463.8 Bitcoin

CS463/ECE424

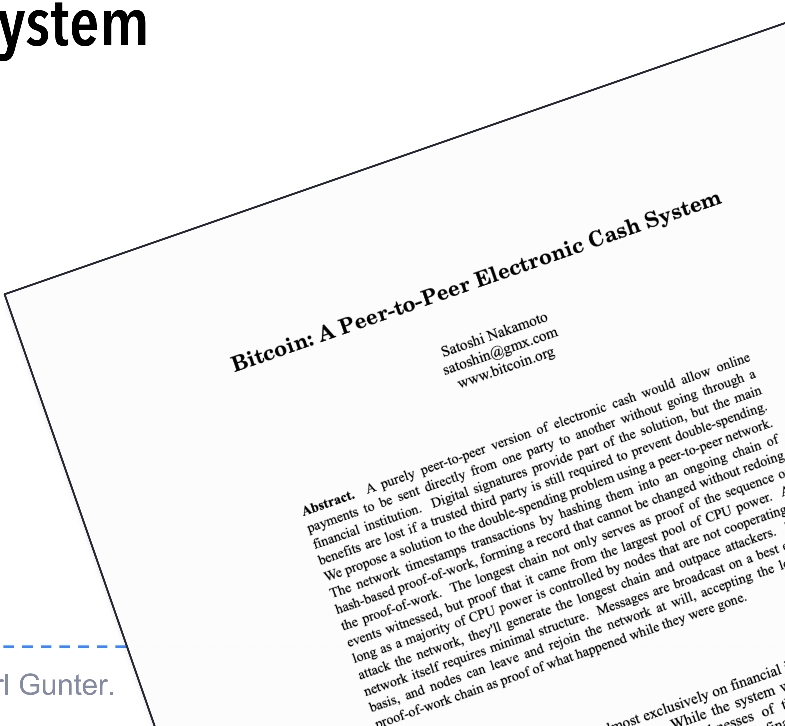
University of Illinois

Reference:

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

https://bitcoin.org/bitcoin.pdf



Bitcoin: A Peer-to-Peer Electronic Cash System

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

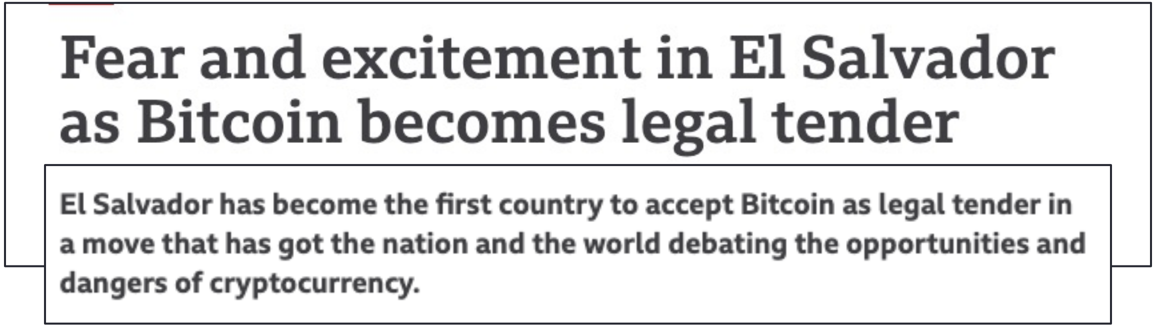
Abstract. A purely peer-to-peer version of electronic cash would allow online
payments to be sent directly from one party to another without going through a
financial institution. Digital signatures provide part of the solution, but the main
benefits are lost if a trusted third party is still required 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 o
events witnessed, but proof that it came from the largest pool of CPU power. A
long as a majority of CPU power is controlled by nodes that are not cooperating
attack the network, they'll generate the longest chain and outpace attackers.
network itself requires minimal structure. Messages are broadcast on a best
basis, and nodes can leave and rejoin the network at will, accepting the l
proof-of-work chain as proof of what happened while they were gone.

lmost exclusively on financial
While the system w

Slides Credits: Claudio Orlandi, Jon K. Sørensen, Peter S. Nordholt, Carl Gunter.

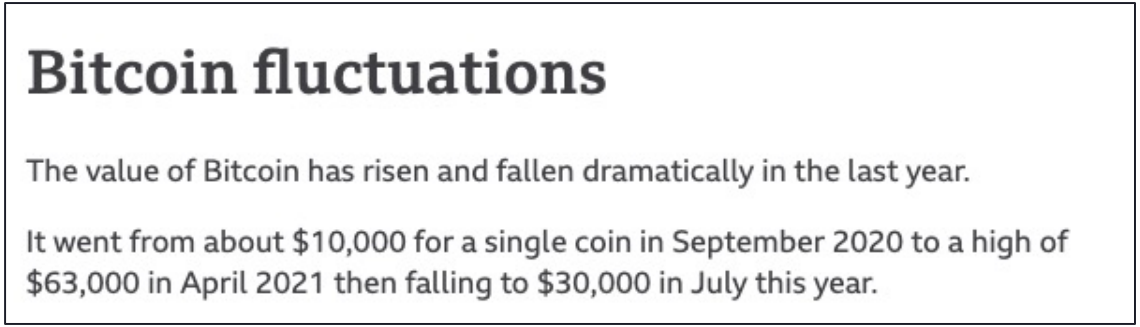
Bitcoin and Cryptocurrency

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?

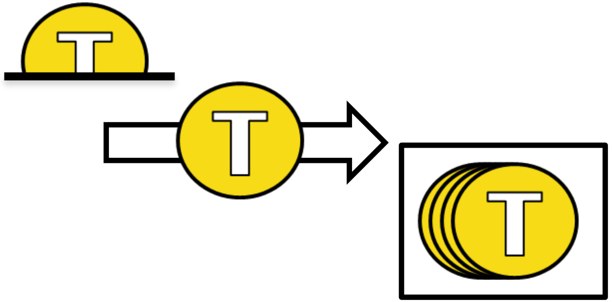
Outline

- **Part 0**: a little history

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

- **Part 2**: diff(T, ₿)

