463.8 Bitcoin

CS463/ECE424

University of Illinois

Reference:

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

https://bitcoin.org/bitcoin.pdf

Bitcoin and Cryptocurrency

https://www.bbc.com/news/world-latin-america-58579415
https://www.bbc.com/news/technology-58473260

Fear and excitement in El Salvador as Bitcoin becomes legal tender

El Salvador has become the first country to accept Bitcoin as legal tender in a move that has got the nation and the world debating the opportunities and dangers of cryptocurrency.

Bitcoin fluctuations

The value of Bitcoin has risen and fallen dramatically in the last year.

It went from about $10,000 for a single coin in September 2020 to a high of $63,000 in April 2021 then falling to $30,000 in July this year.

Overview

- Currency systems rely on trust (government, bank). Is it possible to build a currency without trusted authorities?

- Use a Proof of Work scheme to place authority in the hands of a distributed preponderance of capability

- Bitcoin: implemented in practice, multi-billion-dollar capitalization
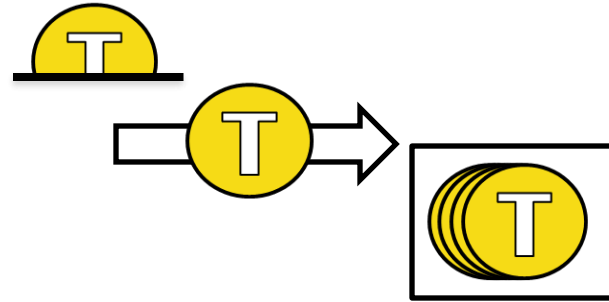
Bitcoin's Three Main Protocols

Network: How can we share transactions & history?

Transactions: How can we agree what the "history" means?

Consensus: How can we agree on "one global history"?

Outline

- **Part 0**: a little history

- **Part 1**: TheoryCoin
  - How to **create** coins
  - How to **transfer** coins
  - How to **store** coins

- **Part 2**: diff(,)

- **Part 3**: Problems and issues
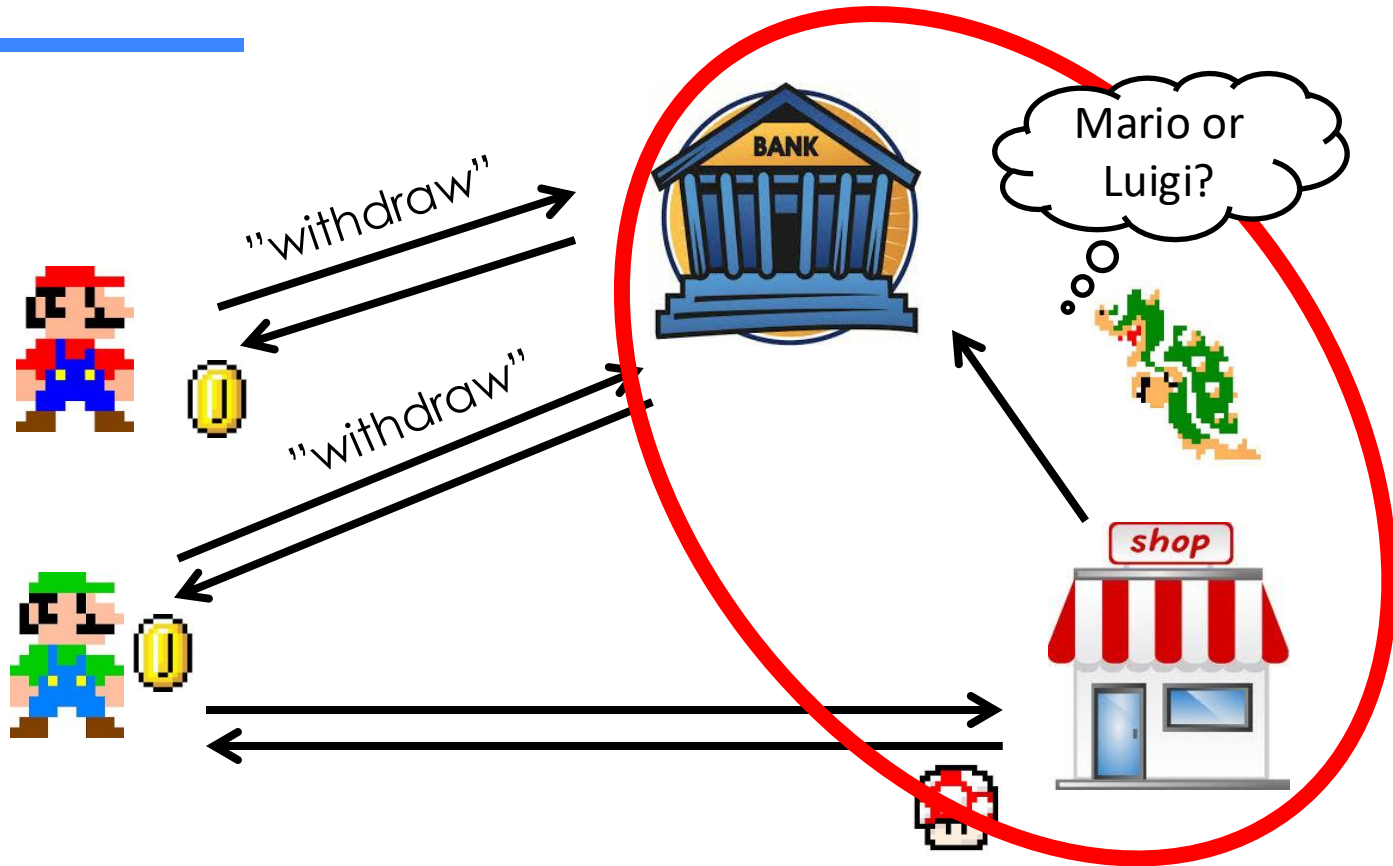
The 1990s
David Chaum and Anonymous ECash

