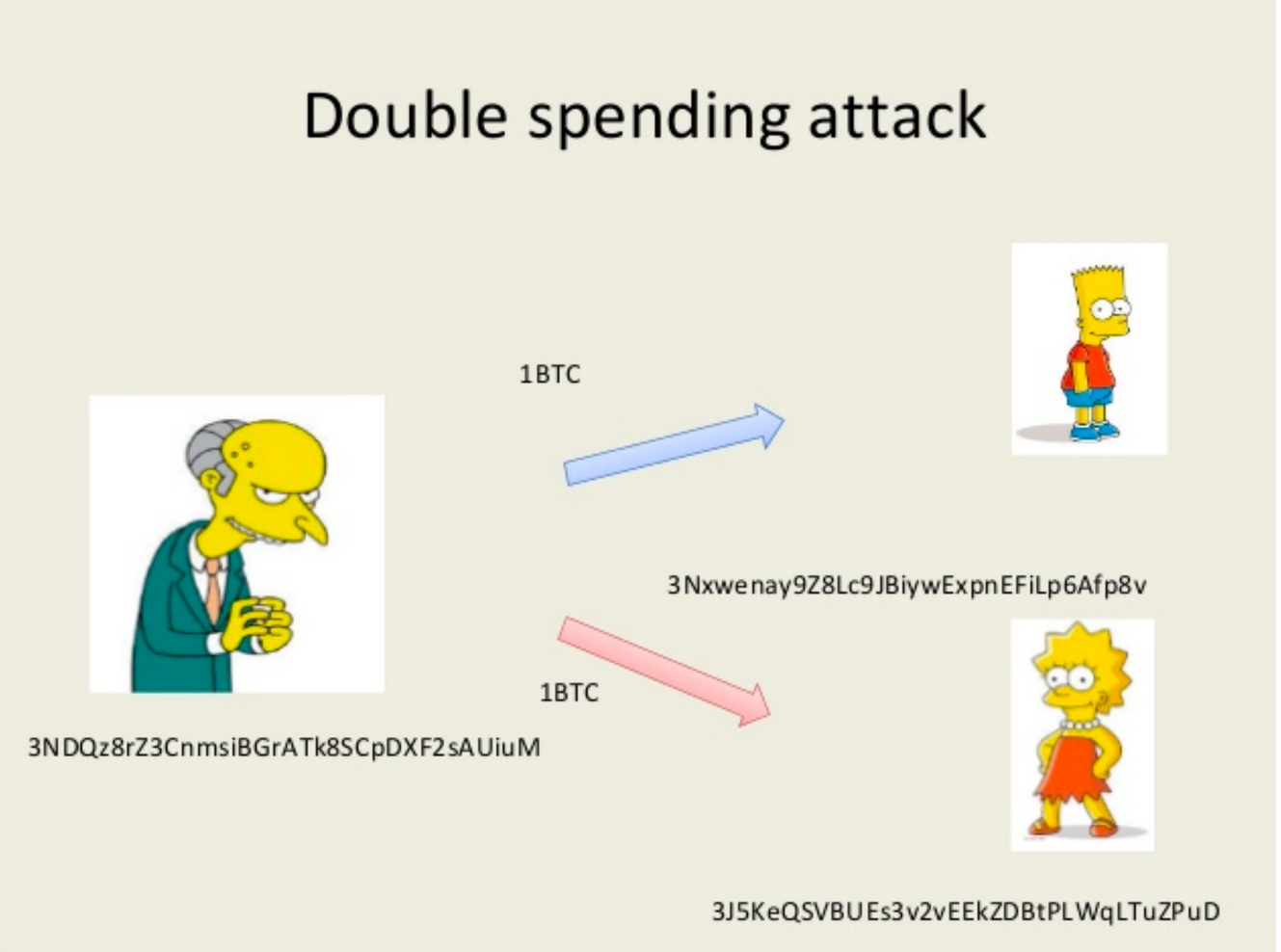
Blockchain

Double Spending Problem



Mint Problem

- Trusted-Third-Party
- Single-Point-of-Failure
- Censorship
- Debasement
- Theft/Confiscation