- **Part 3**: Problems and issues



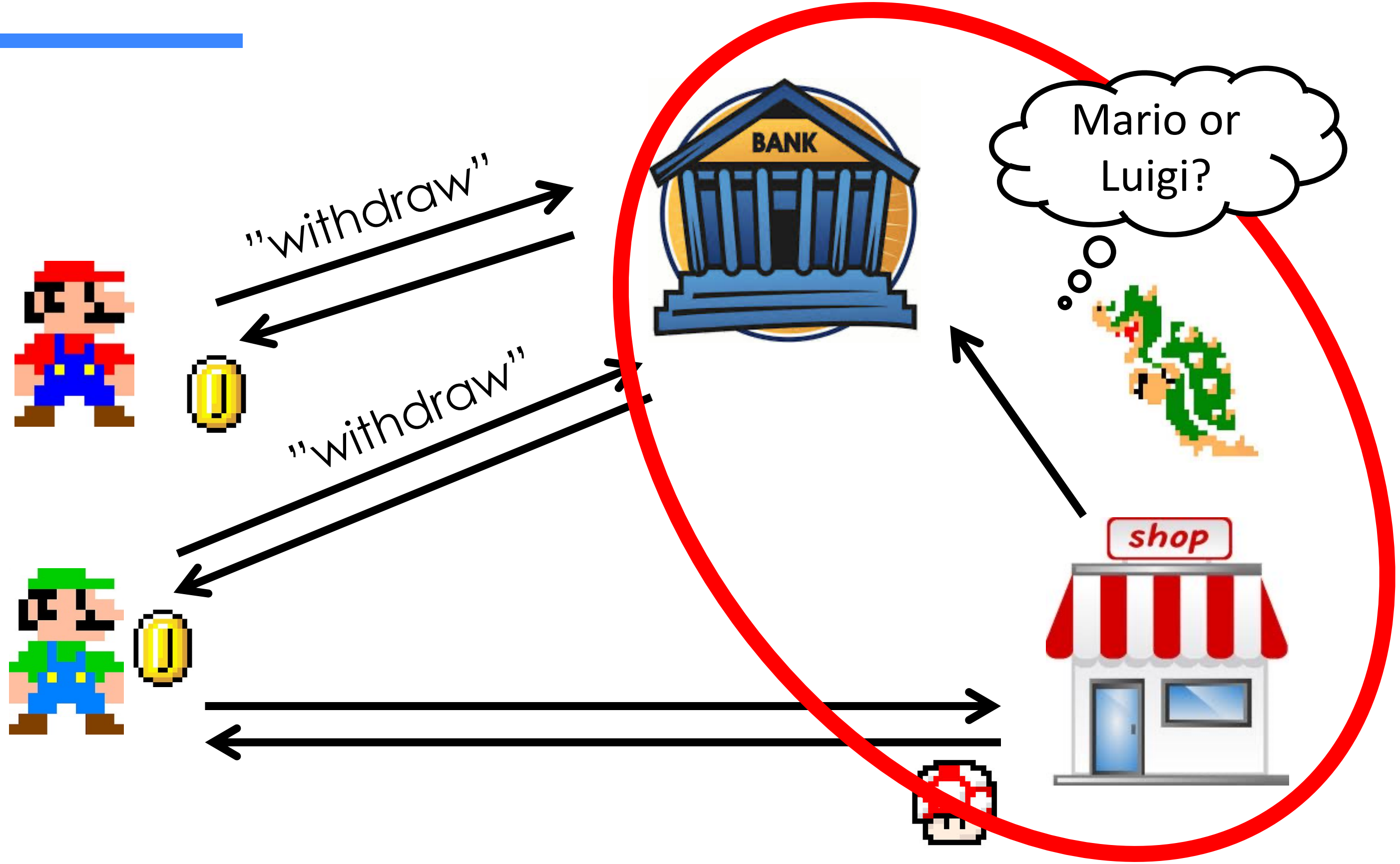
The 1990s
David Chaum and Anonymous ECash

"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

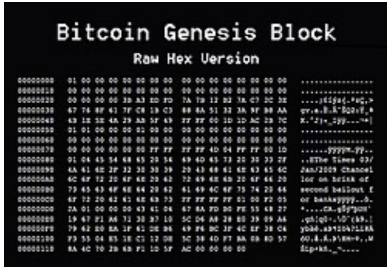
- **Anonymous**
- **Secure** (no double-spending)
- Only **transfer** (no creation/storage)

Still have to work with real banks

...and **bankrupted** in 1999

The Advent of Bitcoin

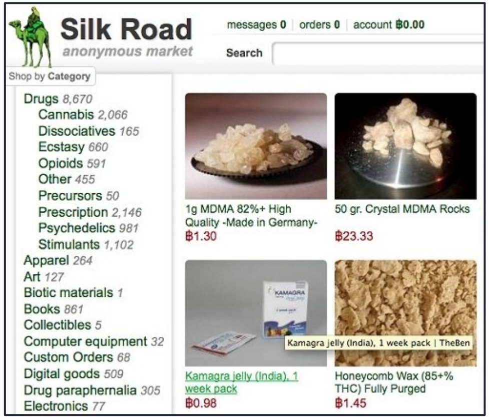
- 2009: **Bitcoin announced** by Satoshi Nakamoto
  - Pseudonym for person or group of people
- 2009-2011: slow start…
- 2011-2013: Silk Road, Dread Pirate Roberts
- End of 2013: **Bitcoin price skyrockets**
  - and the world notices!



Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã.ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.00

Search

Shop by Category

- Drugs 8,670
  - Cannabis 2,066
  - Dissociatives 165
  - Ecstasy 660
  - Opioids 591
  - Other 455
  - Precursors 50
  - Prescription 2,146
  - Psychedelics 981
  - Stimulants 1,102
- Apparel 264
- Art 127
- Biotic materials 1
- Books 861
- Collectibles 5
- Computer equipment 32
- Custom Orders 68
- Digital goods 509
- Drug paraphernalia 305
- Electronics 77

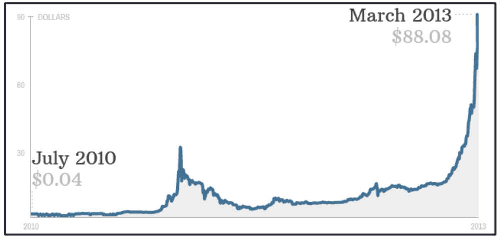
1g MDMA 82%+ High Quality -Made in Germany-
฿1.30

