

INF3510 Information Security

Lecture 13: Security Applications



Audun Jøsang

University of Oslo
Spring 2014

Outline

- Digital Payments
 - DigiCash
 - BitCoin
 - 3D Secure

- Information Warfare

What is a currency ?






- Requirements to qualify as currency
 1. Must be a store of value,
 - Practical to keep savings with the currency
 2. Must be a medium of exchange
 - Practical to compose & split value, and to trade with the currency
 3. Must be a unit of account
 - Practical to fix prices and do book-keeping with currency
- Most government-issued currencies satisfy requirements
 - But high inflation can threaten requirements
- Commodities generally do not satisfy requirements
 - Barter economy impractical
 - Commodities can be difficult to split
 - Commodities can be difficult to store




Properties of currencies




- Depends on trust in central issuing authority
 - Originally based on inherent value as commodity 
 - Gold-standard from around 1700, abandoned during 1900s 
 - Modern currencies based on government monetary policy
 - Adjust interest rates and amounts of money in the market 
 - Keep large quantities of gold to back up value of currency

• Physical currency

- Anonymous 
- Leaves no trace of payer's identity
 - Good for privacy, bad for law enforcement

• Electronic currency

- Payer and payee are identified 
- Can be traced
 - Bad for privacy, good for law enforcement

The 1990s

David Chaum and anonymous e-cash

*“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)

Chaum's **anonymous e-cash**

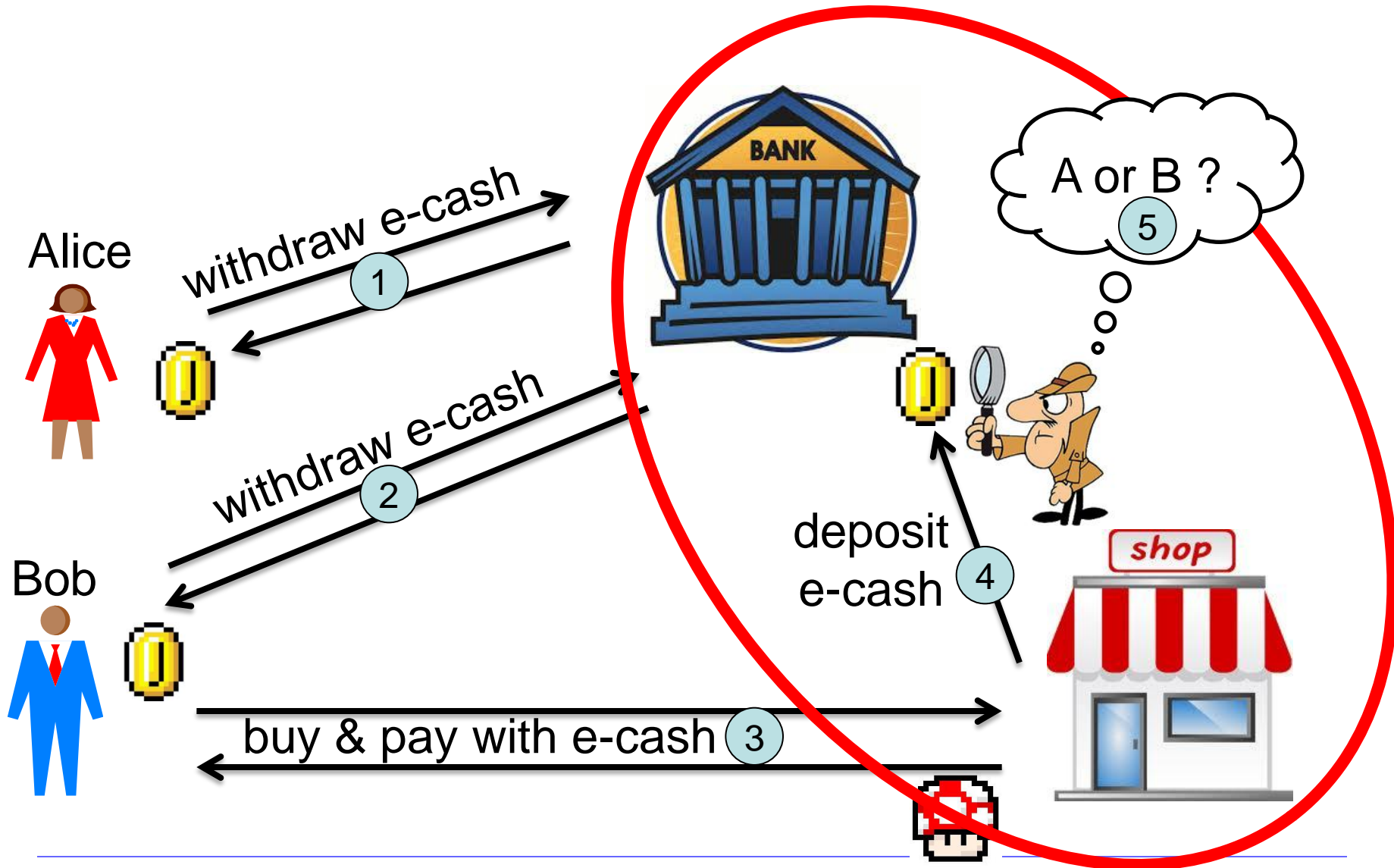
- **Digital representation** of existing currencies
 - each DigiCash coin was a string of bits
- **Anonymous coins**, based on blind digital signatures
- **Transfer** requires bank to clear and deposit value of coin
- **Secure** (guarantee against double-spending)
- **Storage of coins**, as physical cash, i.e. no interest gain