Consensus

- Coordination and Agreement of a group of people
- Agreement of a group of people on the order and character of transactions
- Coordinating people to build the record of transaction
- Getting people who do not trust each other to agree to a single record of truth
- Maintaining and securing this record
- Cocreating this record

Satoshi's Proposition

To Mine, Or Not to Mine

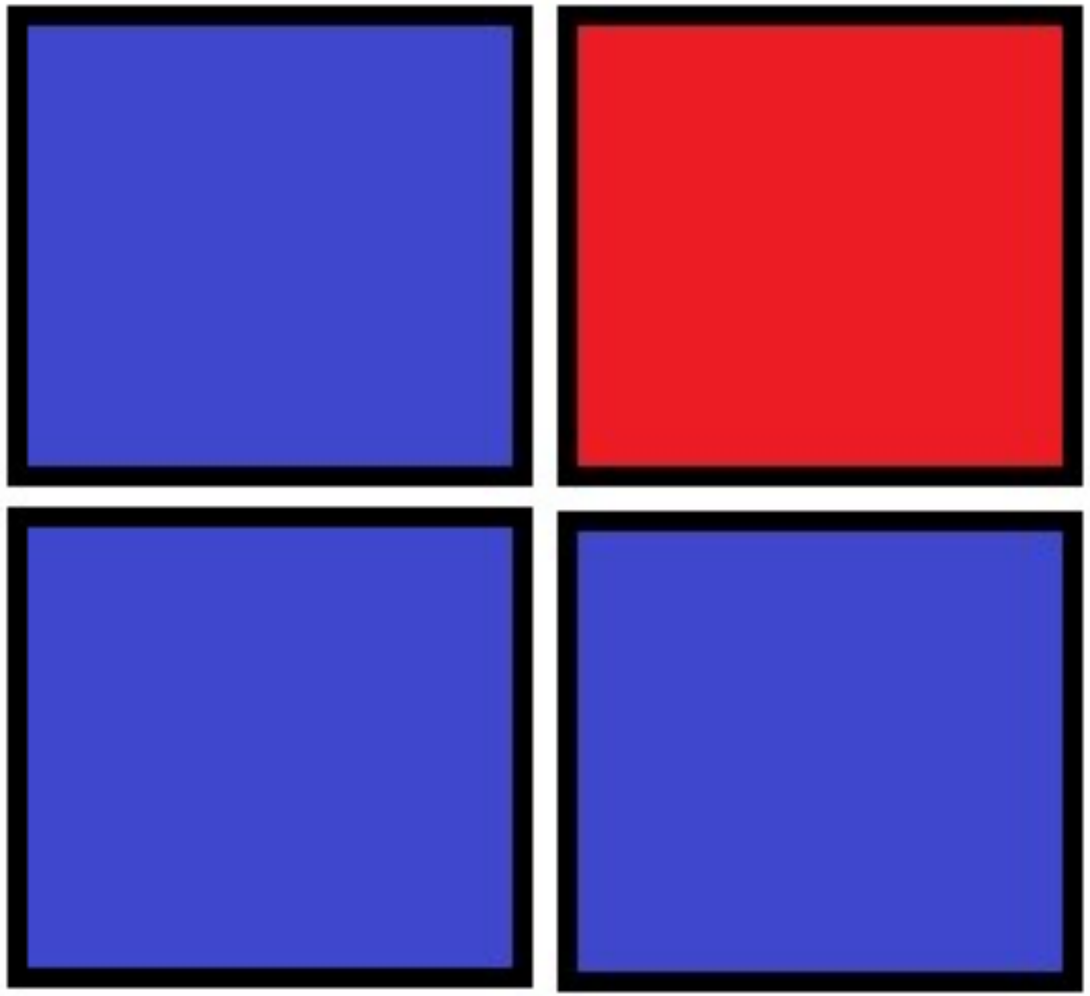
Satoshi's Proposition

	Don’t Mine	Mine
Don’t Mine	0, 0	0, 50
Mine	50, 0	25, 25

Prisoners’ Dilemma

	Rat	Don’t Rat
Rat	2.5, 2.5	0, 5
Don’t Rat	5, 0	0, 0

Schelling Point



Two General's Problem

"Two armies, each led by a different general, are preparing to attack a fortified city. The armies are encamped near the city, each in its own valley. A third valley separates the two hills, and the only way for the two generals to communicate is by sending messengers through the valley. Unfortunately, the valley is occupied by the city's defenders and there's a chance that any given messenger sent through the valley will be captured.

While the two generals have agreed that they will attack, they haven't agreed upon a time for attack. It is required that the two generals have their armies attack the city at the same time in order to succeed, else the lone attacker army will die trying. They must thus communicate with each other to decide on a time to attack and to agree to attack at that time, and each general must know that the other general knows that they have agreed to the attack plan. Because acknowledgement of message receipt can be lost as easily as the original message, a potentially infinite series of messages is required to come to consensus.