50 gr. Crystal MDMA Rocks
฿23.33

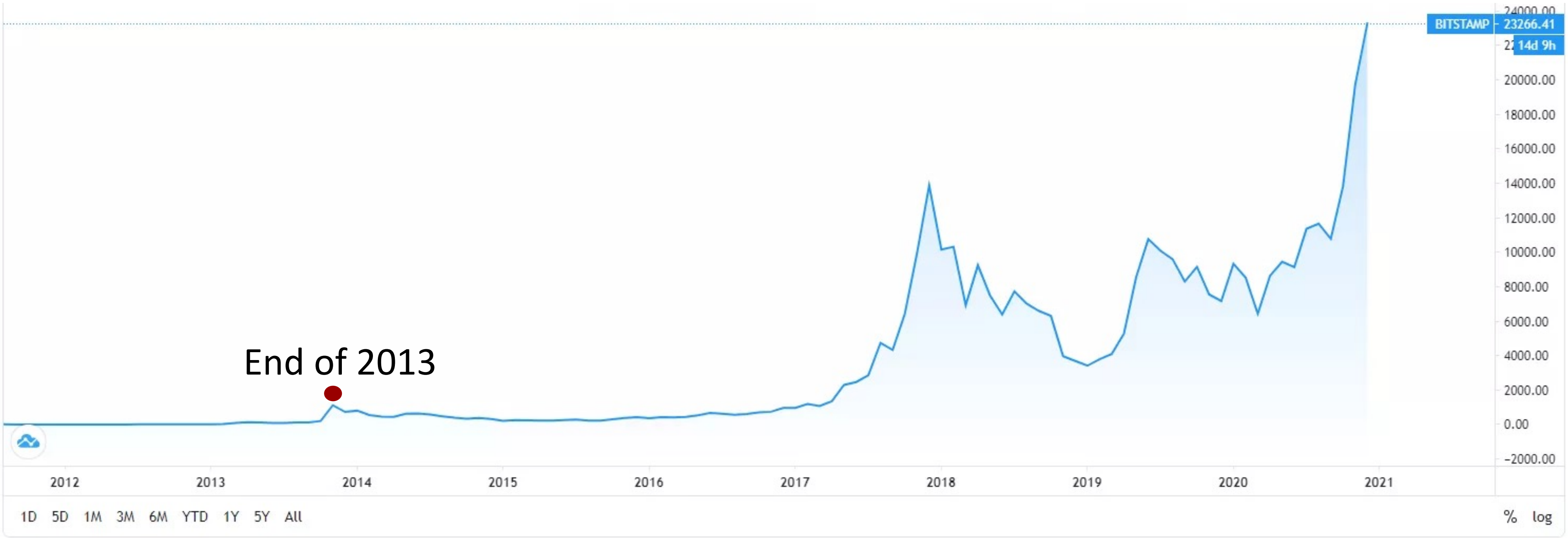
Kamagra jelly (India), 1 week pack
฿0.98

Kamagra jelly (India), 1 week pack | TheBen

Honeycomb Wax (85+% THC) Fully Purged
฿1.45



Price is Even Higher Now

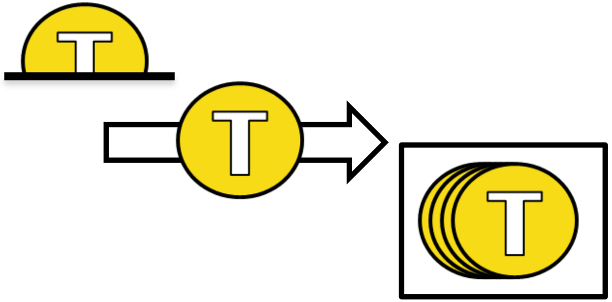


End of 2013

Outline

- **Part 0**: a little history

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

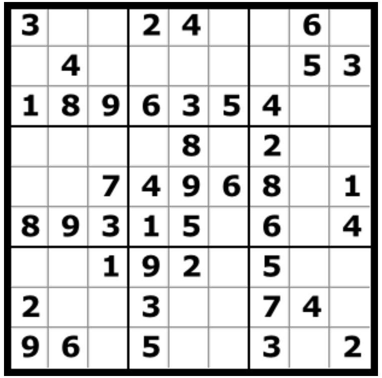


- **Part 2**: diff(T ₿

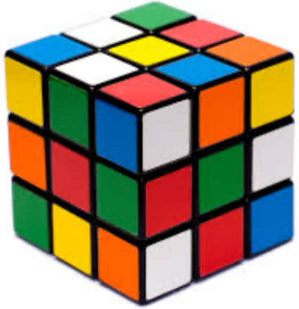
- **Part 3**: Problems and issues

TheoryCoin: How to create money

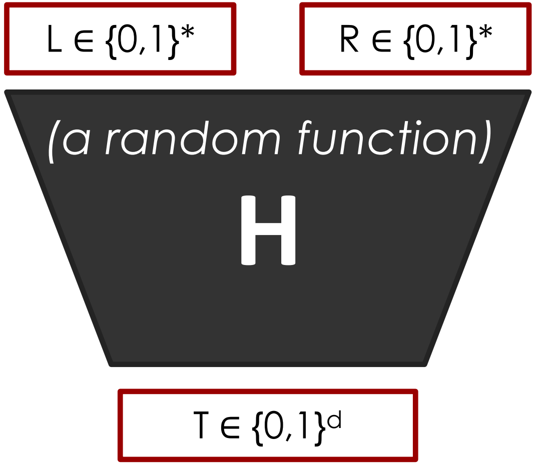
1. Everyone **tries to solve** a puzzle
2. The **first one** to solve the puzzle **gets 1 TC**
3. The solution of **puzzle *i* defines puzzle *i+1***



3			2	4			6	
	4						5	3
1	8	9	6	3	5	4		
				8		2		
		7	4	9	6	8		1
8	9	3	1	5		6		4
		1	9	2		5		
2			3			7	4	
9	6		5			3		2



TheoryCoin: How to create money



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

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

(a random function)