- **Company started** in 1990



...and **bankrupted** in 1999

Anonymous e-cash payments



From DigiCash to Bitcoin

- The vision of DigiCash 1990
 - Anonymous
- Assumed problem with DigiCash
 - Dependent on traditional currencies
 - Cooperation from banks required
- The vision of Bitcoin 2008
 - Anonymous
 - Independent from government currencies
 - Independent from banks
- The problem of Bitcoin
 - Extreme volatility due to independence from currencies
 - Technical complexity
 - Security vulnerabilities



The history of Bitcoin

- 2008: Theory paper describing Bitcoin published
 - Title: *Bitcoin: A Peer-to-Peer Electronic Cash System*
 - Pseudonym author: *Satoshi Nakamoto*
 - Unclear who is behind pseudonym, possibly single person or group
- 2009: Bitcoin open source software available
 - First Bitcoins created and first transactions executed
- 2010: Gavin Andresen takes control of Bitcoin software
 - Currently leads the Bitcoin Foundation software development
- 2010-2013: Slow increase in usage
- End 2013: Bitcoin price skyrockets
 - and the world notices!
- 2014 problems
 - Chinese authorities crack down on Bitcoin
 - Some Bitcoin exchanges go bankrupt

BITCOIN PRICE VERSUS USD



- The Bitcoin price skyrocketed during 2013
- Falling sharply in 2014

Bitcoin fundamentals

- Two types of participants

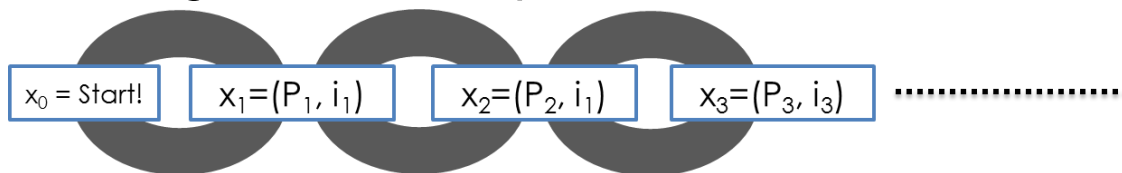
1) Miners:



2) Shoppers and shops

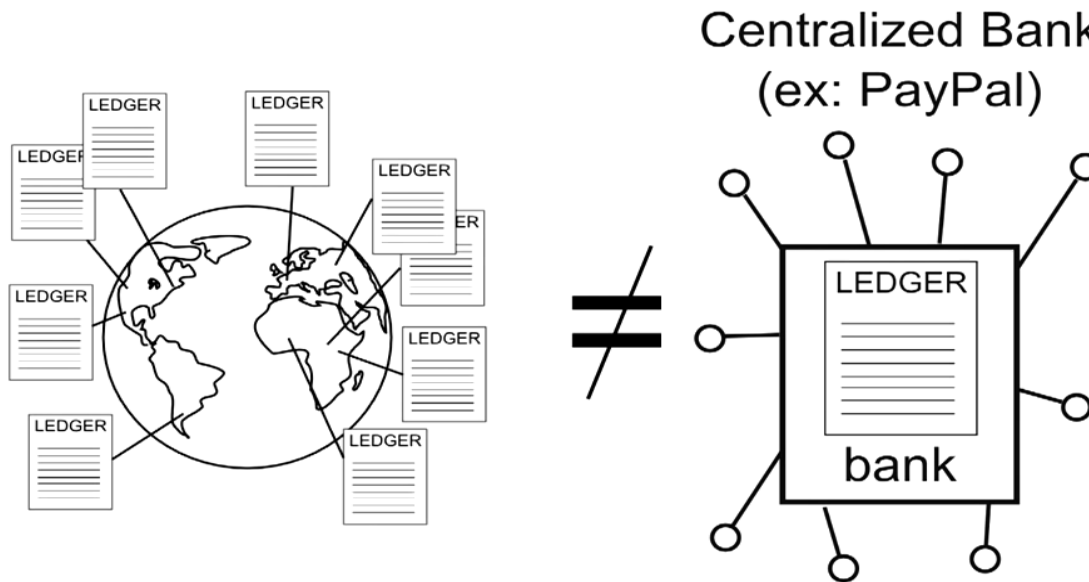


- All participants must run Bitcoin software
- Peer-to-Peer network
- Each participant has public/private key pair
- Transactions are hashed and signed by payer
- Every transaction is chained cryptographically
 - The ledger is the complete list of all transactions

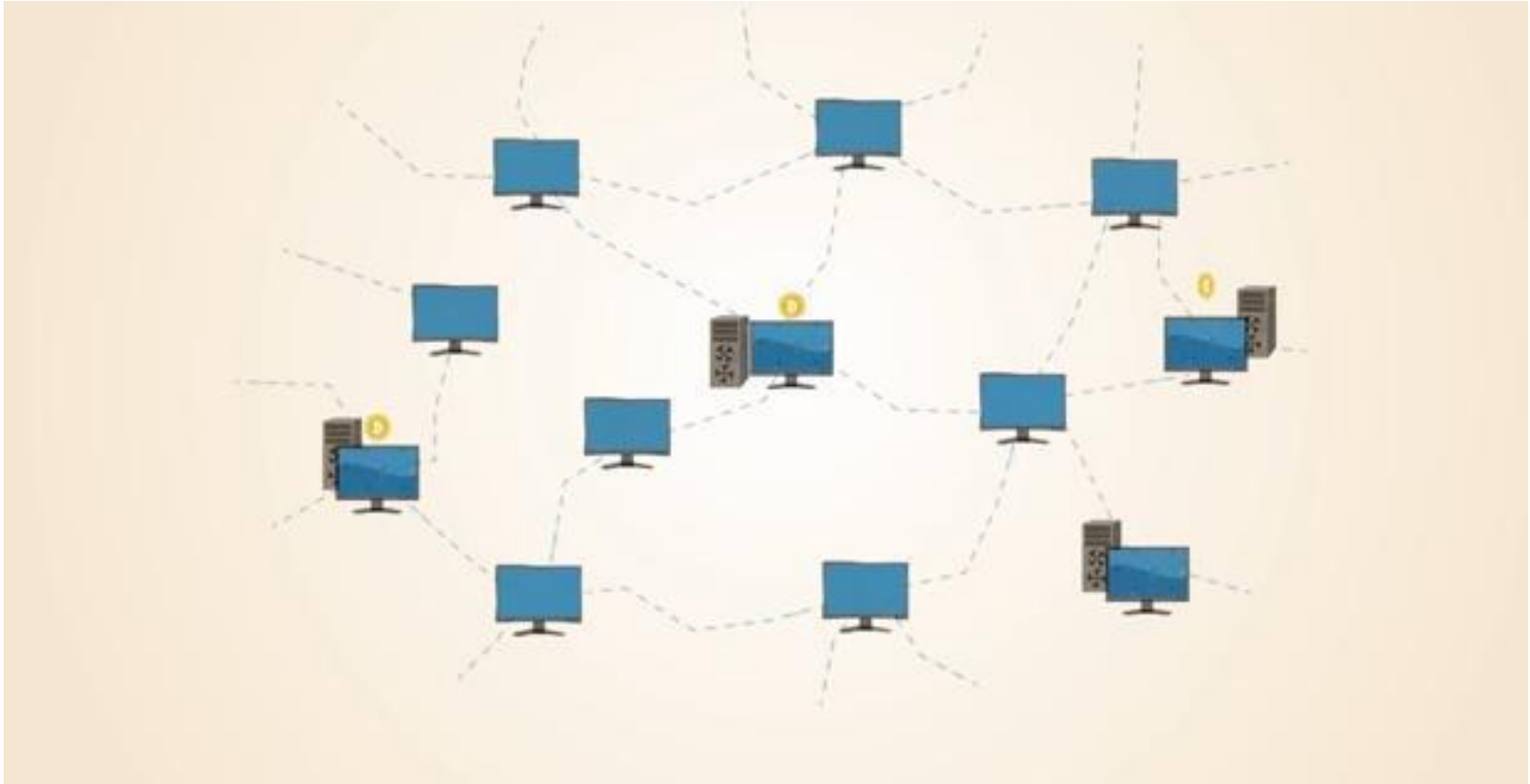


The Bitcoin ledger

- In a bank, the ledger is the list of all transactions
 - Centrally managed by the bank
- The Bitcoin ledger is decentralized
 - Each node has it's own copy of the ledger
 - Synchronization of ledger copies through P2P network



Peer to Peer



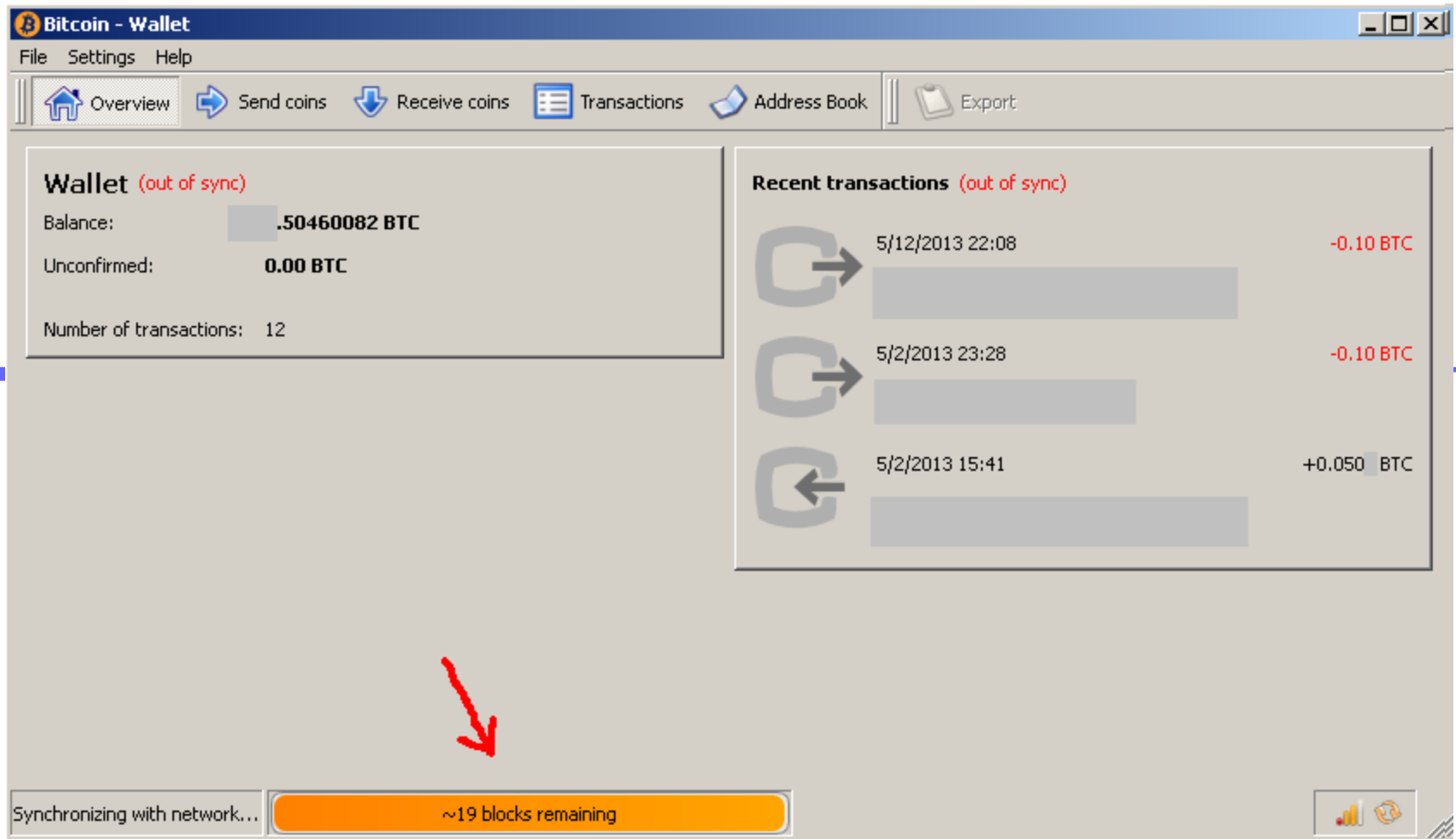
Bitcoin wallet balances

- Transactions and balances are public available for all
- Computed as a function of the ledger from start to end
- As the ledger keeps growing, the balances change ...

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

...

Bitcoin Wallet



Each wallet keeps a record of ALL Bitcoin transactions.
Yes, all of them.

How to create Bitcoins



- Find hash value with a number of zeros
 - First n bits must be 0, e.g, for $n = 8$ find hash value 00000000.....
 - Likelihood of finding correct hash value is: $(\frac{1}{2})^n$
 - Finding hash value is **proof of work**
 - The higher n , the more difficult it is to find correct hash values
 - Value of n is adjusted to make difficulty appropriate
- Input to hash function H:
 - Fixed part L consists of previous transaction
 - Dynamic part R consists of my Id (public key) + incremental value
- Many parties try to find correct hash values
 - First party to find the correct hash for given L gets 25 Bitcoins
 - Correct hash value defines new block on ledger and new L value
 - L value depends on previous block, so blocks are chained

How to create Bitcoins



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

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

(a random function)

H

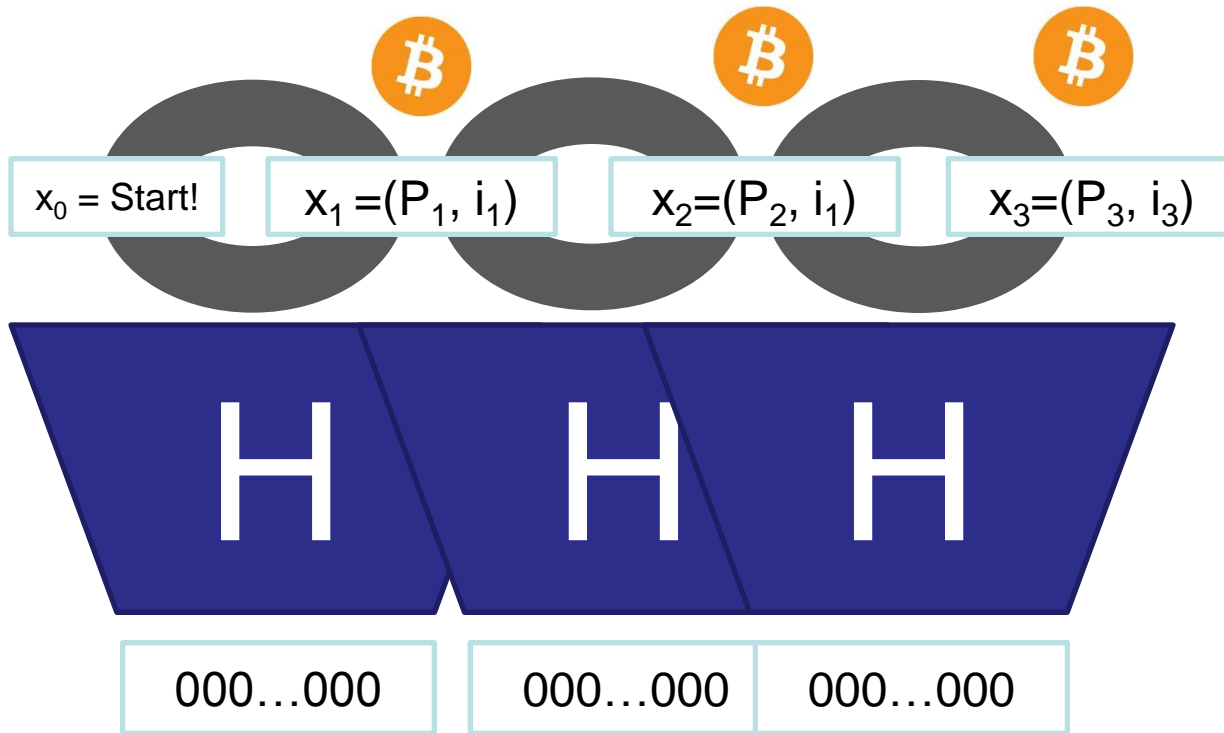
$T \in \{0,1\}^d$

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

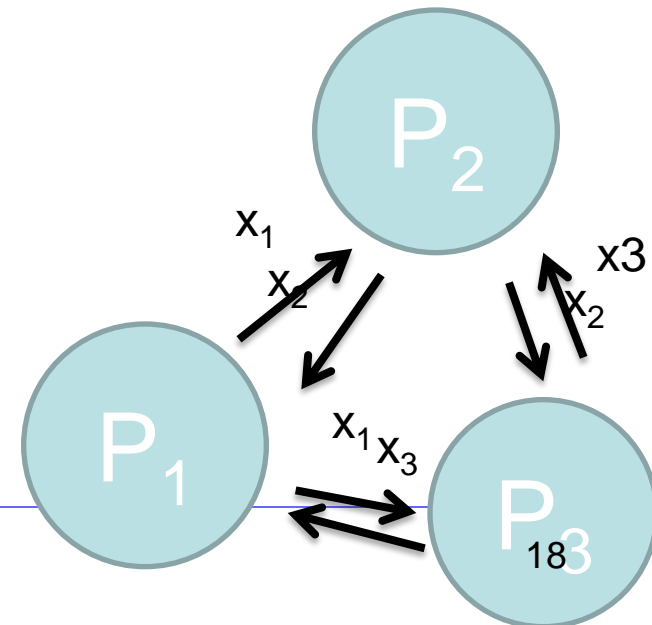
```
SolvePuzzle(L) {  
  repeat {  
    R = my_name || i++  
    T = H(L,R)  
  }while(T ≠ 0d)  
  return R  
}
```

** aka Proof-of-Work*

How to create Bitcoins



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



How to create Bitcoins

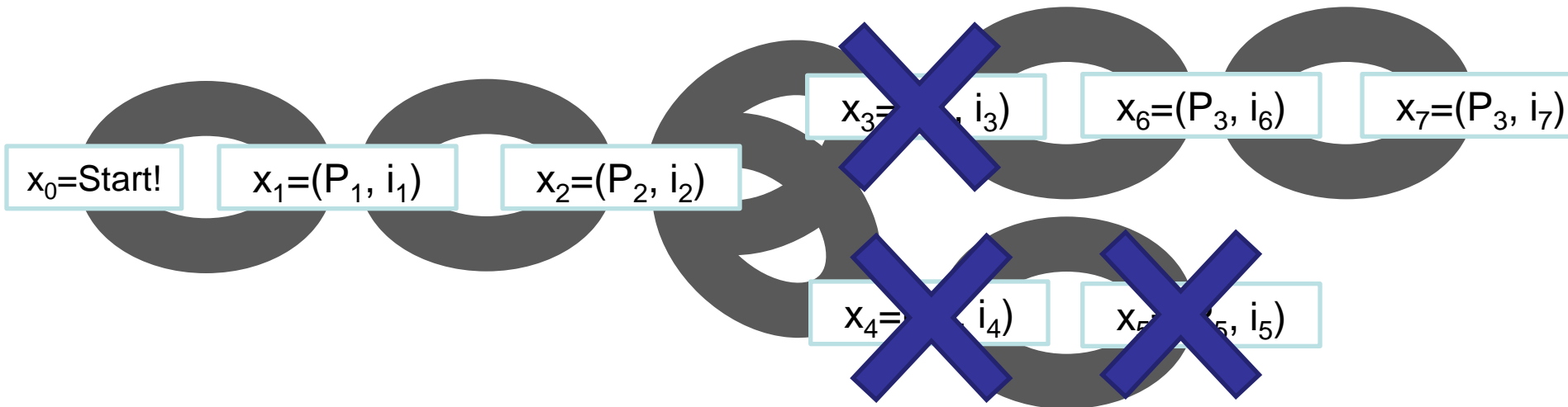
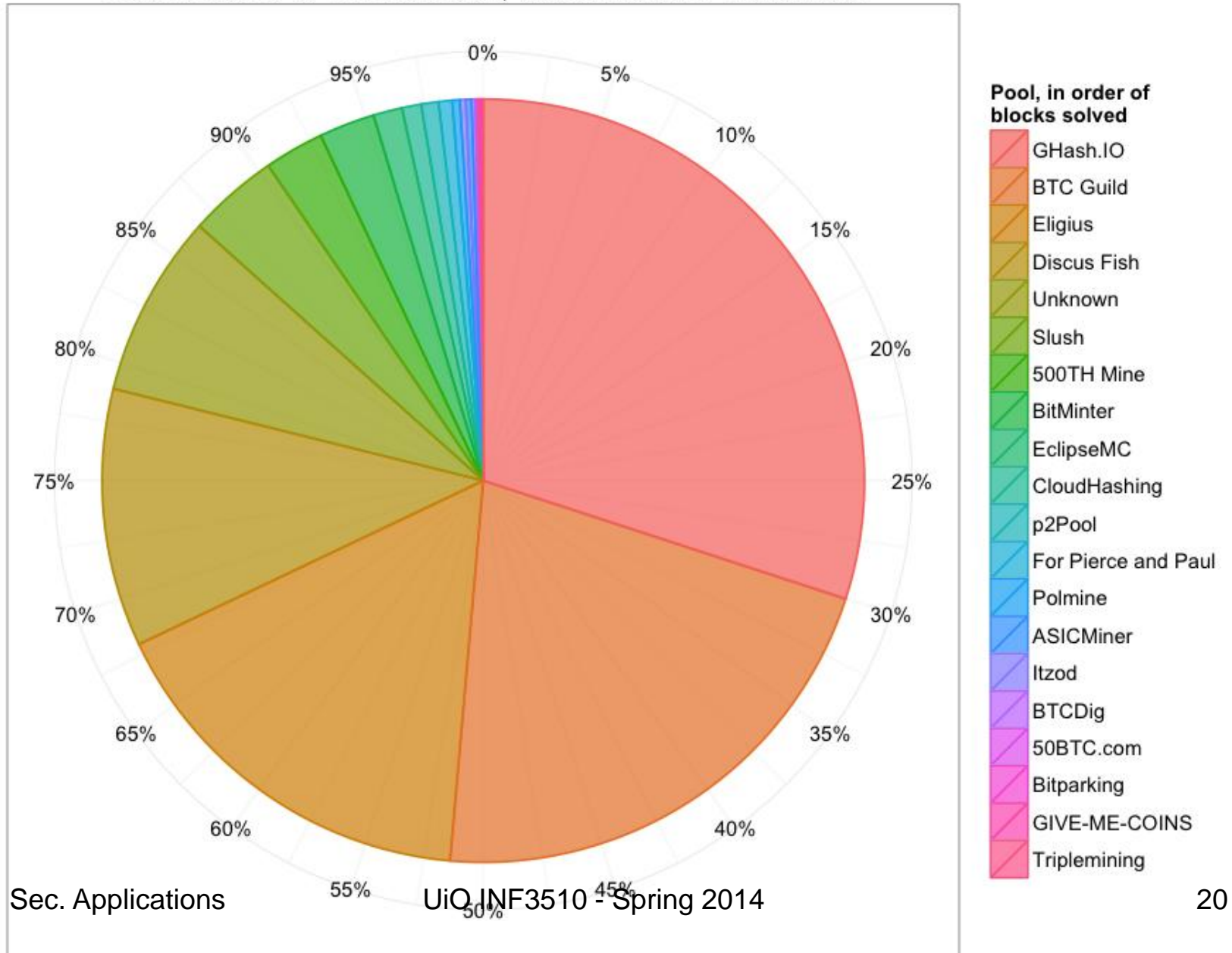


Figure 1:
 Percentage of valid network blocks
 Feb 02 2014 to Feb 08 2014, blocks 283657 to 284882



Bitcoin Mining



Specialized hardware for Bitcoin Mining



Home

Products

Drivers

Consulting

FAQ

Support Forums

RELATED PRODUCTS

Check items to add to the cart
or [select all](#)



25 GH/s Bitcoin
Miner



\$1,249.00

[Add to Wishlist](#)



50 GH/s Bitcoin
Miner



\$2,499.00

[Add to Wishlist](#)



1,500 GH/s Bitcoin Miner
BitForce Mini Rig SC

51% Attack?

EXTREMETECH

Top Searches: Windows 8 • Autos • Quantum • Intel Trending: Linux • Windows 8 • NASA • Batteries

↑ **Computing** / Mobile / Internet / Gaming / Electronics / Extreme

↑ > COMPUTING > **THE BITCOIN NETWORK OUTPERFORMS THE TOP 500 SUPERCOMPUTERS COMBINED**

The Bitcoin network outperforms the top 500 supercomputers combined

By Grant Brunner on May 13, 2013 at 3:15 pm | [Comment](#)



For some, Bitcoin conjures ideas of a utopian decentralized currency, but many others these days think of it as a quick way to make a buck. Countless hordes of Bitcoin prospectors are now using their computers to “mine” for Bitcoins by solving for specific hashed values. Now, the processing power of these miners is being estimated to be six to eight times greater than the top 500 supercomputers combined.

[Share This Article](#)

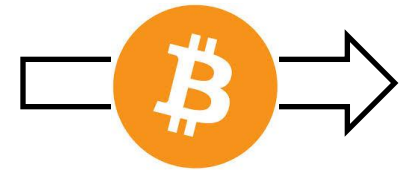
How to create Bitcoins



Recap:

- Solve the next puzzle → get new Bitcoins
- To “**solve**” puzzle i find x_i so that $H(x_{i-1}, x_i) = 0^d$
- The name in block x_i “**gets**” 25 new Bitcoins
- Each new block defines “**next puzzle**”
- In case of competing blocks, **the longest chain “wins”**

How to transfer Bitcoins

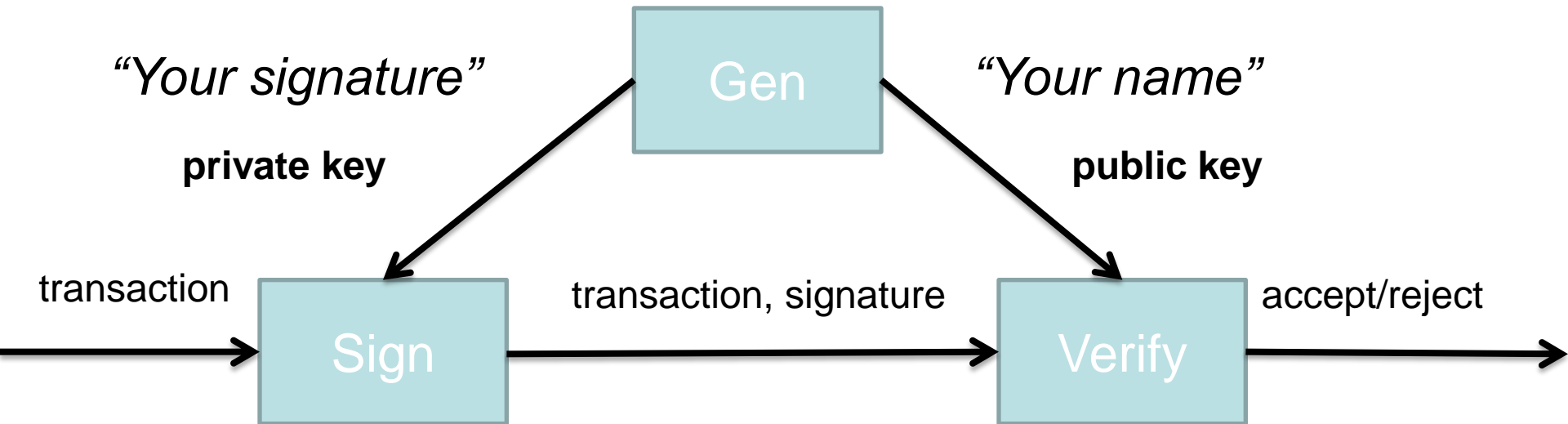
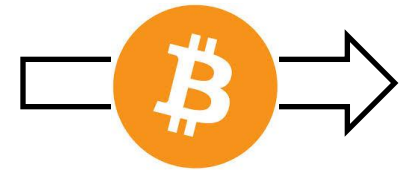


