ☐ Some games have hard and soft currencies.
- ☐ Funds go in and out of games.
- ☐ Sometimes used for money laundering.
- ☐ Gold farming and Chinese prison.
- ☐ Wuffie and reputation.

Virtual currency summary

- Banking system and wire transfers changed money from physical tokens to information.
- On-line commerce originates with trusted third parties.
  - Credit cards, PayPal, etc.
  - Escrow accounts.
- Game currencies have actual value.
- Currency moving further from national to market control.
- Virtual worlds hire economists to act as central bankers.

Bitcoin

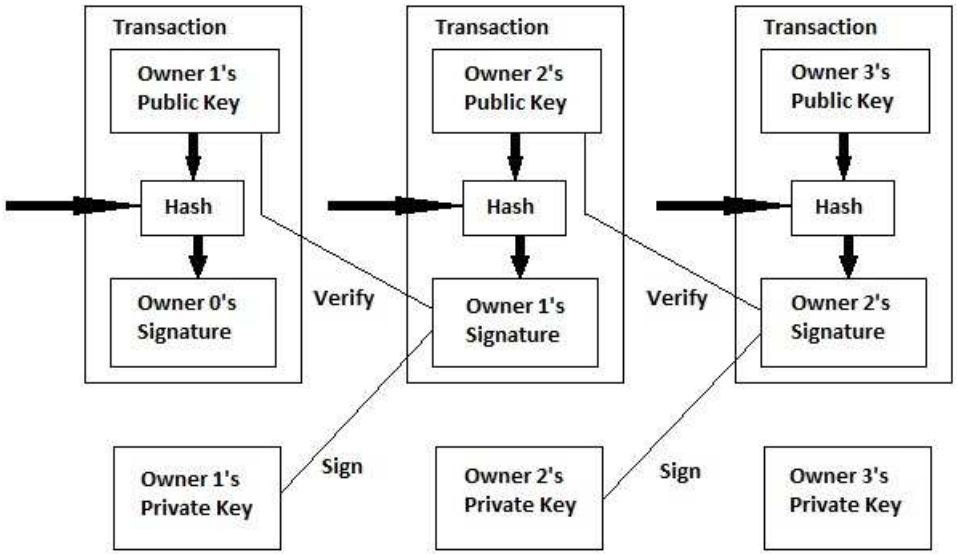
Origin story

- May 2007 – "Satoshi Nakamoto" started coding Bitcoin.
- August 2008 – bitcoin.org registered.
- December 2010 – Satoshi stops talking to people.
- "He" is a billionaire. He is anonymous.
- "He" may be male, female, or a team.
- Built on b-money, Bitgold, HashCash and other proposals.
- Solved many important problems to create first real crypto-currency.
- Only Newsweek believes the person in the picture is Satoshi,

Byzantine Generals Problem

- Posed by Lamport.
- Known solutions exist. Including my dissertation.
- Distributed data base on multiple nodes.
- Transaction verification by winner of competition.
- No centralized point of control.
- Hack has to change multiple nodes in real-time.

Blockchain



- Each transaction signed by spending party.
- Transactions put into blocks by 3rd party "miner".
- Hash of previous block becomes part of next block.
- Hash is random mapping of inputs to fixed number of bits.
- Next block signed by another "miner".
- Public key signing is encryption of hash using (secret) private key.
- Signature easily verified using (publicly available) public key.
- Hack has to compromise all nodes to change distributed database in real-time.

Mining

- ☐ Mining verifies transactions and stops inflation.
- ☐ Miners receive and verify transactions.
- ☐ Miners compute hash of block with random value appended.
- ☐ Proof of work – Hash has to start with n zeros.
- ☐ Proof of work requires trying random values for hash.
- ☐ Miner that solves problem gets new BTC and transaction fees.
- ☐ Stop inflation – n varies to create 1 block per 10 minutes.
- ☐ Energy for 1 block could heat house for week.

BTC summary

- ☐ Working system.
- ☐ Public ledger does not allow double spending.
- ☐ Transactions independently verified by miners.
- ☐ Blockchain universally stored in cloud.
- ☐ Malicious modification effectively impossible.
- ☐ Value maintained by limited number of BTC.

Social impact

Heroin

THE PEOPLES DRUG STORE pride ourselves on offering the best quality products at competitive prices and making every effort to go above and beyond when it comes to customer satisfaction!

Choose a category by clicking on any of the following:

Heroin*, *Cocaine*, *Ecstasy*, *Speed*, *Cannabis* *Prescriptions*, *Bitcoins* and *Services

WANNA MAKE SOME FREE BTC??

Tell others about this shop, and earn 5% from every purchase they will make. Simply give them the following link: http://www.peoplesdrugstore.org/?ref=YOURUSERNAME (or the original http://newpdsuslmzqazvr.onion/?ref=YOURUSERNAME) Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.

SW Asian #4 Heroin

The Heroin we offer comes **direct from the importer** with no middle man

It is white/light beige in color and we take great pride in the fact that ***we do not cut our product whatsoever*** and we ensure that our source does not do so either!

We would much prefer to offer a high quality product and have repeat customers

Whats the difference between #3 and #4 heroin?