H

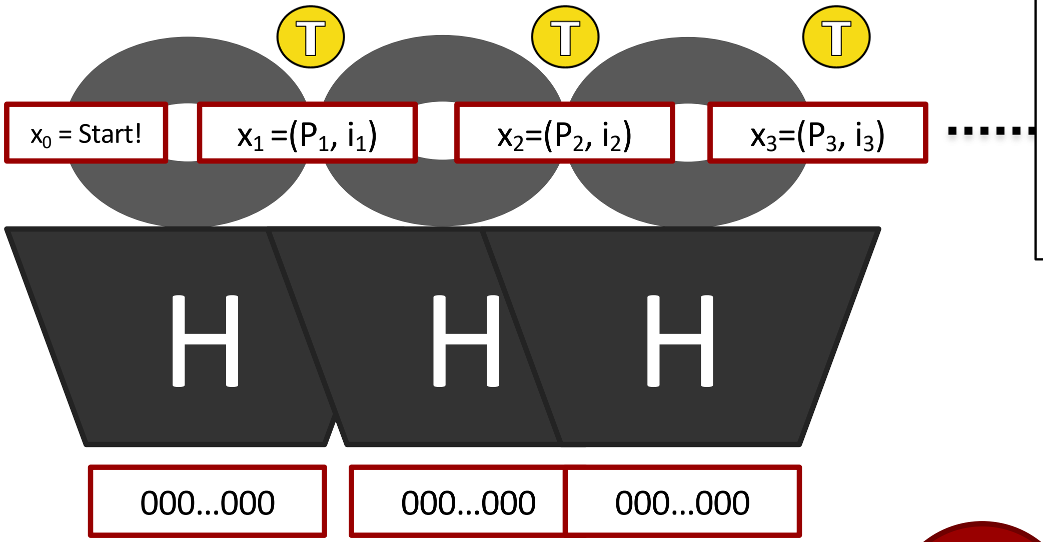
$T \in \{0,1\}^d$

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

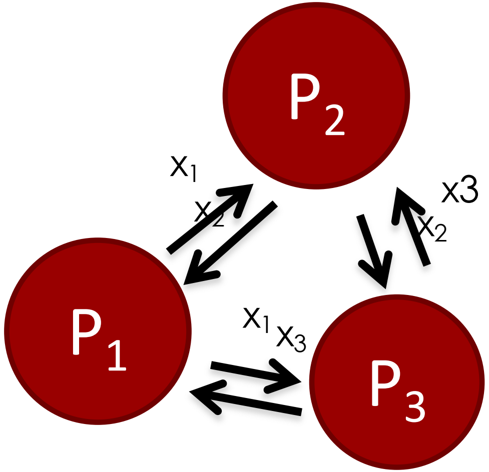
```
SolvePuzzle(L){
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T ≠ $0^d$)
  return R
}
```

* *aka* ***Proof-of-Work***

TheoryCoin: (coins to ppl)
How to create money

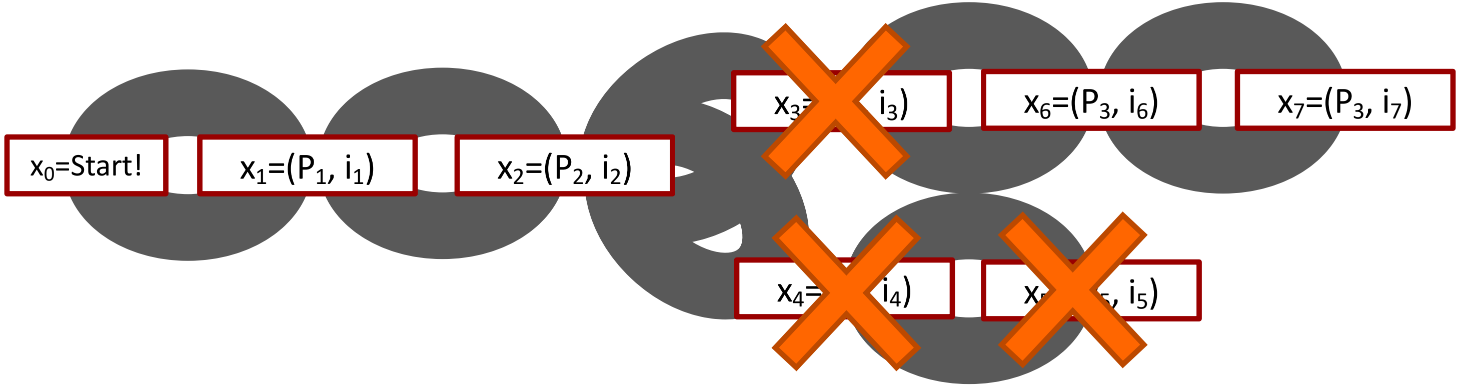


```
SolvePuzzle(L){
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T ≠ $0^d$)
  return R
}
```



* *aka* ***the blockchain***

TheoryCoin:
How to create money



* *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.