"The difference between

a bad electronic cash system

and well-developed digital cash

will determine whether

we will have a dictatorship

or a real democracy"

(attributed to Chaum)

Anonymous Payments

Either the bank or the shop knows who spent the coin

Chaum's Anonymous e-Cash

- **Anonymous**
- **Secure** (no double-spending)
- Only **transfer** (no creation/storage)

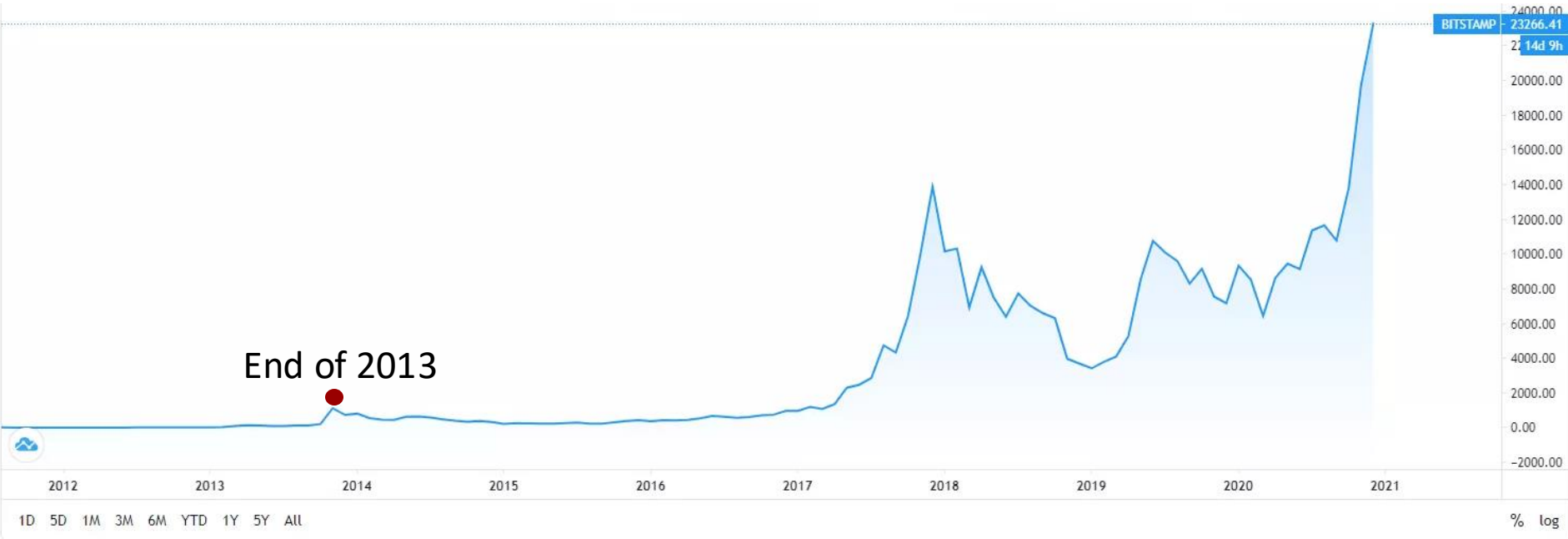Still have to work with real banks

…and declared **bankrupt** in 1999

Chaum's Anonymous e-Cash

- **Problem 1:** How do we assign value to coins?

- **Problem 2**: No use-case for anonymous payments in the 90s

The Advent of Bitcoin

- 2009: **Bitcoin announced** by Satoshi Nakamoto

  – Pseudonym for person or group of people

- 2009-2011: slow start…