Cocaine

(http://lchudifyeqm4ldjj.onion/viewProduct?offer=101646.654956)

FE 2g Kokain Cocaine Free Shipping (http://lchudifyeqm4ldjj.onion /viewProduct?offer=101646.654956)

lchudifyeqm4ldjj.onion...uct?offer=101646.654956 (http://lchudifyeqm4ldjj.onion /viewProduct?offer=101646.654956) Dream (http://lchudifyeqm4ldjj.onion)

This is our Listing for Cocaine Your will get a Sample with 2g Cocaine from Columbia This is high quality shit Feel free to order and see for yourself Please make sure to read our Profil before ordering PS The Picture will be updated asap The Cocaine looks like this but is from a rock with rocks

Vendor YOURDEALER Price ฿0.0295 Location Germany (32)

(http://grams7enufi7jmdl.onion

Drug markets

- Started 2011 with Silk Road (Ross Ulbricht).
- Convicted and in prison.
- FBI tracked his network use and he hired informant.
- Alpha Bay replacement stopped earlier this year.
- Password reset emails sent to owner's email.
- Combination on-line market, user reviews, and escrow accounts.
- Delivery by mail is feature not a bug.

Credit Cards

[Who I am]

I am a independent security researcher. Hacking and social engineering is my business since I was 16 years old. I never had a real job so I had the time to get really good at this because I have spent the half of my life studying and researching about hacking, engineering and web technologies. I have worked for other people before in Silk Road and now I'm also offering my services for everyone with enough cash here.

[Prices]

I'm not doing this to make a few bucks here and there, I'm not some shit of eastern europe country who is happy to scam people for 50 euro.
I'm a proffessional computer expert who could earn 50-100 euro an hour with a legal job.
So stop reading if you don't have a serious problem worth spending some cash at.
Prices depend a lot of the problem you want me to solve, but the minimum amount for smaller jobs is 200 euro.
You can pay me anonymously using Bitcoin.

[Technical Skills]

- Web (HTML, PHP, SQL, APACHE).
- C/C++, Java, Javascript and Python.
- 0day Exploits, Highly personalized trojans, Bots, DDOS attacks.
- Spear Phishing Attacks to get passwords from selected targets.
- Hacking Web Technologies (Fuzzing, NO/SQLi, XSS, LDAP, Xpath).

Guns

BMG
BLACK MARKET GUNS

Our web address is 5xxqhn7qbtug7cag.onion Check it before ordering. If in doubt, email bmguns@secmail.pro Watch out for clone sites that steal your bitcoin.

Thank you for choosing us for your arms needs. We have large collection of guns and equipments for you to choose from. **All of our guns and equipments are brand new and have been checked thoroughly for defects.** We want you to feel safe when you're purchasing from us.

We ship all of our items with FedEx Standard Overnight within USA and FedEx International Priority for countries outside of USA. All shipping cost is free - as we have already added into the price.

All of our guns are brand new and 100% gun-oil free. So it clears custom without any issue. Handguns are taken apart and shipped inside power tool. Rifle or bigger equipments are taken apart and shipped inside computer case or other item. **All purchases comes with instruction for assembling and maintaining your equipments.** Due to the openness of this website, we cannot disclose example of the package.

Please enter the amount you wish to purchase below and fill in the form. (BTC value updates periodically via BTPAY)

(more photo)

NEW! CZ P-07 DUTY 9MM

Caliber: 9mm
Capacity: Two 15 round magazines included
Barrel: 4" Cold Hammer Forged
Weight: 1.7 pounds

$475 (0.0587 BTC)
amount 0

(more photo)

COLT MUSTANG POCKETLITE .380

Caliber: .380 ACP
Capacity: Two 6 round magazines included
Barrel: 2.75"
Weight: 11.8 ounces unloaded

$570 (0.0704 BTC)
amount 0

(more photo)

GLOCK 19 GEN 3

Caliber: 9mm
Capacity: Two 15 round magazines included
Barrel: 4" Cold Hammer Forged
Weight: 30.2 ounces loaded

$470 (0.058 BTC)
amount 0

Murder

Hitman service with escrow! Threaded Mode | Linear Mode

Author Message

Aircor
Unregistered

Hitman service with escrow! #1

Hitman service around Europe! WE DON'T WORK IN USA, only Europe!!!

Firstly, FULL escrow accepted, you don't have to pay anything before the job not done! Just When the job it's done.

Processing time is usually 2-3 weeks, depends to the target. It's possible urgency ordering! That's more expensive.
Also prices depend to the target. So I don't write prices, as I wrote it's depend the target!
We don't kill children under 17 years old!

If you have any questions please contact us:

2016-05-31, 10:17 PM

Counterfeit

BTC advert

IS BITCOIN THE ONLY FORM OF PAYMENT YOU ACCEPT?

Yes, it's secure and anonymous. We don't accept WU, moneygram, Paypal, etc. only Bitcoin.

WHERE IS SHIPPING AVAILABLE?

We ship world wide, we have own delivery technology, it depends on the size of your order. We guarantee 100% safe and discrete delivery!

Contraband markets

- Silk Road found a real demand.
- Less risky payments for contraband markets combined with user reviews and escrow is attractive for crime.
- Hacking services, drugs, guns, counterfeits, etc. available.
- Law enforcement is adapting and has had success.
- Ads for services implementing darkweb stores with BTC wallets.