The thought experiment involves considering how they might go about coming to consensus. In its simplest form one general is known to be the leader, decides on the time of attack, and must communicate this time to the other general. The problem is to come up with algorithms that the generals can use, including sending messages and processing received messages, that can allow them to correctly conclude:

Yes, we will both attack at the agreed-upon time."

Consensus

“The consensus problem requires agreement among a number of processes (or agents) for a single data value. Some of the processes (agents) may fail or be unreliable in other ways, so consensus protocols must be fault tolerant or resilient. The processes must somehow put forth their candidate values, communicate with one another, and agree on a single consensus value.”

Consensus Attacks

- Sybil Attacks
  - Censorship
  - Debasement
  - Theft/Confiscation
- (Hal) Finney Attack, 51% Attacks

Economic Calculation Problem

- Planners don’t have information
- No way to turn Subjective Values into Objective information?
- Discussed by Austrian Economists Friedrich Hayek and Ludwig Von Mises
- Part of the Socialism vs Capitalism Debate
- Predates the Internet
- “Economic Calculation in the Socialist Commonwealth”, 1920
- Qualitative Reduction in cost of calculation and access to information results in qualitative expansion of possibilities

Collective Action Problem

All individuals would be better off cooperating but fail to do so because of conflicting interests between individuals that discourage joint action

- Cryptocurrency requires massive scale cooperation between people who do not know or trust each other
- Participants Can Enter and Exit at will
- Expand the set of people you can collaborate with and the ways in which you can collaborate
- Qualitative Reduction in cost of coordination/collective action results in qualitative expansion of possibilities

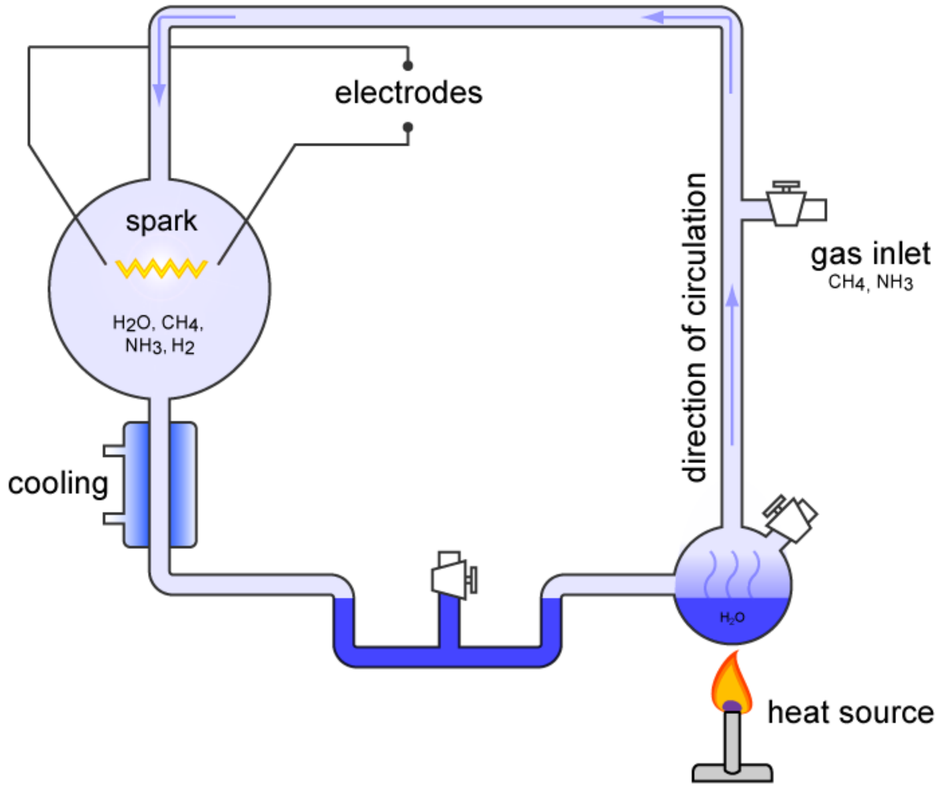
We All Win Together

OP_RETURN

Standard way to put information onto the Blockchain

- Replaced non-standard ways to post ways to
- Provably unspendable, therefore it can be pruned
- Do not sit in the UTXO set
- 80 Bytes in BTC Chain
- 100 kb in BSV Chain
- Basis For Several OP_Return Protocols

Miller–Urey experiment



Proof-of-Existence

Prove that data existed in a certain state at a certain time. From that point on, anyone with access to the data can verify it against the blockchain version.

- **Post the Actual Data/Document**
- **Post a Proof (Hash) of the Data/Document**
- **Prove a Document's Existence without revealing its contents**
- **Prove an agreements existence without revealing its contents**
- **Apps: Commitment Scheme, Blockchain Notary, Decentralized internet**

Proof-of-Process

- Publish Proof of Each Step in a Business Process
- Party that completes step in process posts (and signs) proof
- Auditable by a network of parties that don’t trust each other

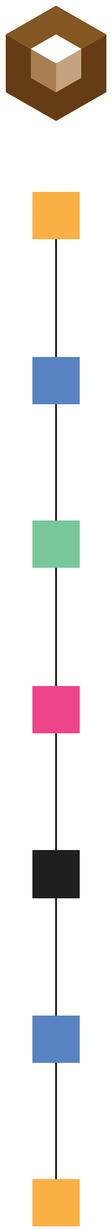
Programmatic Money

Programmatic Money

Satoshi Embedded Programmatic Functionality into the Blockchain
Money that can be conditionally spent based on your stipulations

Multisignature

A dynamic number of parties can participate in any transaction



Smart Property

Transactions can encode arbitrary information: voting, messaging, “smart property”,

Escrow

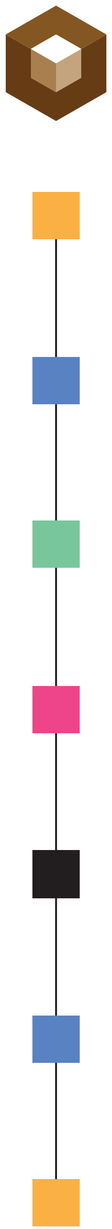
Bounties

Crowdfunding

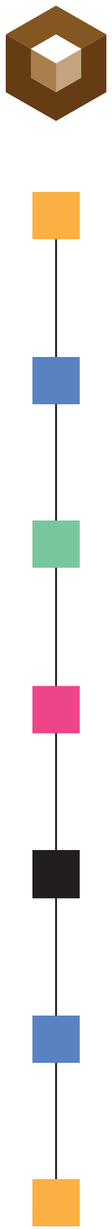
Smart Contracts

Printing Press

Printing Press



Censorship Resistance



Arrow of Time

Decentralized Internet + Web