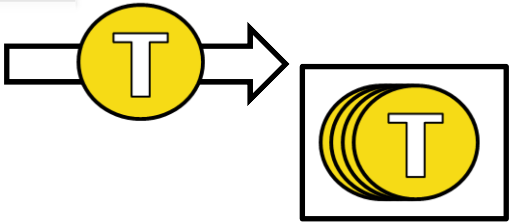
Outline

- Part 0: a little history

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

- **Part 2**: diff(T ₿

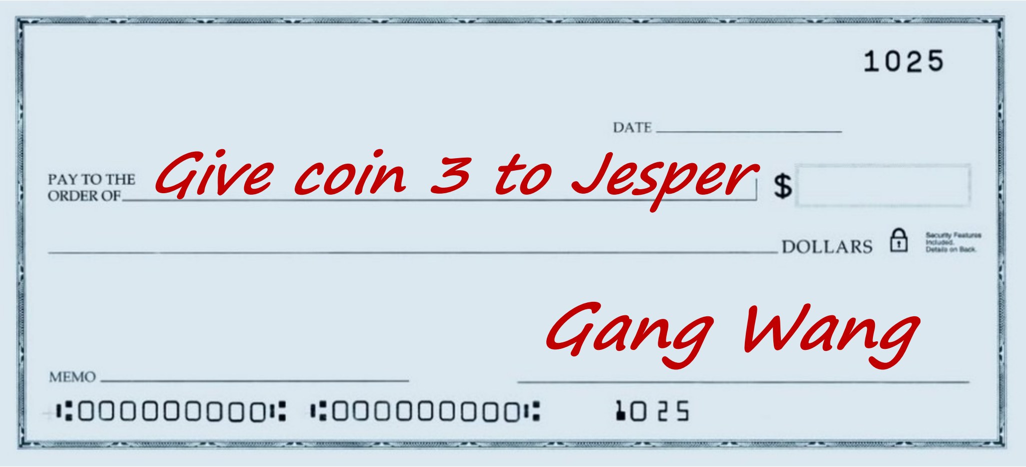
- **Part 3**: Problems and issues



TheoryCoin:
How to transfer money

(Digital) Signatures

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



1025

DATE

PAY TO THE ORDER OF Give coin 3 to Jesper $

DOLLARS

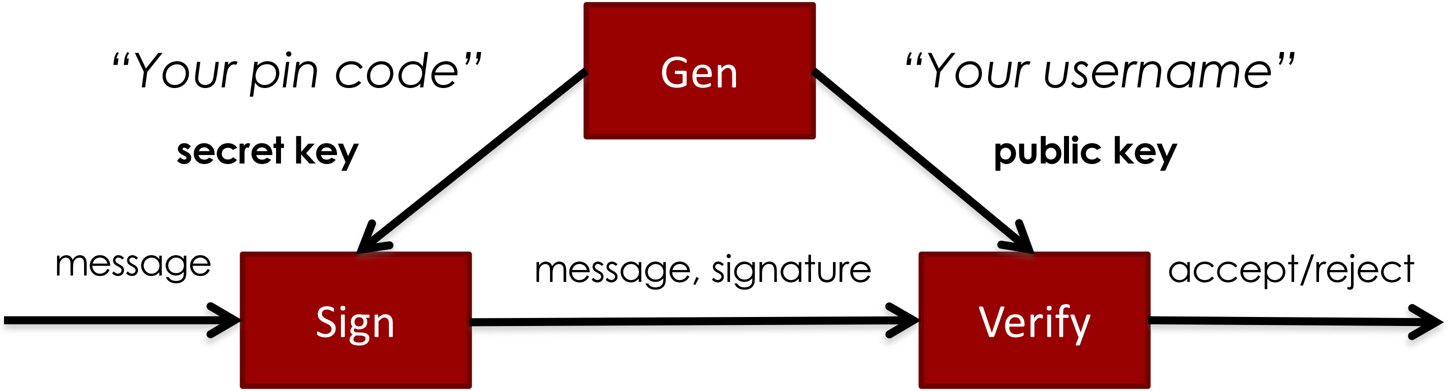
Security Features Included. Details on Back.