Alt-coins

Coin capitalization

CRYPTOCURRENCIES	MARKET CAPITALIZATION	MINING METHOD	MINING ALGORITHM	
Bitcoin	$9,100,732,437	Proof of Work	Hashcash(SHA256d)	
Ethereum	$918,974,347	Proof of Work	EtHash	
Ripple	$217,734,595	Trust based consensus system.	Elliptic Curve Digital Signature Algorithm	
Litecoin	$178,179,674	Proof of Work	Scrypt	
Steem	$137,193,432			Steem is a b platform w posting, co
Monero	$110,589,734	Proof of Work	CryptoNight	
Ethereum Classic	$106,168,559	Proof of Work	EtHash	Hard fork o
Dash	$78,626,173	Proof of Work	X11	
NEM	$51,987,510	Proof of Importance	Rank Calculation	
MaidSafeCoin	$51,035,693	Proof of Resource	n/a	
Factom	$30,863,763	Proof of Work	SHA256	
Lisk	$26,548,000	Delegated Proof of Stake		
Dogecoin	$23,691,094	Proof of Work	Scrypt	
Nxt	$22,476,801	Proof of Stake	SHA256	
DigixDAO	$22,262,800	n/a	n/a	
BitShares	$18,426,950	Proof of Work	SHA512	
Peerplays	$16,863,900	Graphene	n/a	It's a gamin
Waves	$15,514,000	Consensus	n/a	

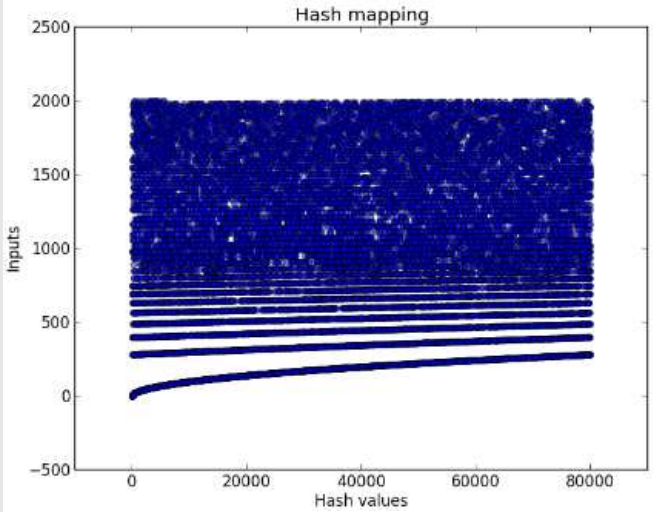
Ethereum

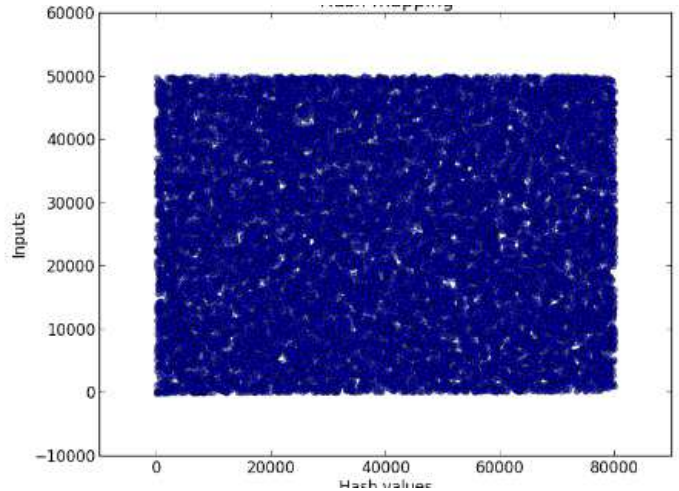
- Second largest capitalization.
- Transactions include scripting language.
- Smart contracts embedded within the payment.
- Possible future where contracts require experts in law, finance, and computer programming.
- Of course, many bugs left to discover.

Mining

- Proof of work.
- Proof of stake (Peercoin) in order to mine transactions, you have to show that you own enough coins.
- Proof of retrievability (Permacoin) to mine, you have to store large amounts of data. Solving problem is showing you can access data.
- Proof of importance (NEM) kind of like wuffie.
- Our lightweight mining.

Hash functions





- SHA-256 (doubled) NIST standard cryptographic hash.
- Scrypt designed for creating symmetric keys. Requires lots of memory. Hard to verify. Adapted to mining.
- EtHash (Ethereum) designed so that ASICS have no advantage. Very fast.
- Blake based on ChaCha stream cipher.
- X11 builds a pipeline of 11 different hashes. ASIC resistant.
- Cryptonight is memory intensive and ASIC resistant.

Privacy

Privacy enhanced coins

- BTC – privacy features. Each transaction with different address.
- Monero – mixes sender address with others. Destination address obfuscated. Transaction amount hidden.
- Zcash, Zcoin – use zero knowledge proofs for transactions. Transactions sent into a common pool.
- Dash – formerly Darkcoin – sends transactions through a number of obfuscation steps on different nodes. Popular with legal marijuana industry.

