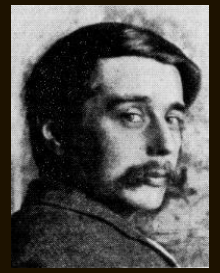
First Principles

The ***sophos*** (the experts)
the ***demos*** (the people)

The ***episteme*** (knowledge)
the ***doxa*** (opinion)

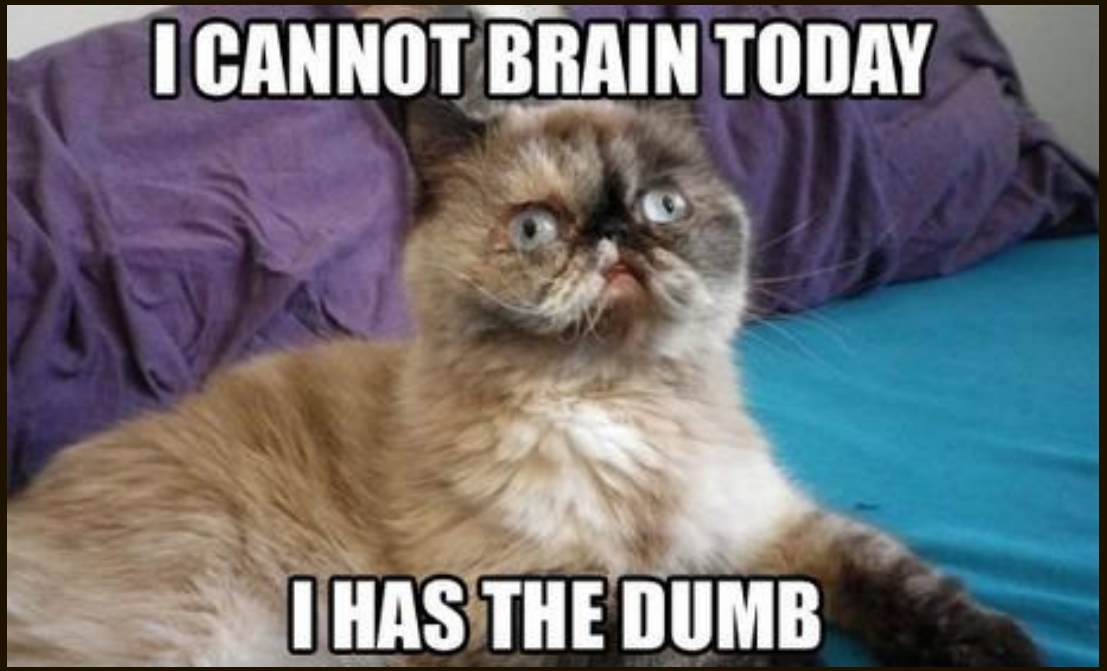


“

Civilization is a race between **education** and **catastrophe**.

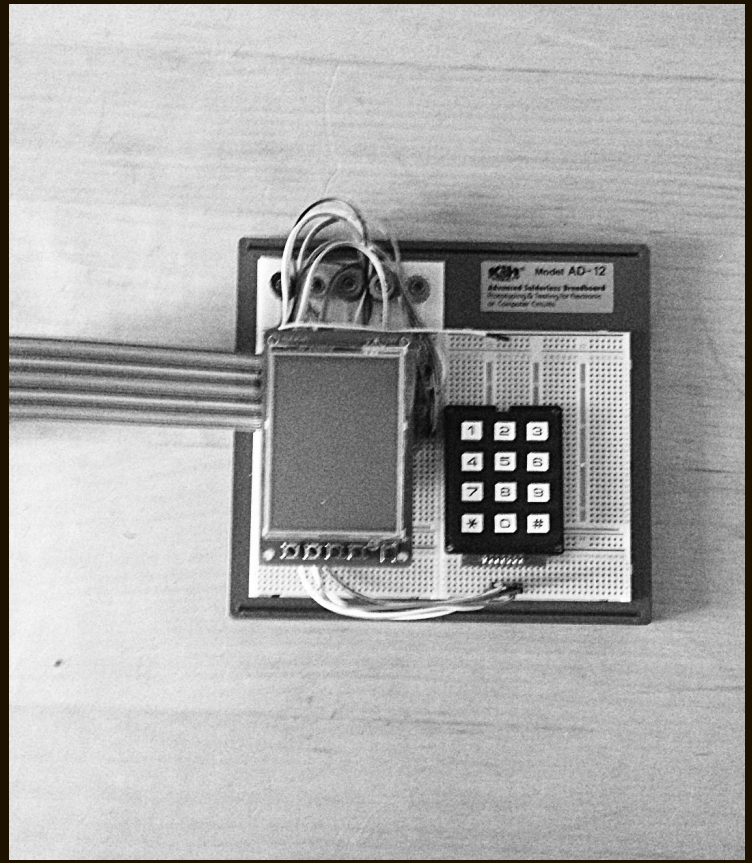
Let us learn the truth and spread it as far and wide as our circumstances allow. For the truth is the greatest weapon we have.