Gang Wang

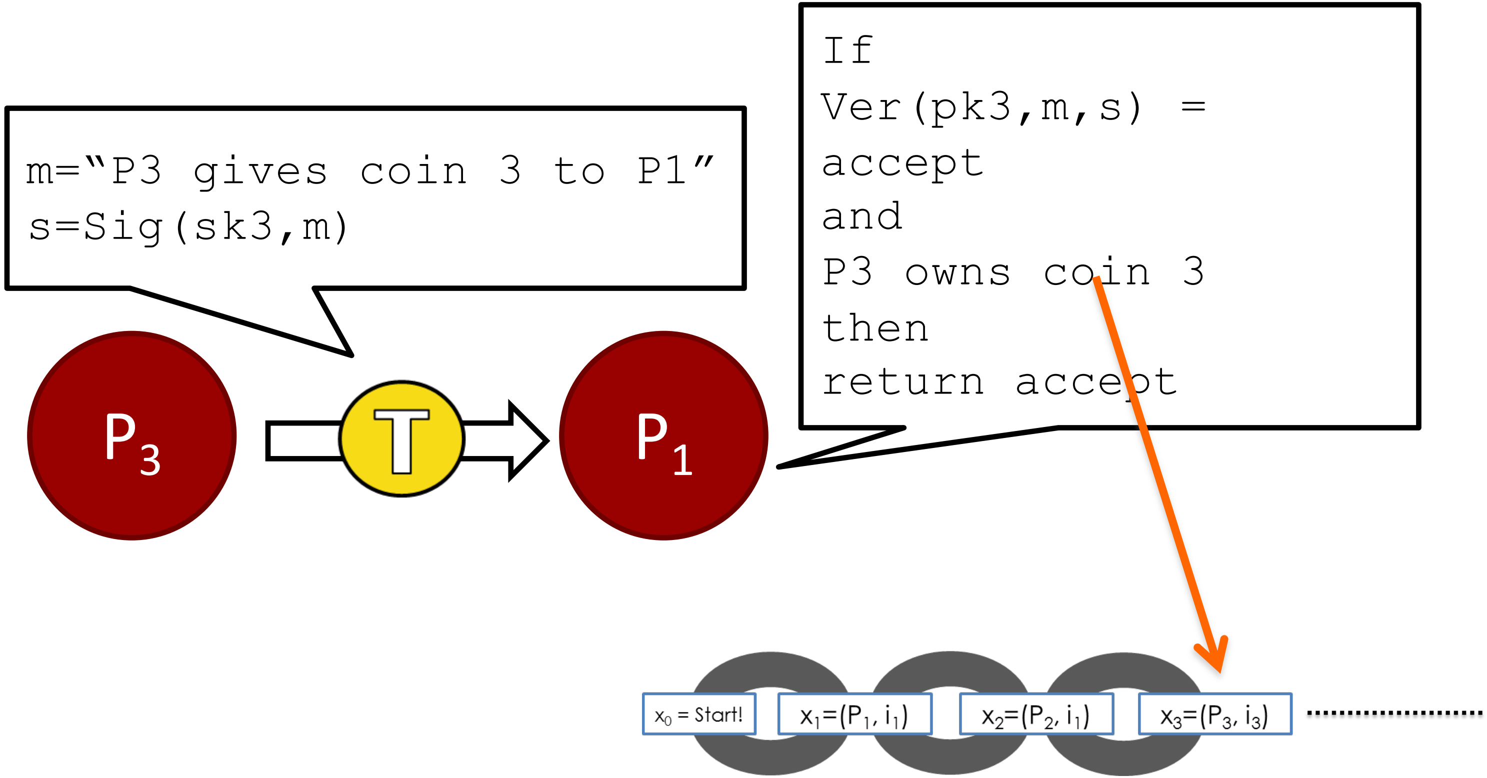
MEMO

⑆000000000⑆ ⑆000000000⑆ 1025

TheoryCoin:
How to transfer money



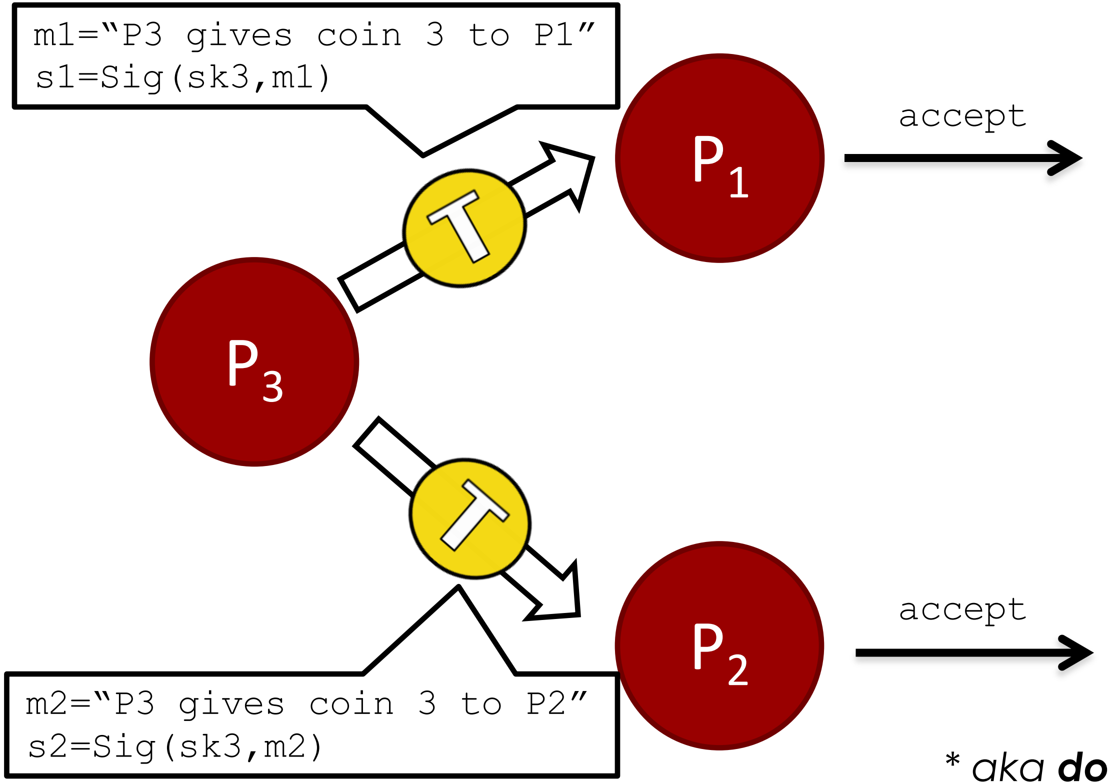
TheoryCoin:
How to transfer money



```
m="P3 gives coin 3 to P1"
s=Sig(sk3,m)
```

```
If
Ver(pk3,m,s) =
accept
and
P3 owns coin 3
then
return accept
```

TheoryCoin: How to transfer money

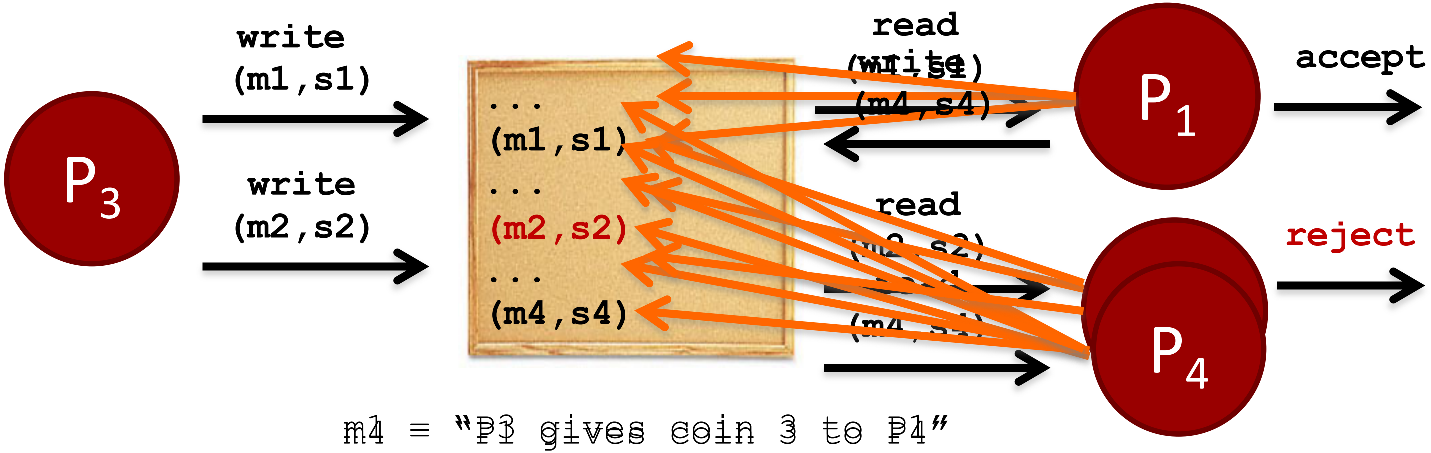


```
m1="P3 gives coin 3 to P1"
s1=Sig(sk3,m1)
```