Mixing Services

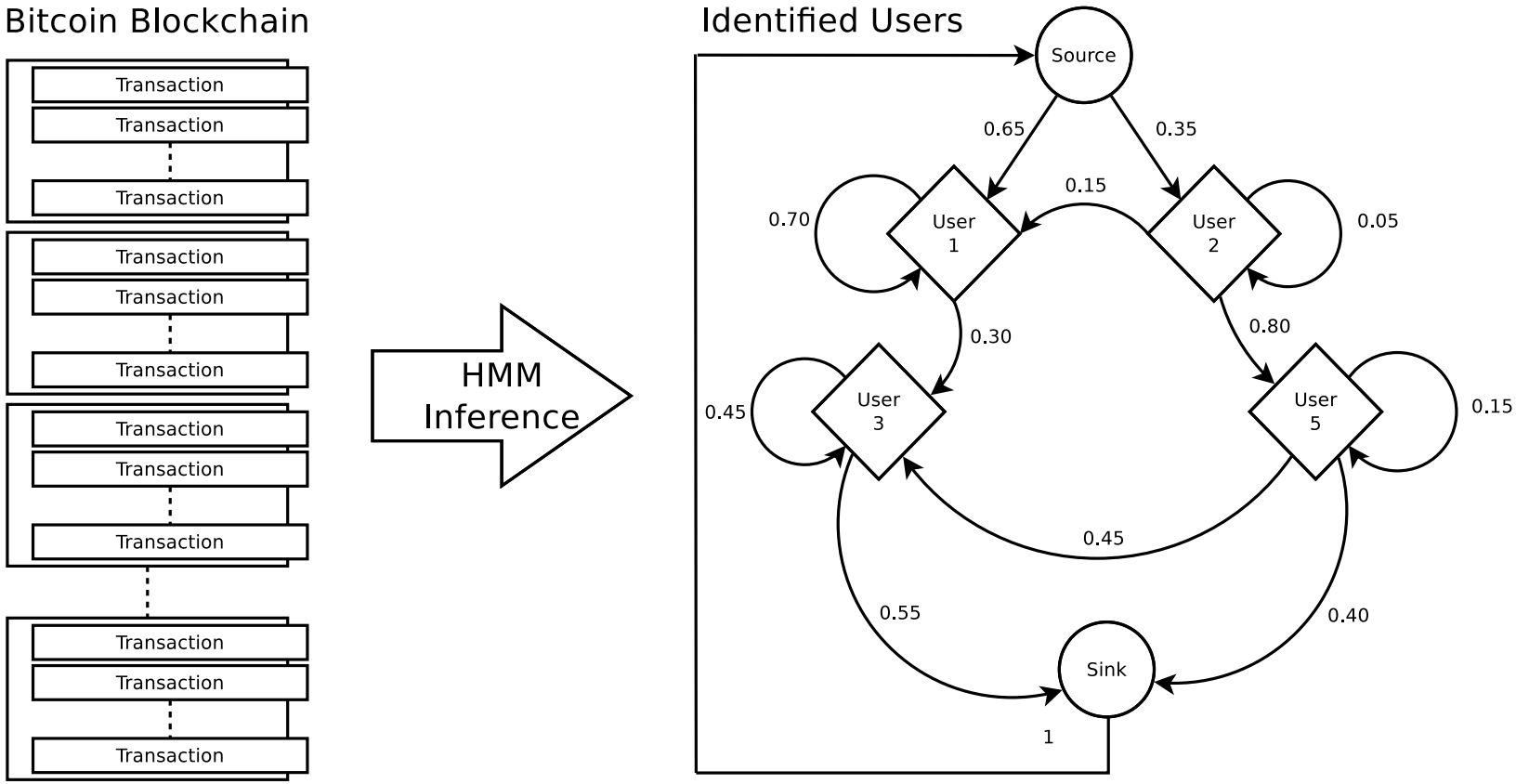
From The Hidden Wiki

List of mixing services:

- Bitcoin Fog (http://foggeddriztrcar2.onion/) - Bitcoin anonymization taken seriously
- Bitcoin Blender (http://bitblendervrfkzr.onion/) - Bitcoin mixing
- washbit (http://washbitcom2qv6wa.onion/) - Serious yet simple bitcoin washing.
- TOR Wallet (http://darktordcsm63mc2.onion/) - Bitcoin Wallet with integrated Bitcoin Mixer.
- Laundry King (http://1f3loxy2wibubh67.onion/) - The King of Bitcoin Laundry.
- (Helix) (http://grams7enufi7jmdl.onion/helix/GRAMS) Clean coins in 30 minutes.
- Shared Coin (http://sharedsnhrq2fnxg.onion/) - Free, fast and privacy-oriented Darknet Bitcoin Mixer, any amount from 0.0001 to 50 BTC.
- AnonCoin (http://ecfyacp4vwjiz363.onion/) - Clean your coins 100% anonymously! For a 0.1% fixed fee.
- Bitmixer.io (http://bitmixer2whesjgj.onion/) - High volume bitcoin mixing service (Tor Version)
- OnionWallet (http://owalletj32gvqkrj.onion/) - Anonymous Bitcoin Wallet and Bitcoin Laundry.
- EasyCoin (http://easycccnif2sfjfq.onion/)
- Pay Shield (http://payshld6oxbu5eft.onion/) - Sigaint's Darknet Tumbler (down - 02/2017).