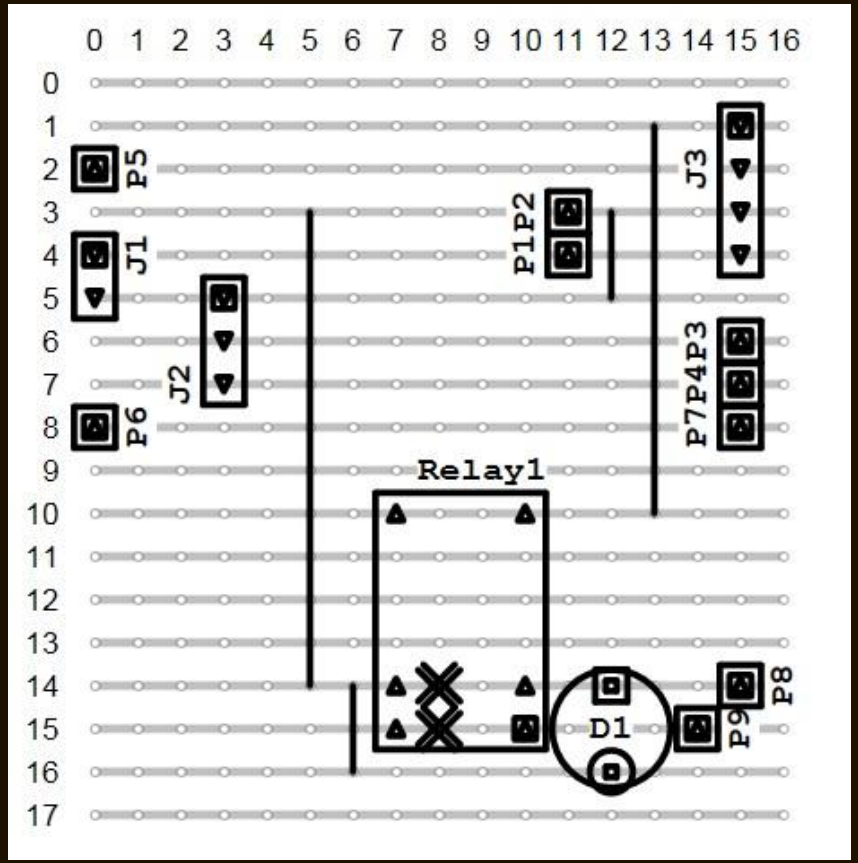
~H.G. Wells



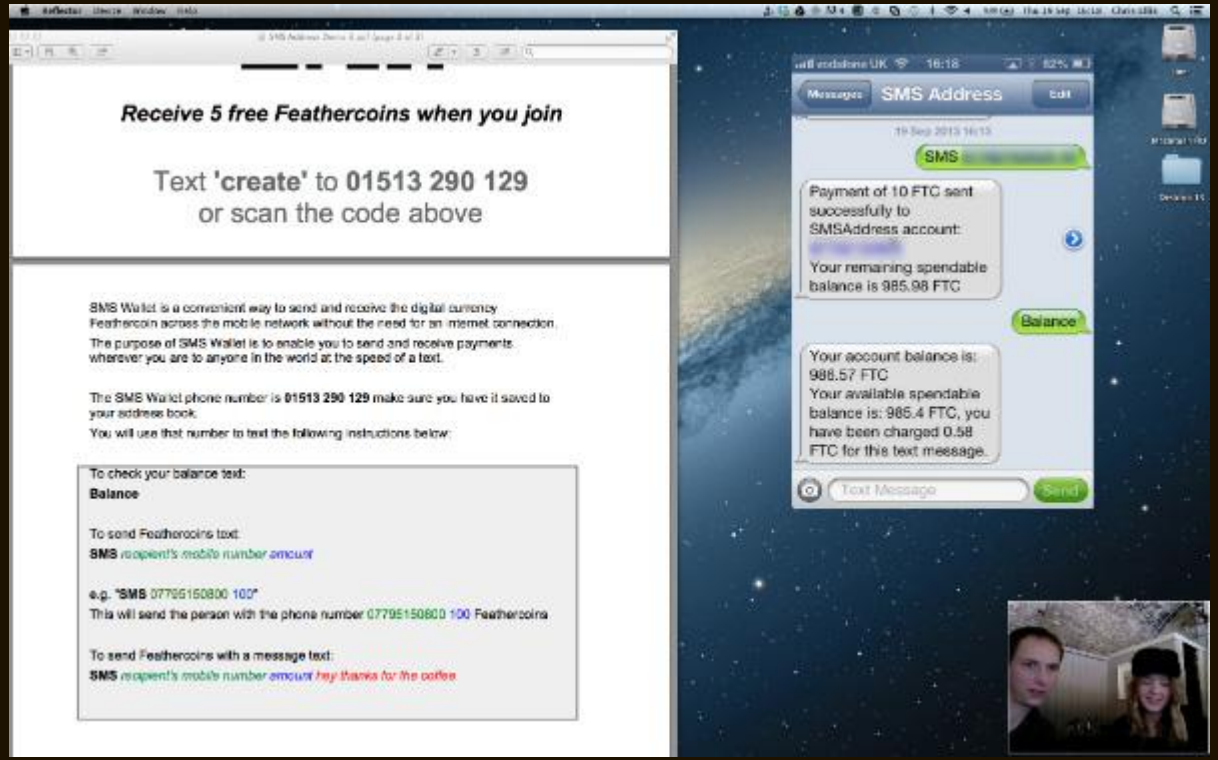
So why does it feel like this is what the internet has turned in to?

Feathercoin Point of Sale by Rob at Feathercoin





Open Source Hardware



User Experience Research

What I have learned so far:

- ‘Money’ was already digital
- But it’s not the money we want,
  - it’s each other;
  - where it takes us;
  - and who it helps us become
- Helping one another have impact
- Helping one another stay relevant
- “Help me make my contribution”

Bitcoin: A Peer-to-Peer Electronic Cash System