- 2011-2013: Silk Road, Dread Pirate Roberts

  – Illegal business! Best place for anonymity

- End of 2013: **Bitcoin price skyrockets**
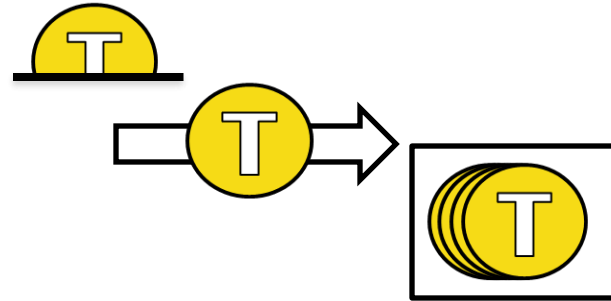
  – and the world notices!

Price is Even Higher Now

Outline

- **Part 0**: a little history

- **Part 1**: TheoryCoin
  - How to **create** coins
  - How to **transfer** coins
  - How to **store** coins

- **Part 2**: diff(
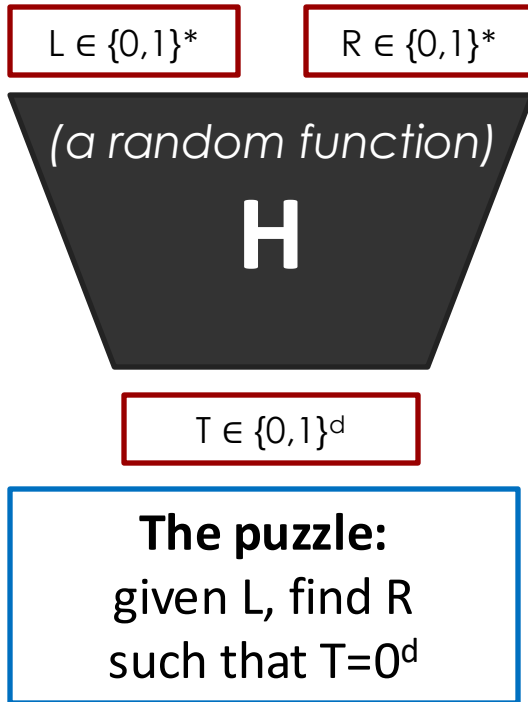
- **Part 3**: Problems and issues

TheoryCoin: How to create money

1. Everyone **tries to solve** a puzzle

2. The **first one** to solve the puzzle **gets 1 TC**

3. The solution of **puzzle _i_ defines puzzle _i+1_**

   1. Can't focus on next puzzle without solving this one

TheoryCoin: How to create money

L ∈ {0,1}*   R ∈ {0,1}*

(a random function)