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

* *aka* ***double spending***

TheoryCoin:
How to transfer money

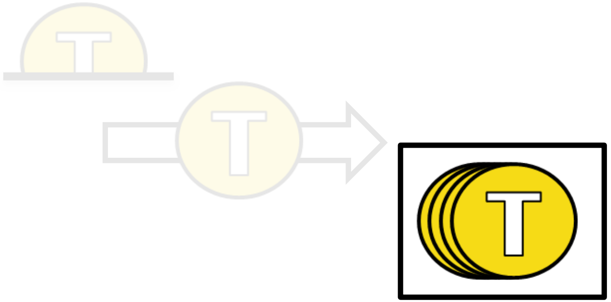


```
m1 = "P3 gives coin 3 to P1"
s1 = Sig(sk3,m1)

m4 = "P1 gives coin 3 to P4"
s4 = Sig(sk1,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



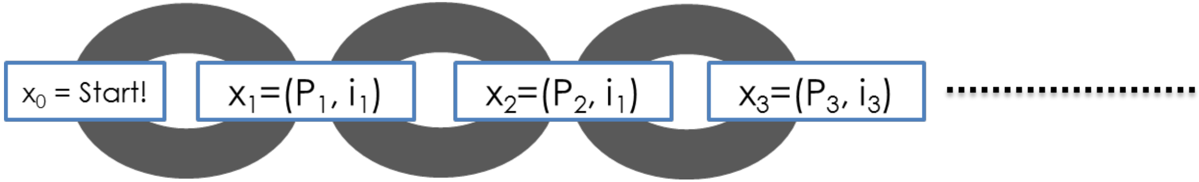
- **Part 2**: diff(T ₿

- **Part 3**: Problems and issues

TheoryCoin:
How to store money

Main Idea:

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



x_0 = Start!

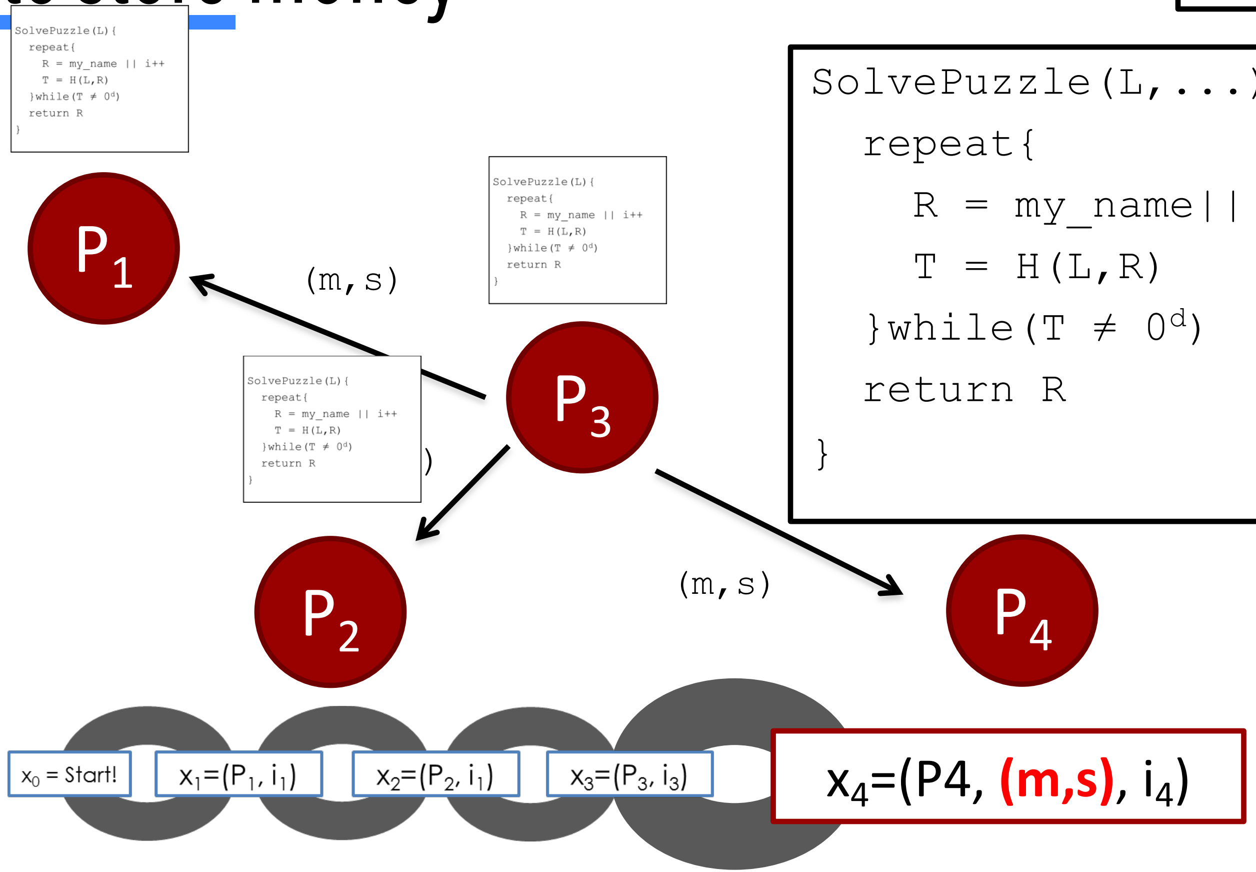
$x_1=(P_1, i_1)$

$x_2=(P_2, i_1)$

$x_3=(P_3, i_3)$

TheoryCoin:
How to store money

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



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

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

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

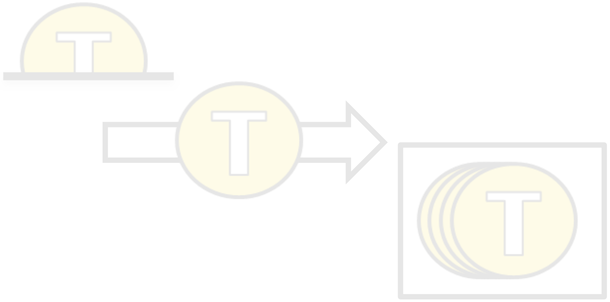
Outline

- **Part 0**: a little history

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

- **Part 2**: diff(T, ₿

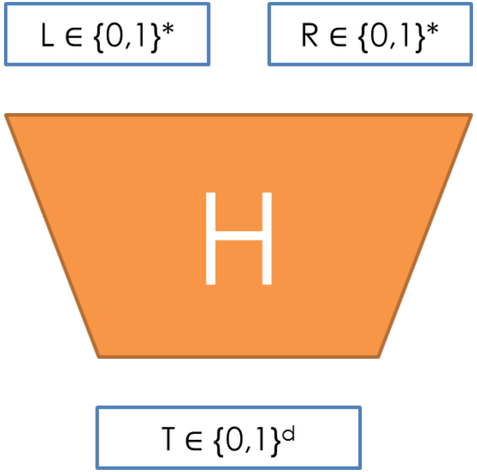
- **Part 3**: Problems and issues



diff(Ⓣ , ₿)