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

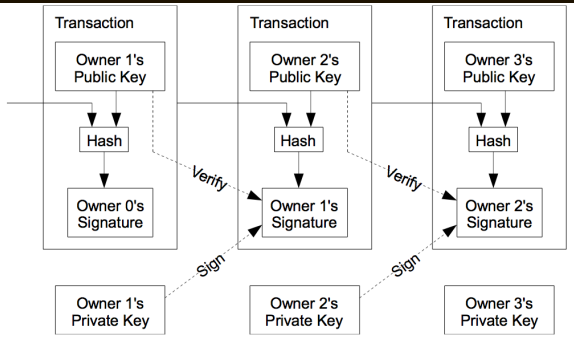
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must

> *Messages are sent on a best effort basis. 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****.*
>
> **~Satoshi Nakamoto**

Norman Rockwell's Freedom from Fear, 1943



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

6. Incentive

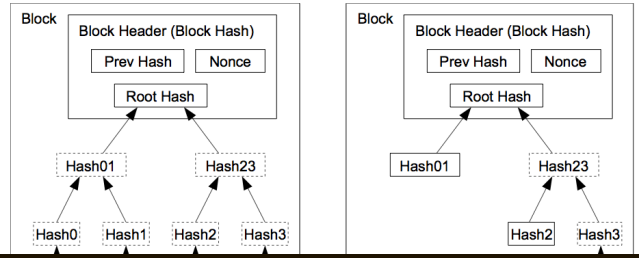
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

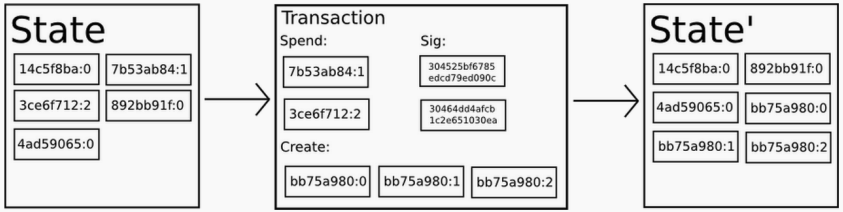
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Bitcoin As A State Transition System