H

$T \in \{0,1\}^d$

The puzzle:
given L, find R
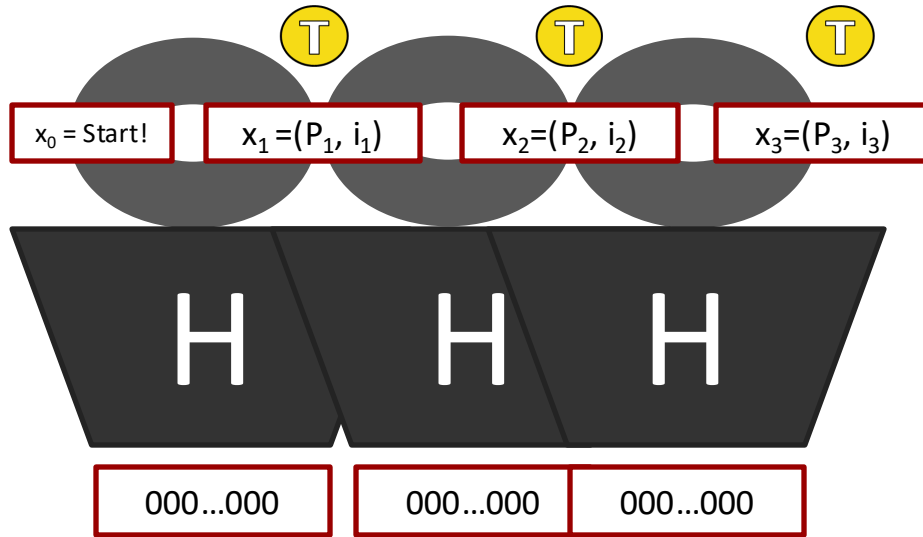such that $T=0^d$

```
SolvePuzzle(L){
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T ≠ 0^d)
  return R
}
```
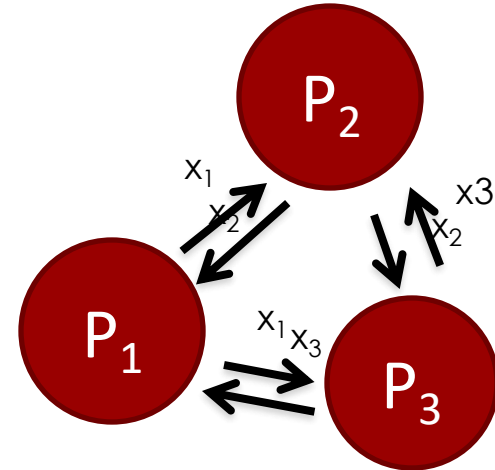
*aka **Proof-of-Work***
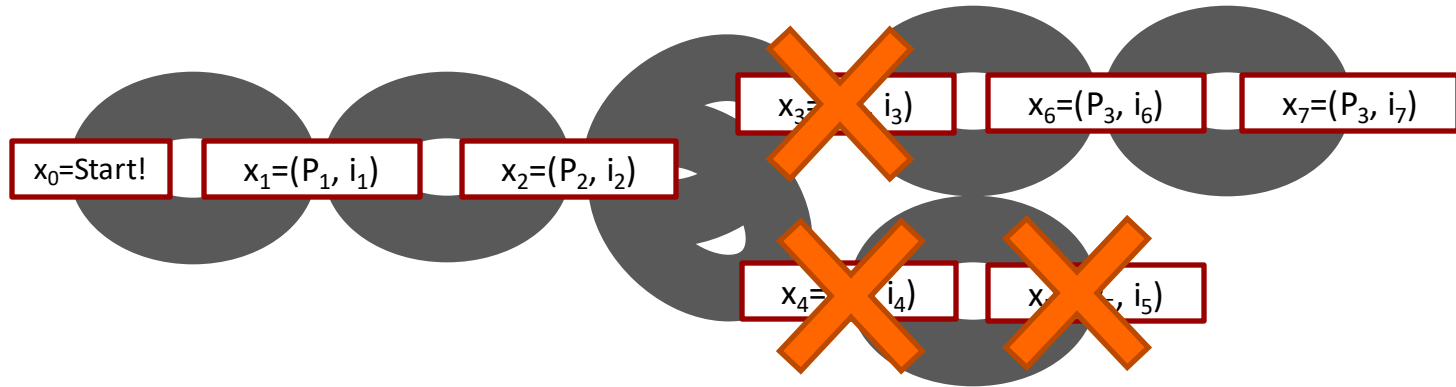
TheoryCoin: (coins to ppl)
How to create money


```
SolvePuzzle(L){
    repeat{
        R = my_name || i++
        T = H(L,R)
    }while(T ≠ 0^d)
    return R
}
```

x_0 = Start! x_1 =(P_1, i_1) x_2=(P_2, i_2) x_3=(P_3, i_3)

H H H

000...000   000...000   000...000

P_2

x_1
x_2
$x3$
x_2

P_1
x_1 x_3
P_3

*aka **the blockchain***

TheoryCoin:
How to create money

x_0=Start! x_1=(P$_1$, i$_1$) x_2=(P$_2$, i$_2$) x_3=(, i$_3$) x_6=(P$_3$, i$_6$) x_7=(P$_3$, i$_7$)

x_4=(, i$_4$) x_5=(, i$_5$)

*aka **the 51% attack***

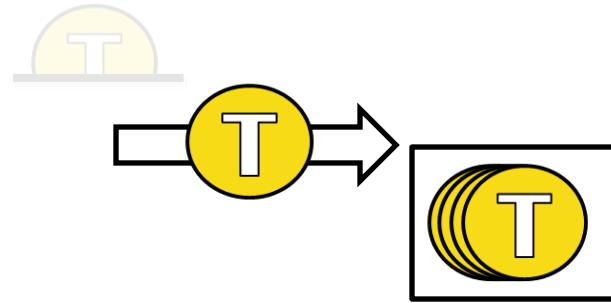# TheoryCoin:
How to create money

Recap:

Solve the next puzzle → get a coin

- To "**solve**" puzzle i find x_i s.t $H(x_{i-1},x_i)=0^d$

- The longest chain defines "**next puzzle**"

- The name in block x_i "**gets**" coin i.

Outline

- **Part 0**: a little history

- **Part 1**: TheoryCoin
  - How to **create** coins
  - How to **transfer** coins
  - How to **store** coins

- **Part 2**: diff(

- **Part 3**: Problems and issues

TheoryCoin:
How to transfer money

(Digital) Signatures

- Only you can sign
- Everyone can verify
- You cannot deny

TheoryCoin:
How to transfer money

"Your pin code"

Gen

"Your username"

secret key

public key

message

Sign

message, signature

Verify

accept/reject

TheoryCoin: How to transfer money
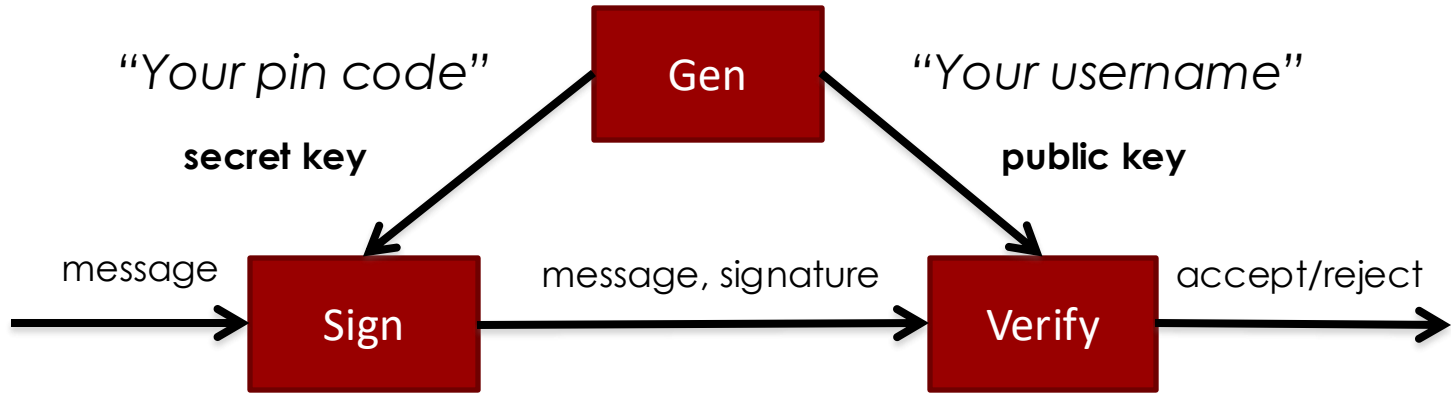
TheoryCoin:
How to transfer money