Retrieved from "http://zqktlwi4fecvo6ri.onion/wiki/index.php?title=Mixing_Services&oldid=470268"

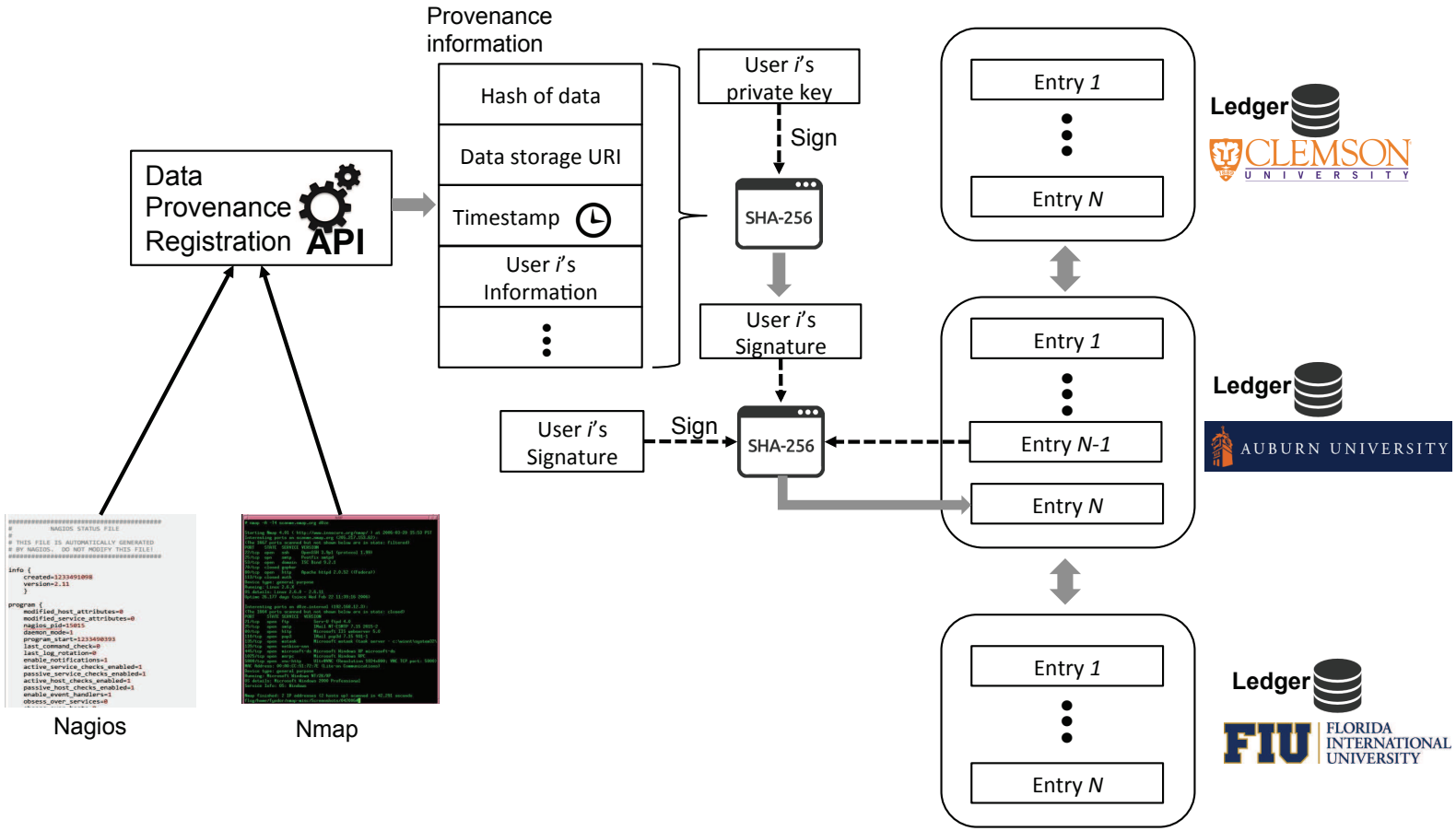
Bitcoin Money Laundering



- Infer transaction patterns from the publicly available blockchain.
- Identify users and link connected addresses.

Our project

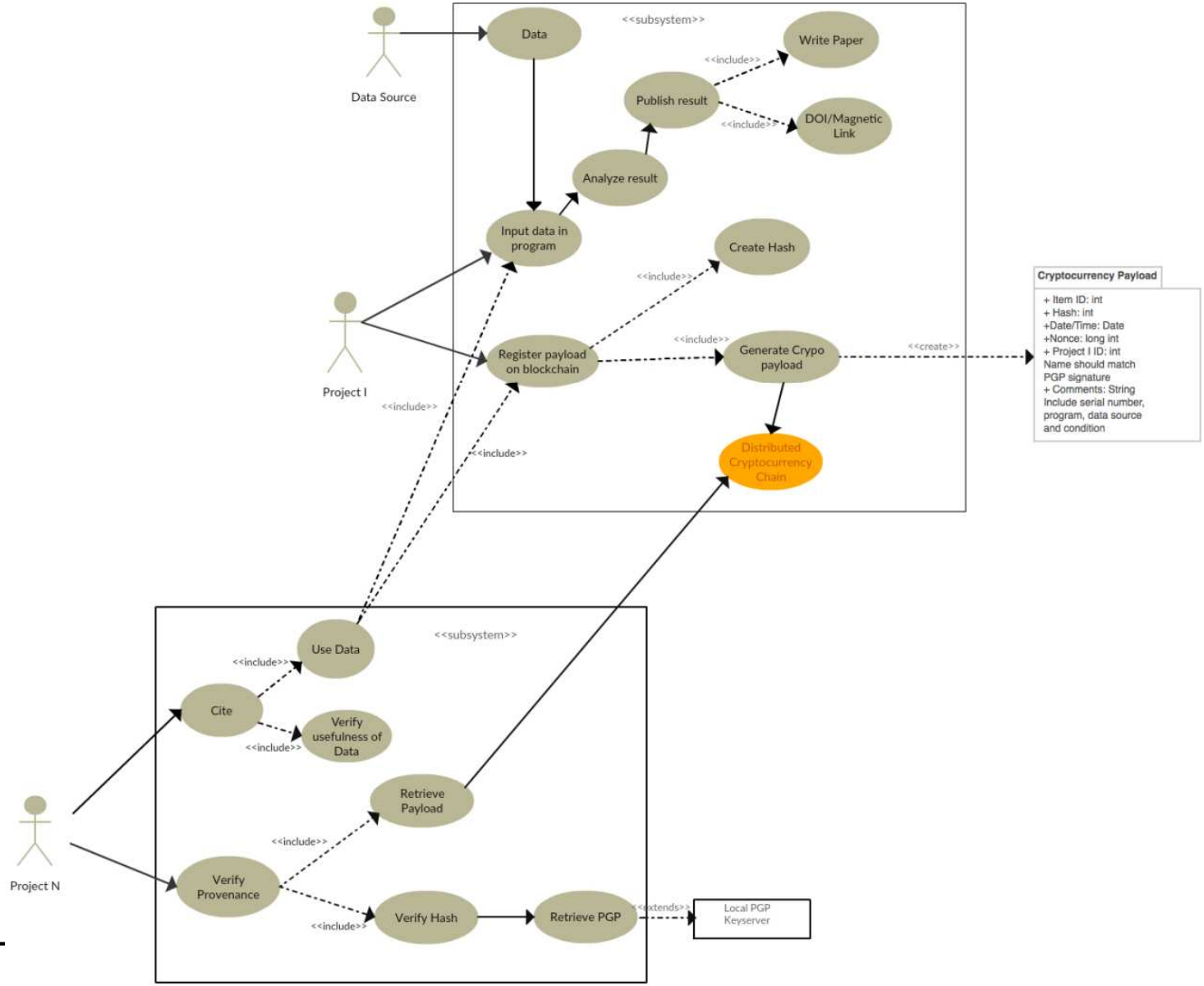
Use Blockchain to Secure Provenance Metadata



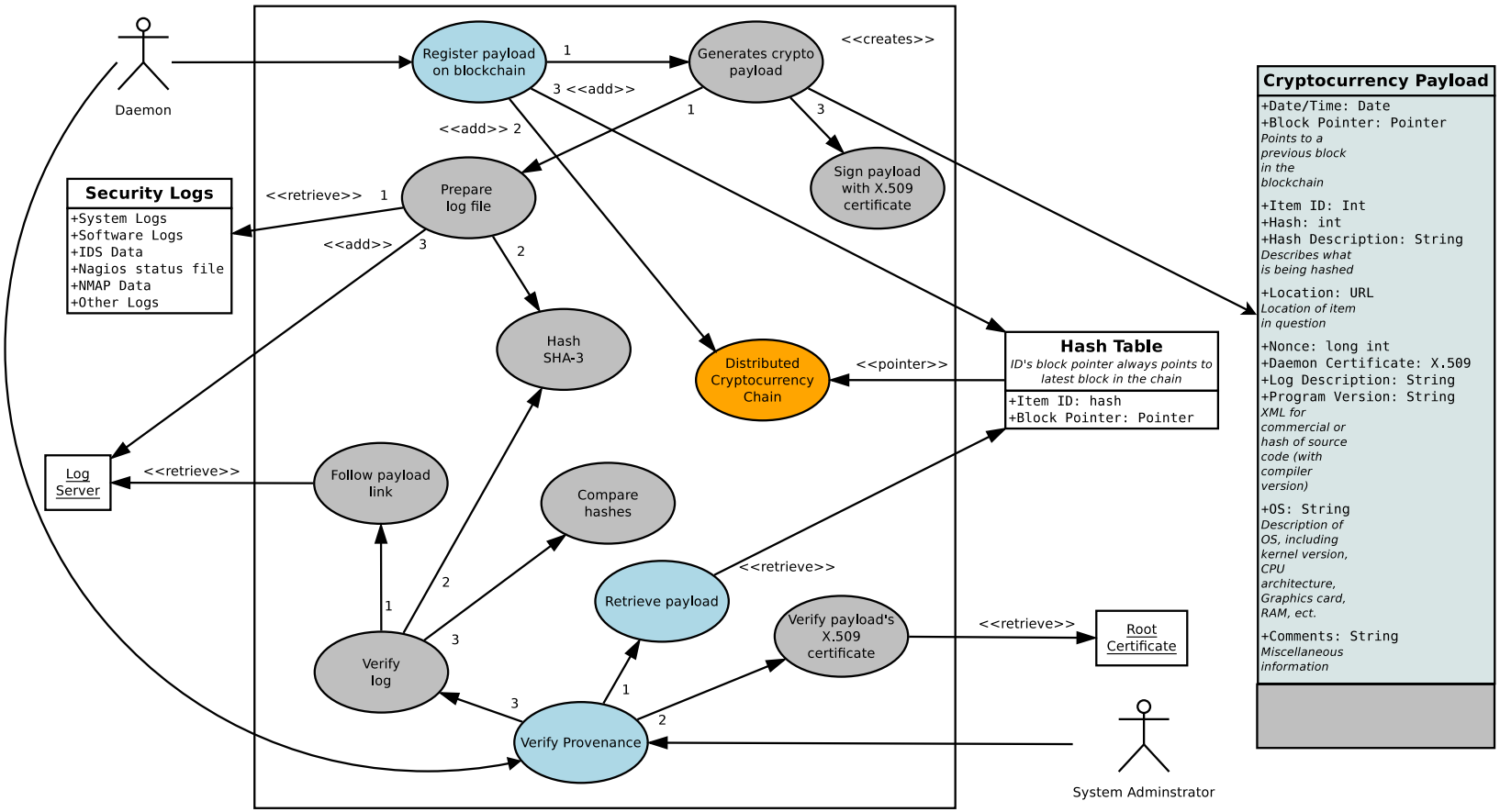
Lightweight mining, more robust than Byzantine fault tolerance (BFT)

Using\the\Blockchain\to\secure\provenance\meta-data\(ACCoEWebinarPresentation).(2017).

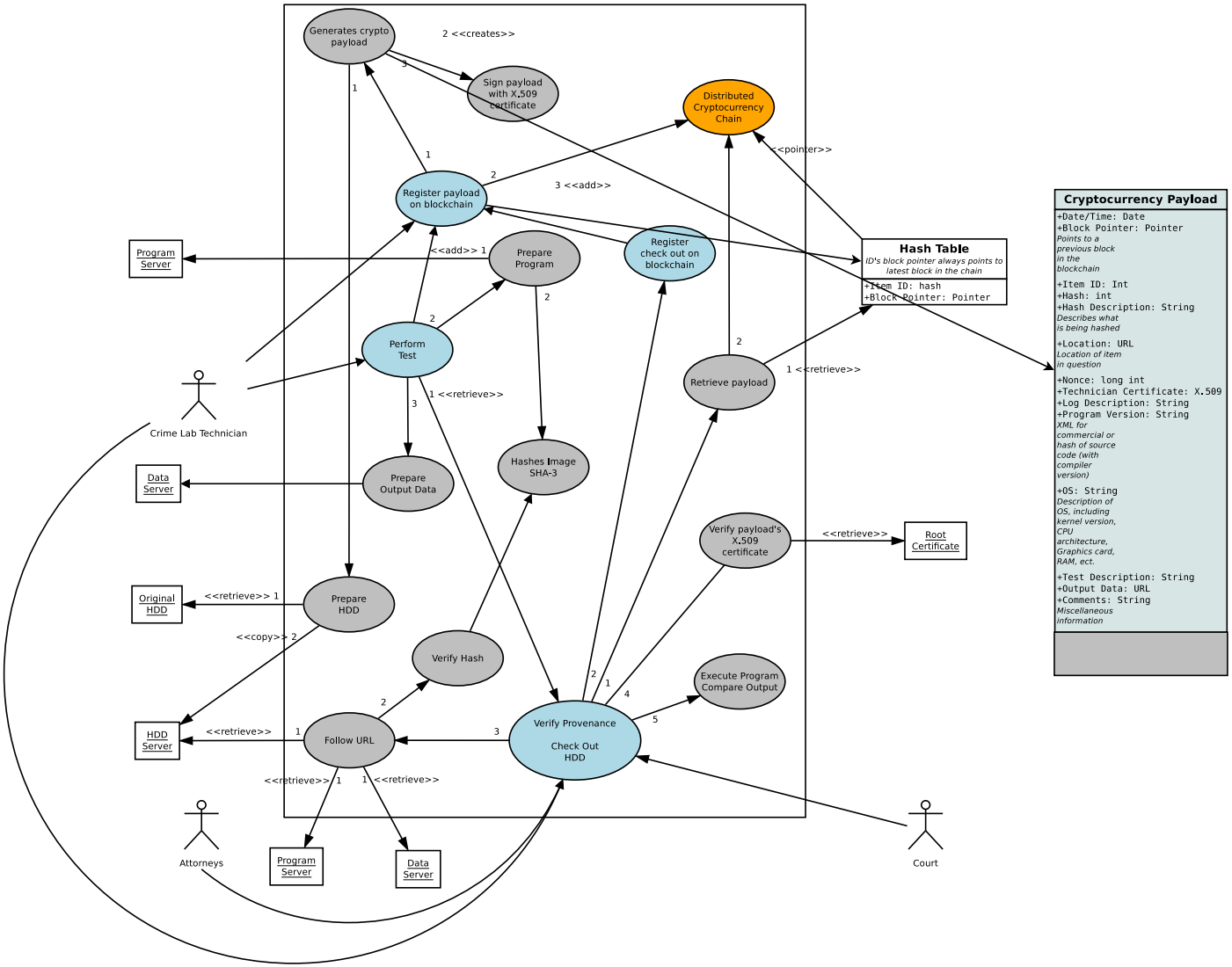
Academic integrity



Security logs



Digital forensics



Conclusions

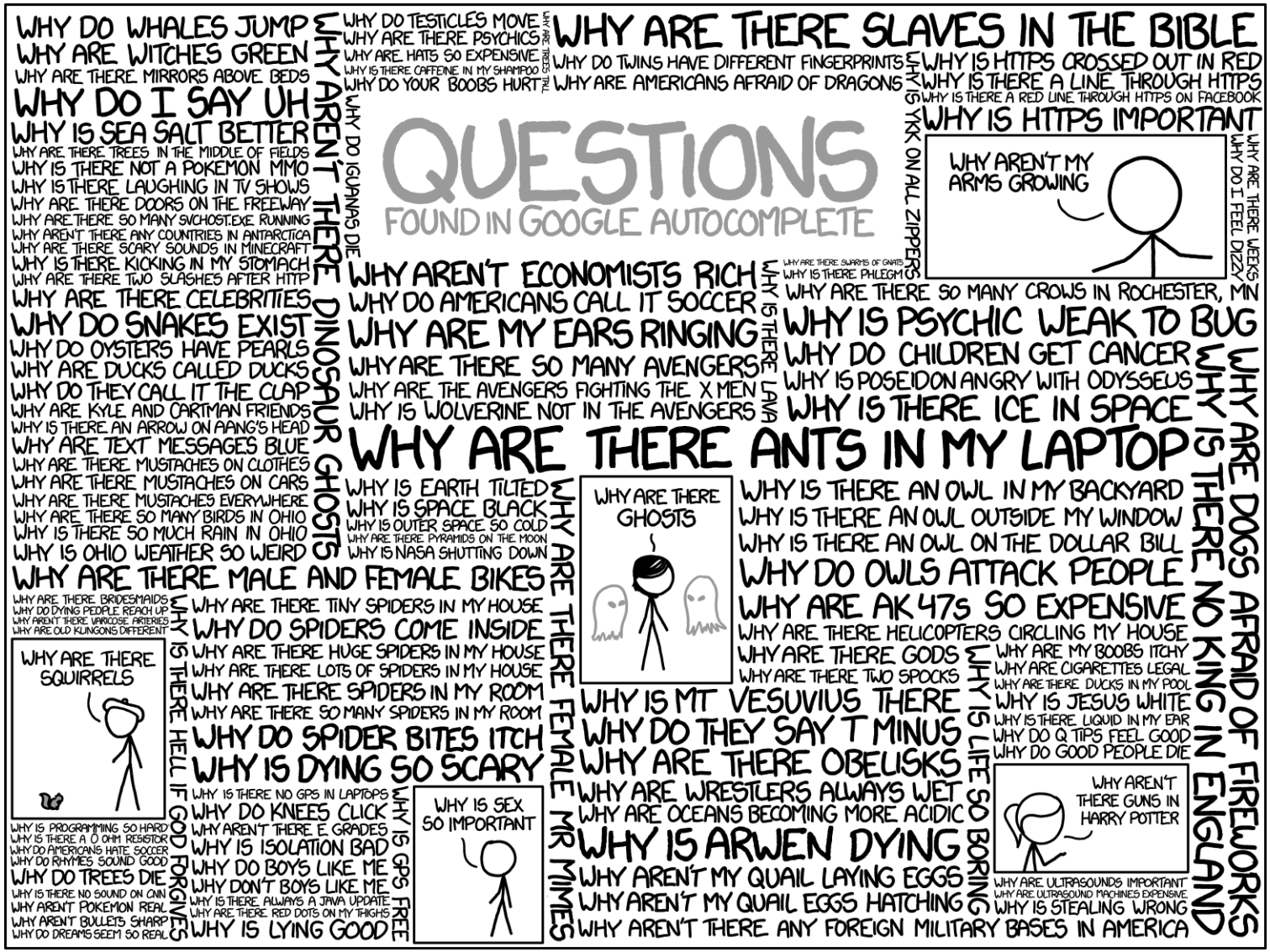
Conclusions

- ☐ Cryptocurrency natural evolution of the concept of money.
- ☐ Implementation required solution of hard technical problems.

- ☐ Elegant integration of many existing concepts.
- ☐ Darkweb is producing a number of social changes, challenges.
- ☐ Alt-coins evolving and disrupting ideas of finance/commerce.

- ☐ Privacy and money laundering present technical and social challenges.
- ☐ Our current project is ongoing and promising.

Questions?



https://xkcd.com/1256