From a technical standpoint, the Bitcoin ledger can be thought of as a state transition system, where there is a "state" consisting of the ownership status of all existing bitcoins and a "state transition function" that takes a state and a transaction and outputs a new state which is the result. In a standard banking system, for example, the state is a balance sheet, a transaction is a request to move $X from A to B, and the state transition function reduces the value in A's account by $X and increases the value in B's account by $X. If A's account has less than $X in the first place, the state transition function returns an error. Hence, one can formally define:

```
APPLY(S,TX) -> S' or ERROR
```

In the banking system defined above:

```
APPLY({ Alice: $50, Bob: $50 },"send $20 from Alice to Bob") = { Alic
```

From the Ethereum White Paper

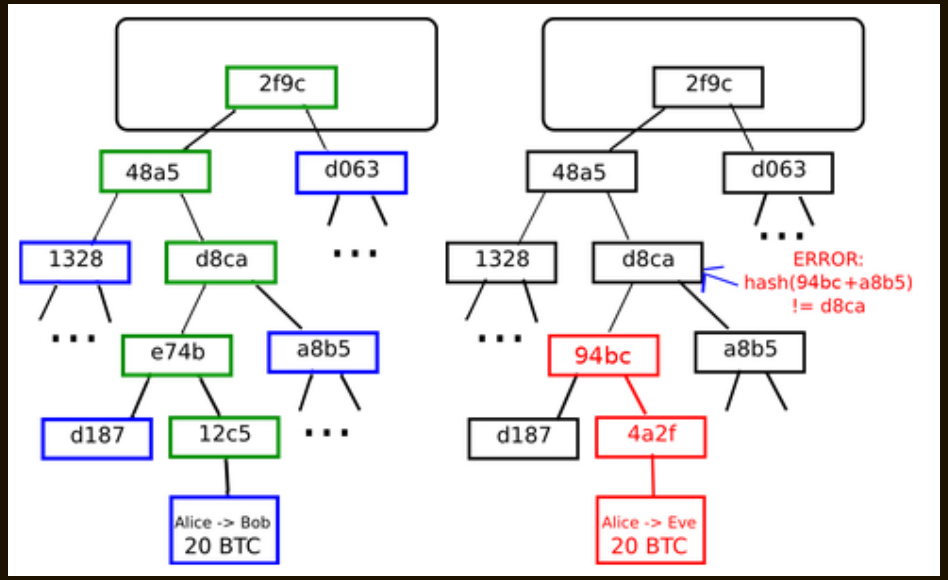
Merkle Root from block #330,459

18e44f11e94a586c

6f0a838ad92cb8b0

61b6f873e1c56635

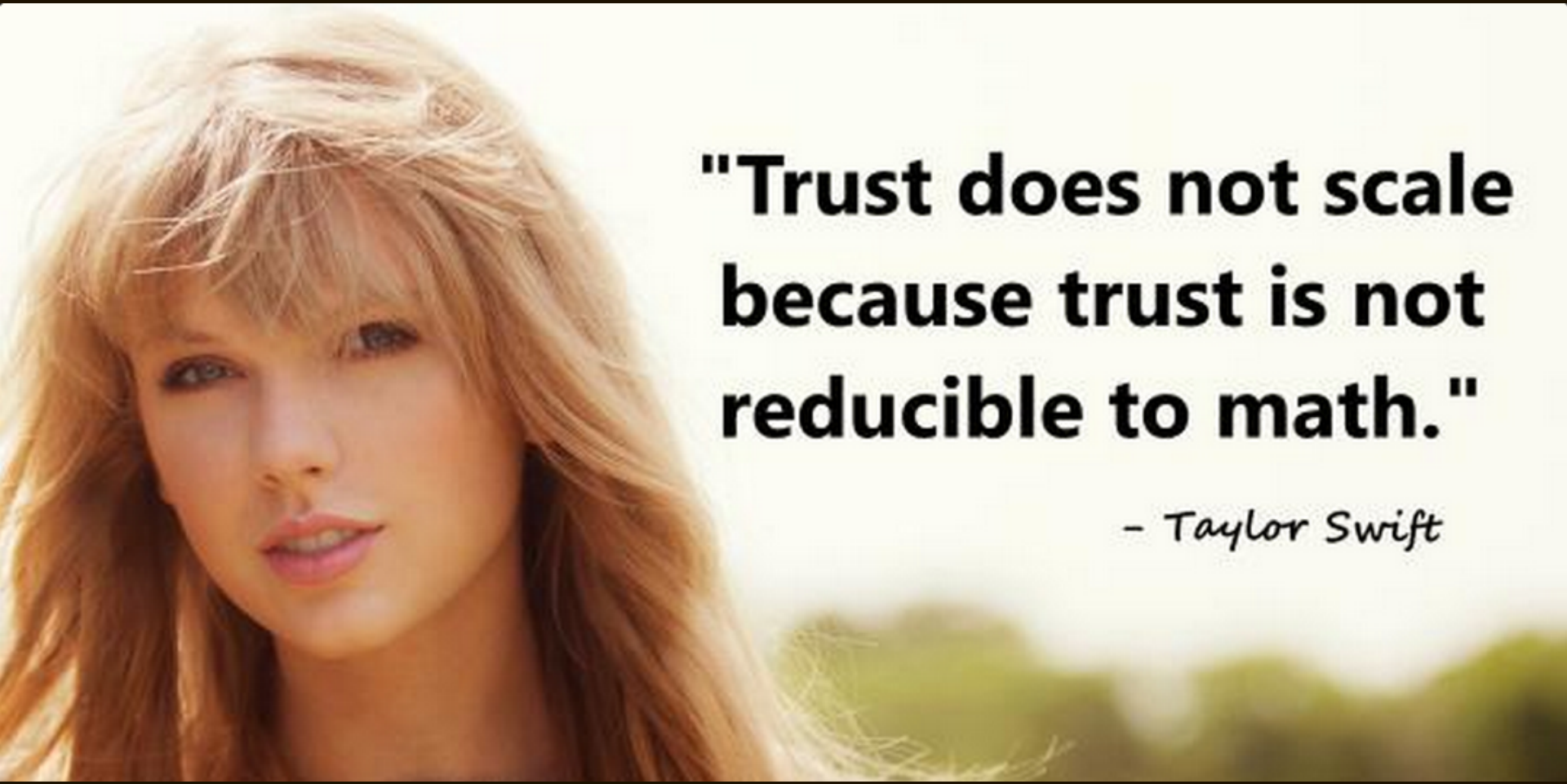
618bf84bca63eab7



Graphic from Ethereum Whitepaper

Learn more in [Bitcoin 101 - Merkle Roots and Merkle Trees]

Try for yourself with James De'Angelo's [Python Script]


"Trust does not scale because trust is not reducible to math."
- Taylor Swift

Chris Before Coffee - Power and Participation - 1st October 2014
Seek 36:18 for timestamp (opens a new window)