m1="P3 gives coin 3 to P1"
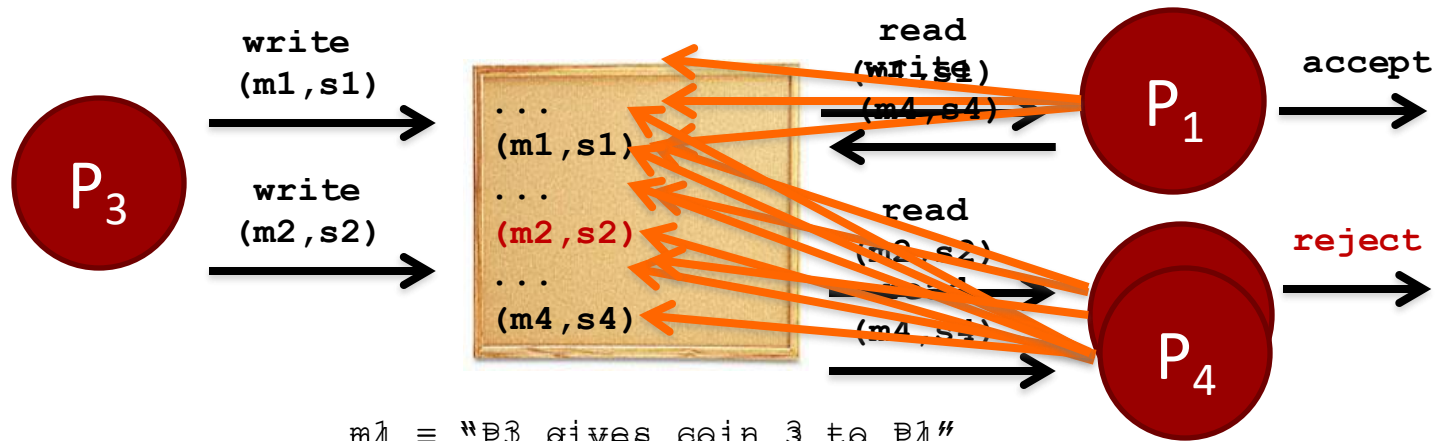s1=Sig(sk3,m1)

accept

P_1

P_3

accept

P_2
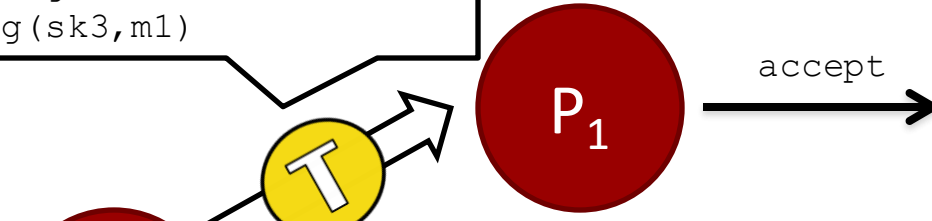
m2="P3 gives coin 3 to P2"
s2=Sig(sk3,m2)
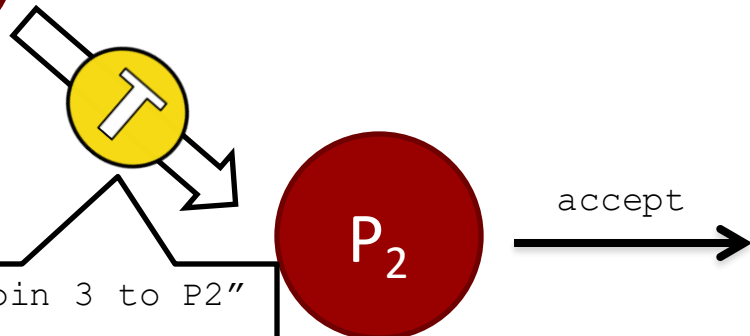
*aka **double spending***

TheoryCoin:
How to transfer money

write (m1,s1)

write (m2,s2)

P_3

```
...
(m1,s1)
...
(m2,s2)
...
(m4,s4)
```

read (write) (m4,s4)

read (m2,s2) (m4,s4)

P_1

P_4

accept

reject

```
m4 = "P3 gives coin 3 to P4"
s4 = Sig(sk3,m4)

m2 = "P3 gives coin 3 to P2"
s2 = Sig(sk3,m2)
```

Outline

- **Part 0**: a little history

- **Part 1**: TheoryCoin
  - How to **create** coins
  - How to **transfer** coins
  - How to **store** coins

- **Part 2**: diff(

- **Part 3**: Problems and issues
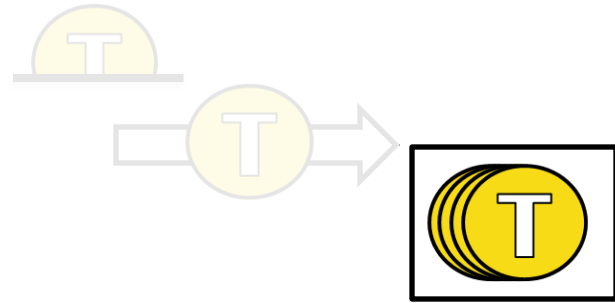
TheoryCoin:
How to store money

Main Idea:

Record **transfers** in the **blockchain**

$x_0 = \text{Start!}$ $x_1 = (P_1, i_1)$ $x_2 = (P_2, i_1)$ $x_3 = (P_3, i_3)$ ....

TheoryCoin:
How to store money


```
SolvePuzzle(L,...){
    repeat{
        R = my_name||(m,s)|| i++
        T = H(L,R)
    }while(T ≠ 0^d)
    return R
}
```

P1

P3

P2

P4

(m,s)

(m,s)

```
SolvePuzzle(L){
    repeat{
        R = my_name || i++
        T = H(L,R)
    }while(T ≠ 0^d)
    return R
}
```

x_0 = Start! $x_1=(P_1, i_1)$ $x_2=(P_2, i_1)$ $x_3=(P_3, i_3)$ $x_4=(P4, (m,s), i_4)$

Outline

- **Part 0**: a little history

- **Part 1**: TheoryCoin
  - How to **create** coins
  - How to **transfer** coins
  - How to **store** coins

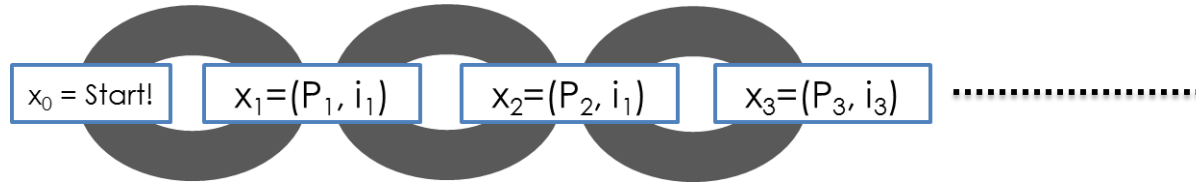- **Part 2**: diff( )

- **Part 3**: Problems and issues

diff(T ₿)
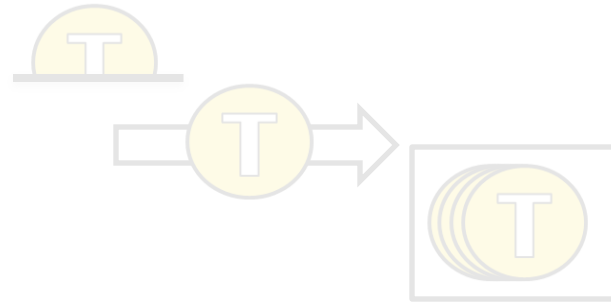
How is money created in Bitcoin?

- New block **every ~10 mins**

  - **d** adjusted every ~2000 blocks

- H = **2-SHA2**

- Initial reward: **50 BTC**

  - Halved every ~4 years (decreased from 12.5 to 6.25 BTC on May 11, 2020)

  - Getting harder to mine bitcoins

$L \in \{0,1\}^*$ $R \in \{0,1\}^*$

H

$T \in \{0,1\}^d$

diff(🪙 ₿)

How is money transferred in Bitcoin?

Example: P1 wants to give 60 to P2

... gives 50 to P1

... gives 25 to P1

P1 gives 60 to P2

P1 gives 14 to P1

Transaction fee 1

diff(T ₿)
How is money stored in Bitcoin?

- Transaction in **orphaned blocks** are invalid
  - **Wait 6 blocks** (~1 hour) before accepting transaction.
  - **Checkpoints** to prevent complete history rollback.
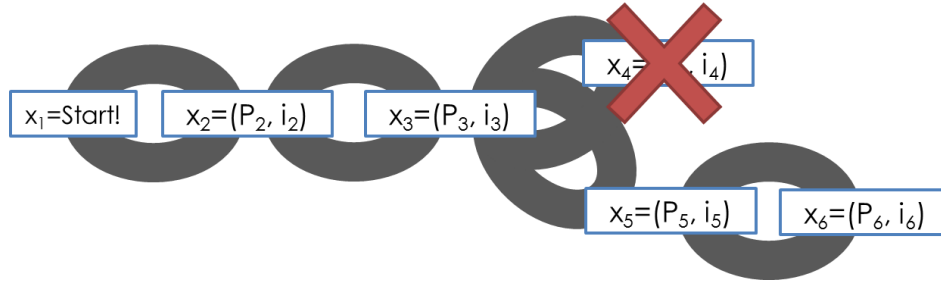
- **All transactions** are stored in the blockchain
  - (Currently hundreds of GB)

Outline

- **Part 0**: a little history

- **Part 1**: TheoryCoin
  - How to **create** coins
  - How to **transfer** coins
  - How to **store** coins

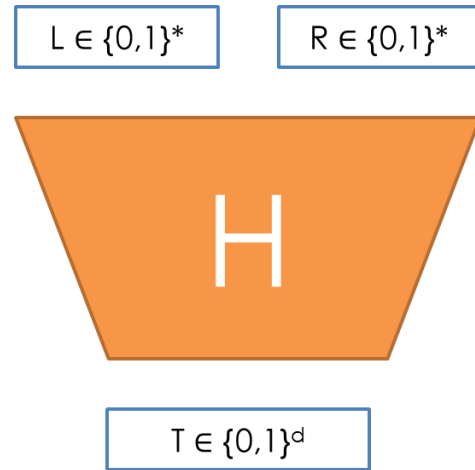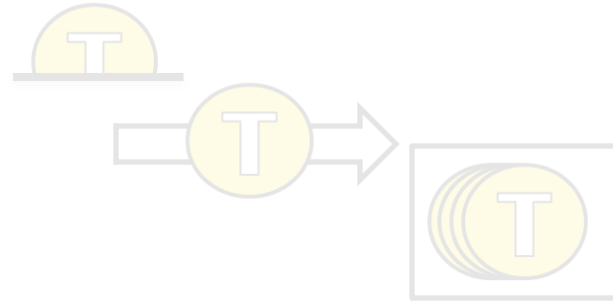- **Part 2**: diff(T B)

- **Part 3**: Problems and issues

Anonymity?

- **Problem**:
  – Every transaction ever made is **recorded forever**
  – Infer user identity based on behavior

- **Solution**?
  – Use **new identity** for each transaction
- **But**:
  – Heuristics allow to **cluster** identities
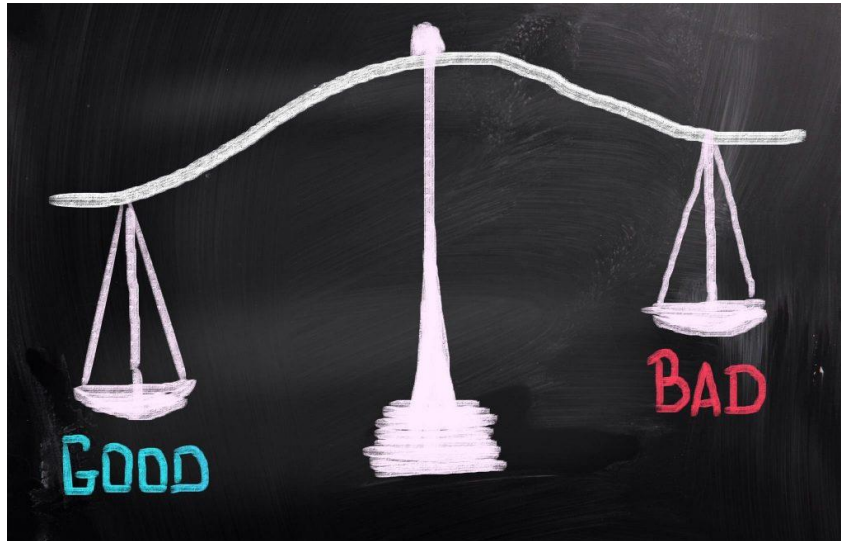- **Anonymous alternatives:**
  – Zerocoin, Zerocash…

A Final Word…

Distributed currencies: for the **good guys** or the **bad guys**?

- Crime is bad! Tax evasion is bad!
- But sometimes governments are bad too!

Discussion

- Is Bitcoin a waste of electricity?

- Will Bitcoin enable criminal activity? Will it support democracy?

- What new capabilities might be enabled by Bitcoin?

- What are the prospects for alternative forms of crypto-currency ("altcoins")?