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



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

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

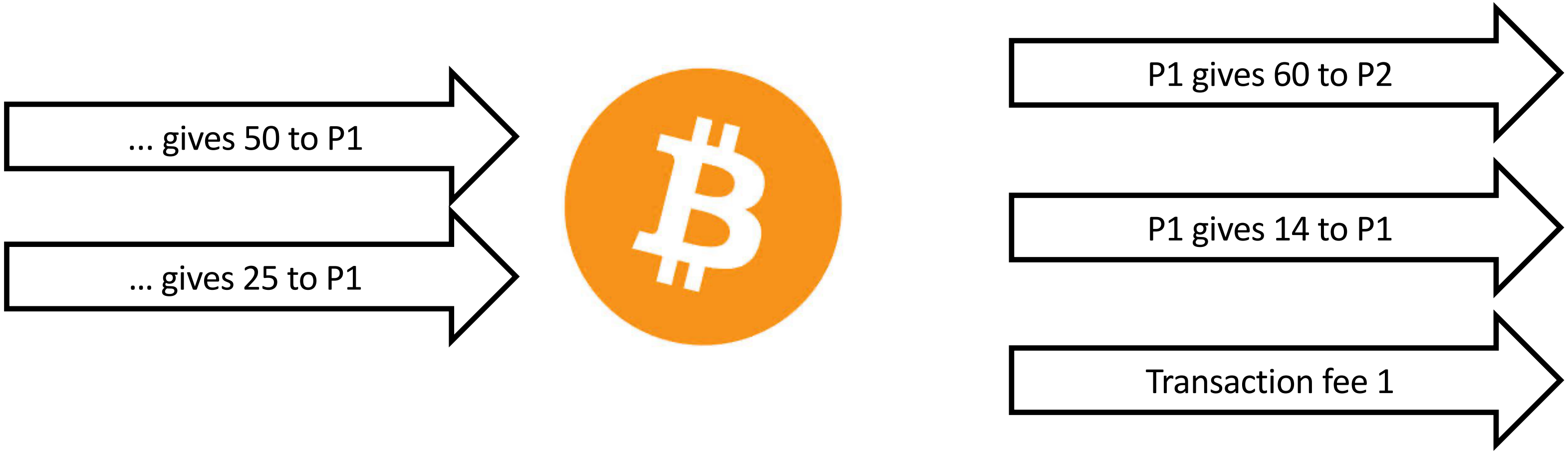
H

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

diff(Ⓣ, ₿)

How is money transferred in Bitcoin?

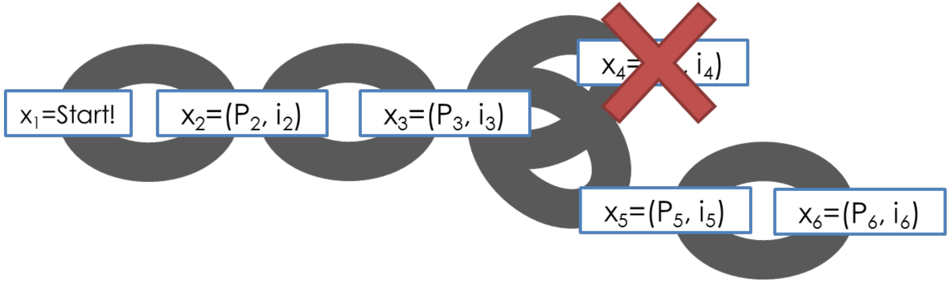
Example: P1 wants to give 60 to P2



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.

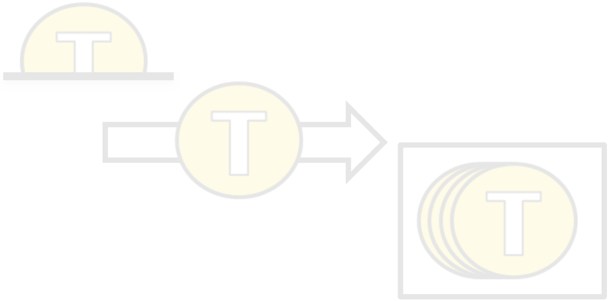


- **All transactions** are stored in the blockchain
  - (Currently hundreds of GB)

Outline

- **Part 0**: a little history

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

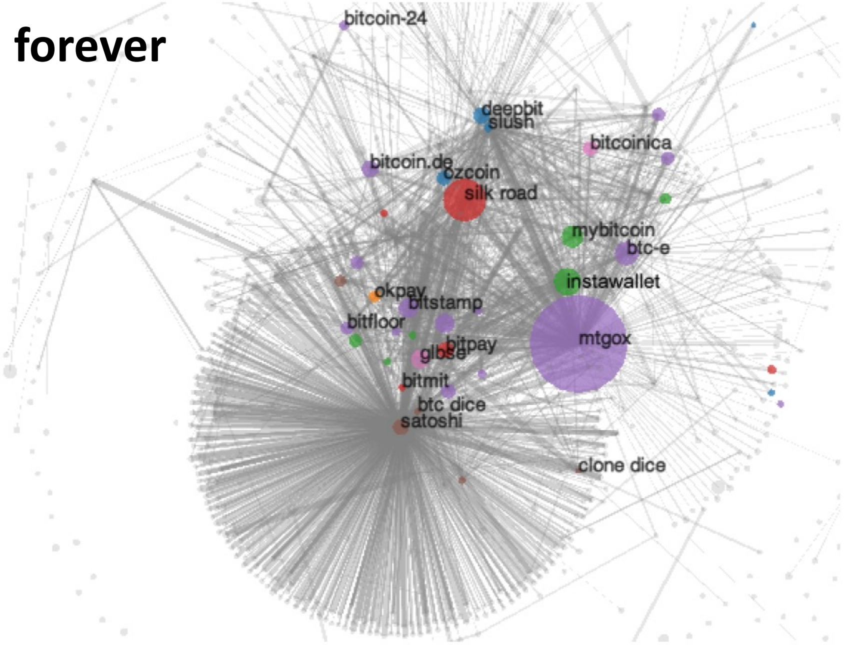


- **Part 2**: diff(T ₿

- **Part 3**: Problems and issues

Anonymity?

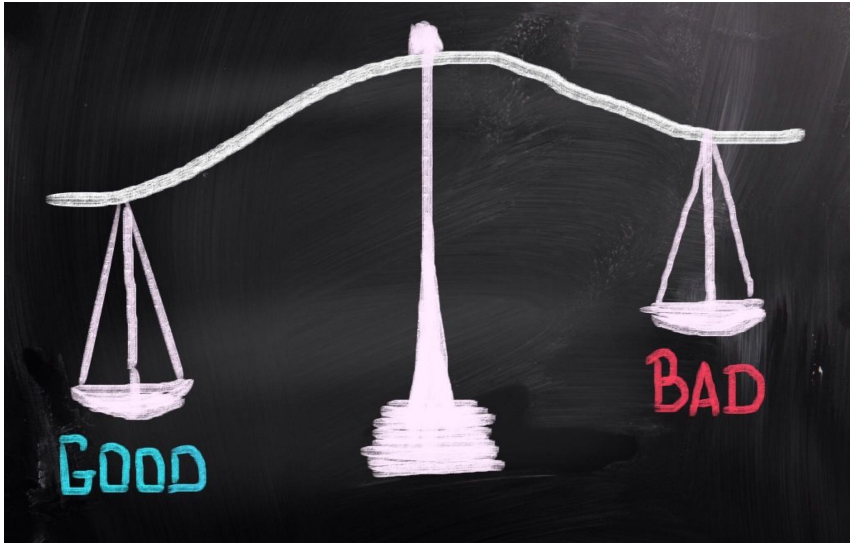
- **Problem**:
  - Every transaction ever made is **recorded forever**
  - Infer user identity based on behavior
- **Solution**?
  - Use **new identity** for each transaction
- **But**:
  - Heuristics allow to **cluster** identities
- **Anonymous alternatives:**
  - Zerocoin, Zerocash…



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”)?