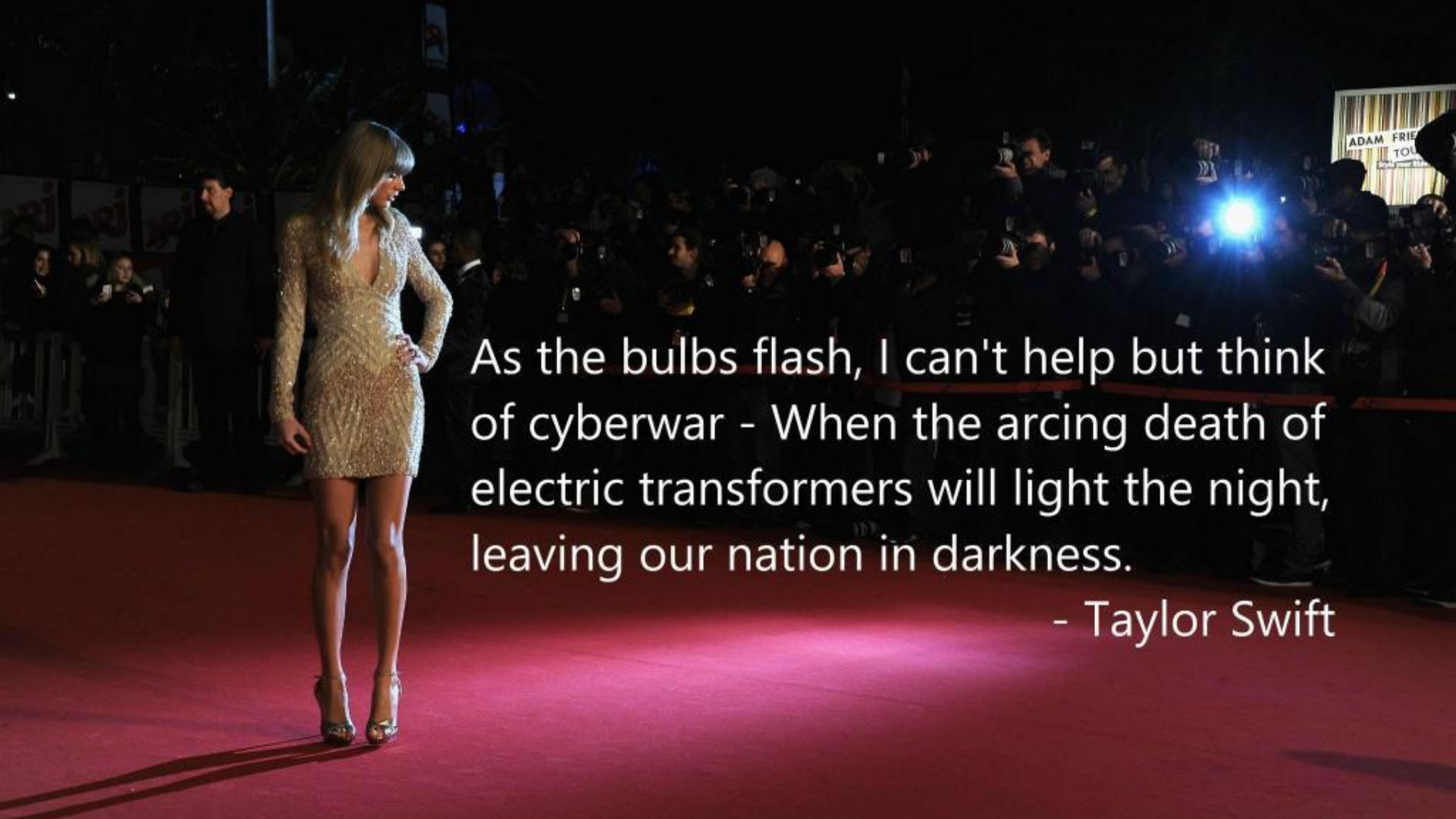
Photograph of James Bang in Action by Alex Hofford

Janina volunteered to be the World's First Blockchain ID
on the 24th October 2014

Apparatus

1. Laptop x2 (one belongs to organisers and the other to our new citizen)
2. Webcam
3. PGP Software Mac | Windows
4. Bitcoin wallet
5. Printer
6. Laminator
7. Cool looking World Citizen Passport design
8. Commercial Venue

```
-----BEGIN PGP SIGNATURE-----

Version: 10.3.2.15413


iQEVAwUAVEqlnew2pfEsR+bQAQoLrwf8DqjM+fHz24tGIzE9Eg1TlLXNdceO53O7

ZjDb98BIZ9SWYlp04acbcoac6QLrWHDhTIqK5qvAvLTkgYrI4rxP30JQDRoTR6F1

n2AQKKWXVrRSw6BHyzqMvCeVyY1xKKl02U+DJWqQ7MIEtLsubpnF4wSEu2ciQT9z

q38JxbCFIYIJGpbNCx20Qjla5Mc36ENJh7HKQ2ZHP3N/Gje0T2C8na7pL7r07UON

UK2XROeKLwTMp9pmqDtruNrUnIQgXZZHXhfuKOclQxmKvEkuW0sgqvrCCyf/pJUi

dFY/FzkV5dZ4Uzq46a7xq4vF8L0I8mRMy1x891yy/6R/iNb3fmgMgQ==

=fDst

-----END PGP SIGNATURE-----
```


As the bulbs flash, I can't help but think of cyberwar - When the arcing death of electric transformers will light the night, leaving our nation in darkness.
- Taylor Swift

Merci pour votre temps

Say ‘hi’ on Twitter @MrChrisEllis

PGP: Keybase.com/chrisellis

Github: https://github.com/MrChrisJ/fOSSa-2014

And: if you enjoyed this presentation show your appreciation

by transitioning the state of the distributed database with your private keys: