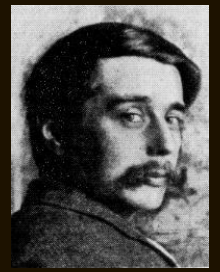


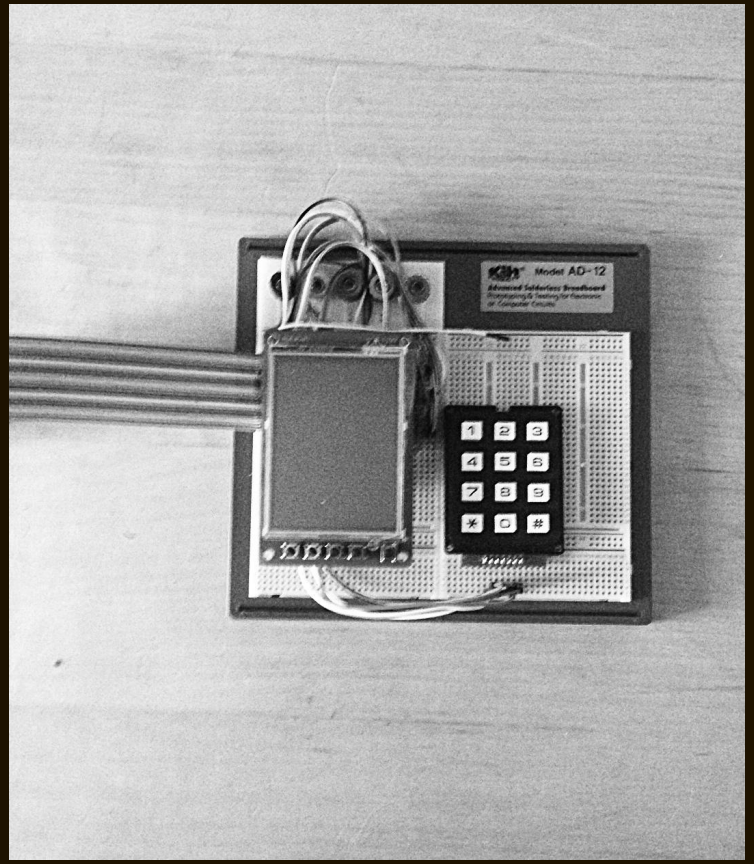
“

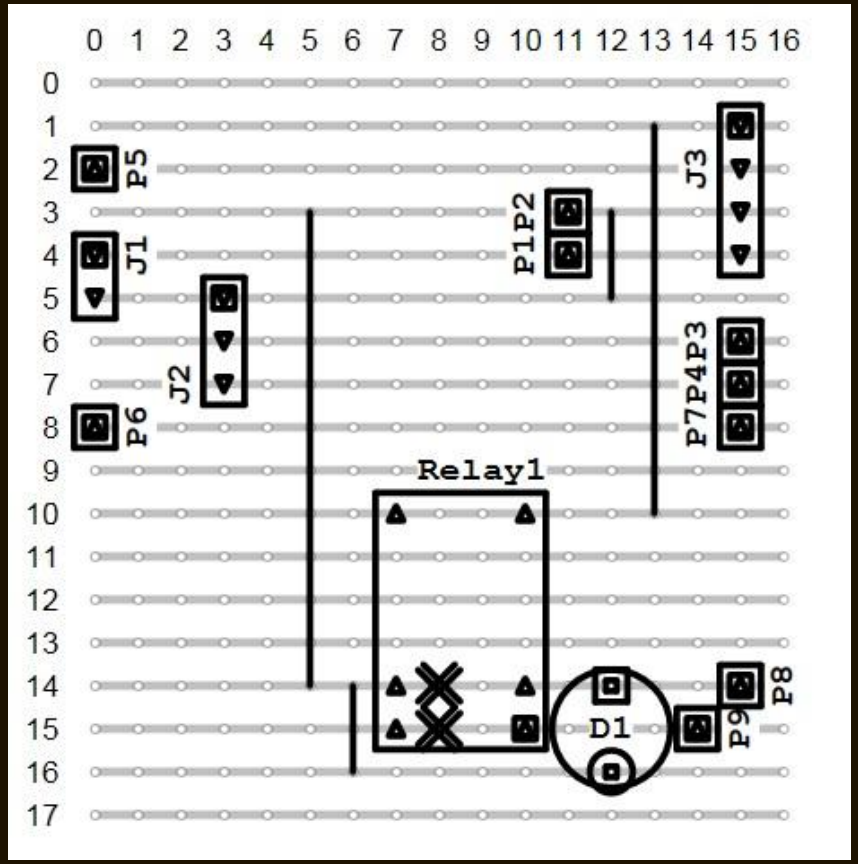
Civilization is in a race between **education** and **catastrophe**.

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

Feathercoin Point of Sale





Hardware is Open Source

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 is 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

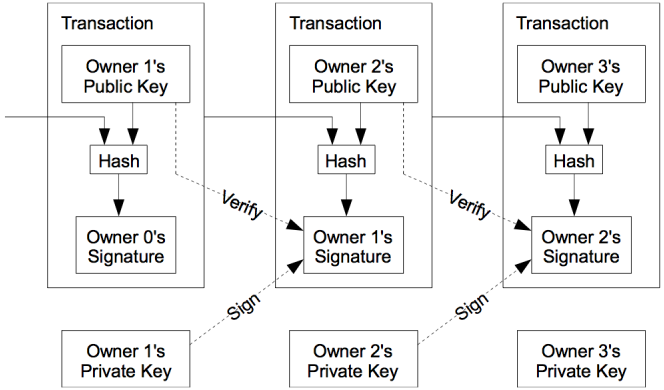
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required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

> *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

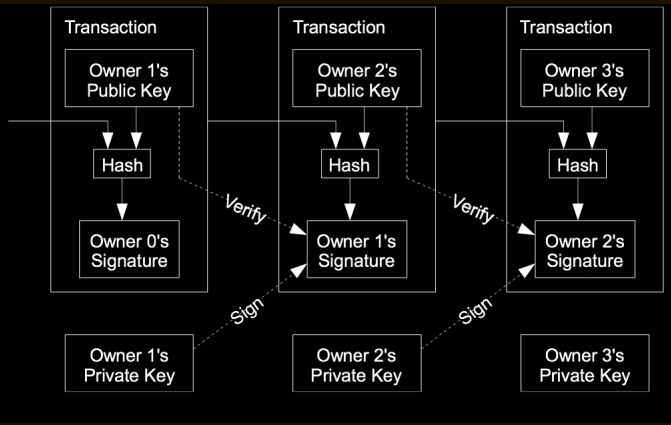


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new 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.

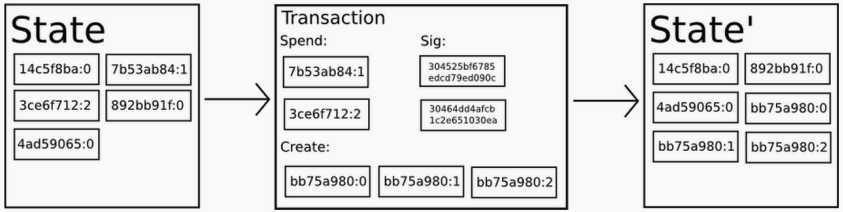
We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. 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.



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:

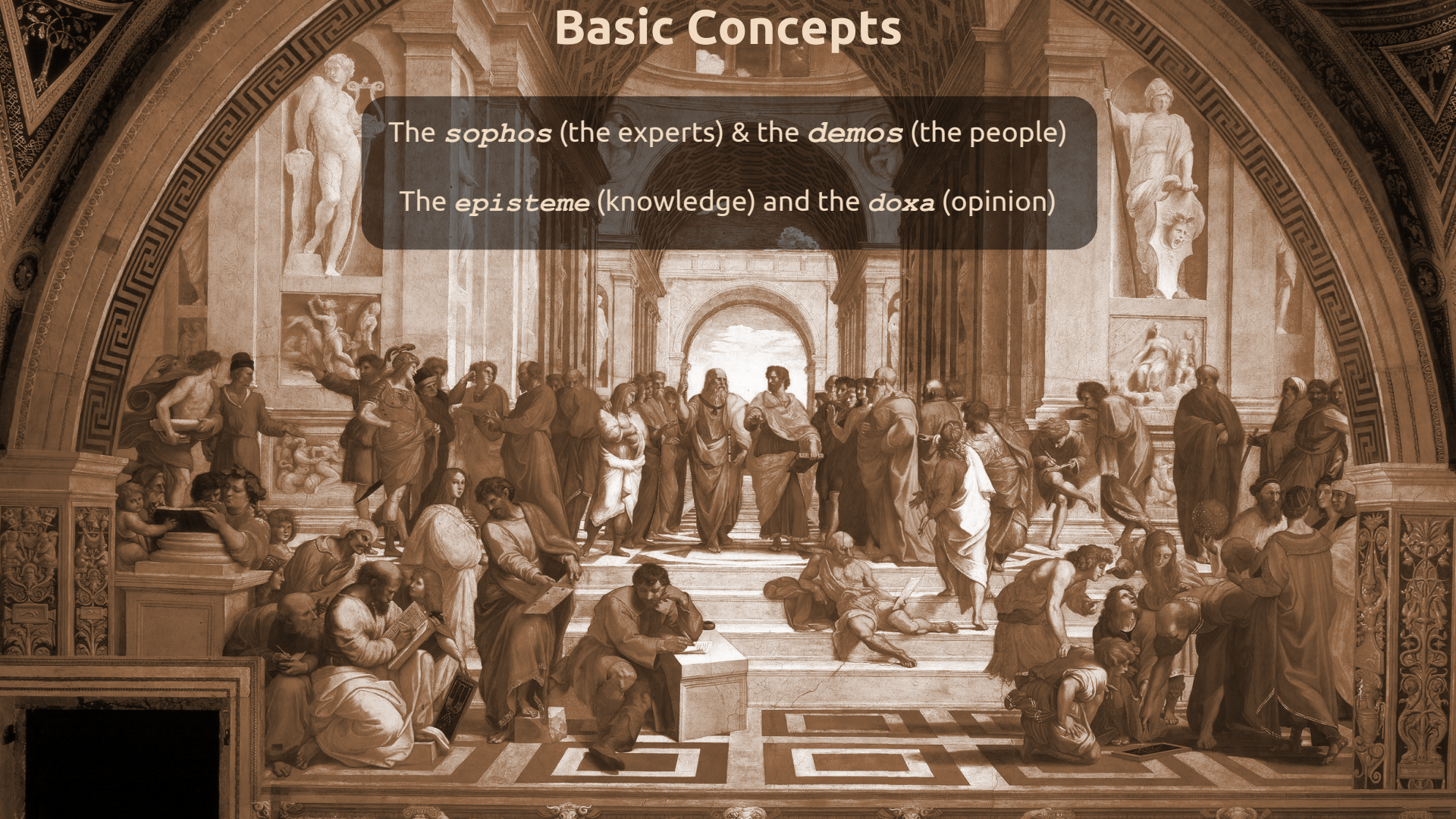
```
APPLY(S,TX) -> S' or ERROR
```

In the banking system defined above:

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

Merkle Root 18e44f11e94a586c
6f0a838ad92cb8b0
61b6f873e1c56635
618bf84bca63eab7

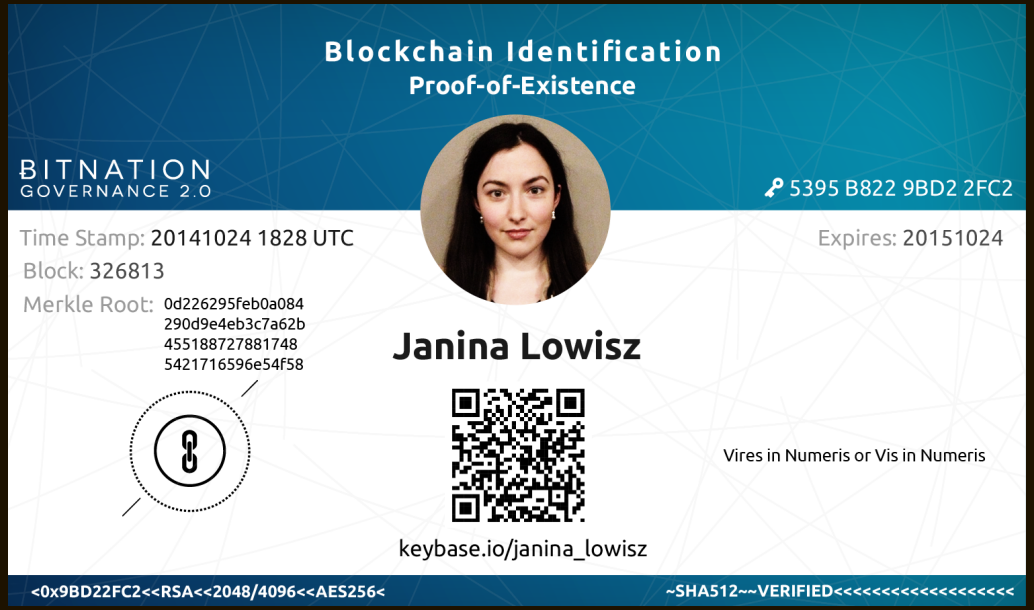
Basic Concepts



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

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

World Citizenship - A Case Study




Block 326813
Jd22695

My Underlying Assumptions

1. **Defining definition**
    a. To demarcate; to draw a border
    b. A good definition should be succinct
2. **Defining Entrepreneurialism**
    a. The ability to anticipate demand
    b. Well performing entrepreneurship is recognised
        i. One who meet the demands of others
        ii. De-risk uncertain environments
        iii. In order to help others achieve their goals

Defining Business

1. Defining Business

A sequence of activities

Thank-you for your time

Say ‘hi’ on Twitter @MrChrisEllis