(Digital) Signatures

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



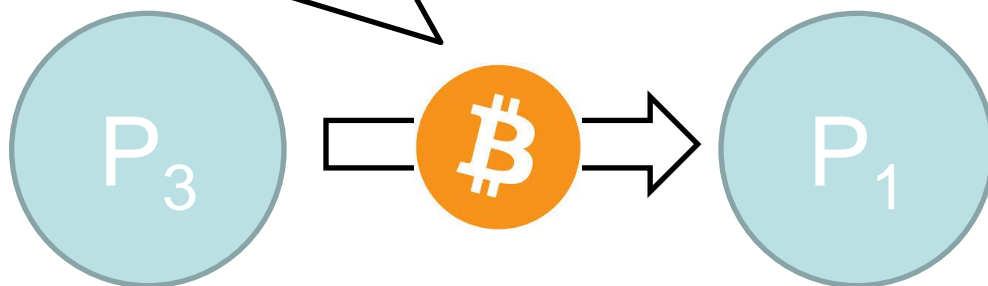
How to transfer Bitcoins



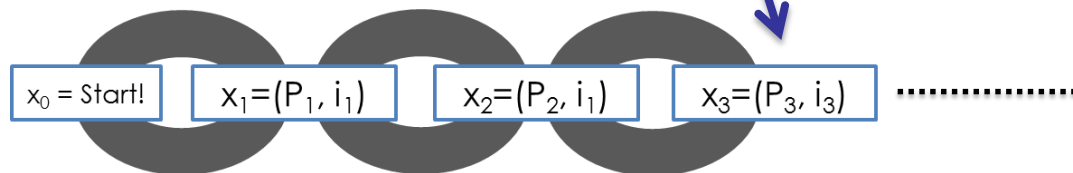
How to transfer Bitcoins



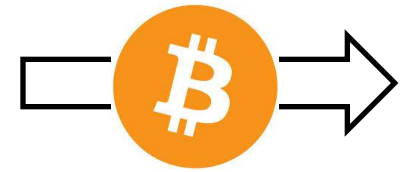
$m = \text{"P3 gives coin 3 to P1"}$
 $s = \text{Sig}(sk_3, m)$



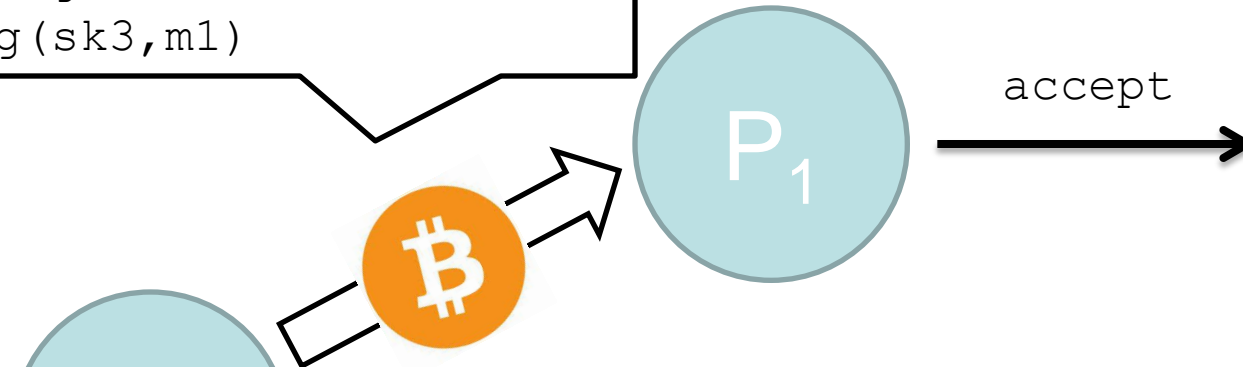
If
 $\text{Ver}(pk_3, m, s) = \text{accept}$
and
P3 owns coin 3
then
return accept



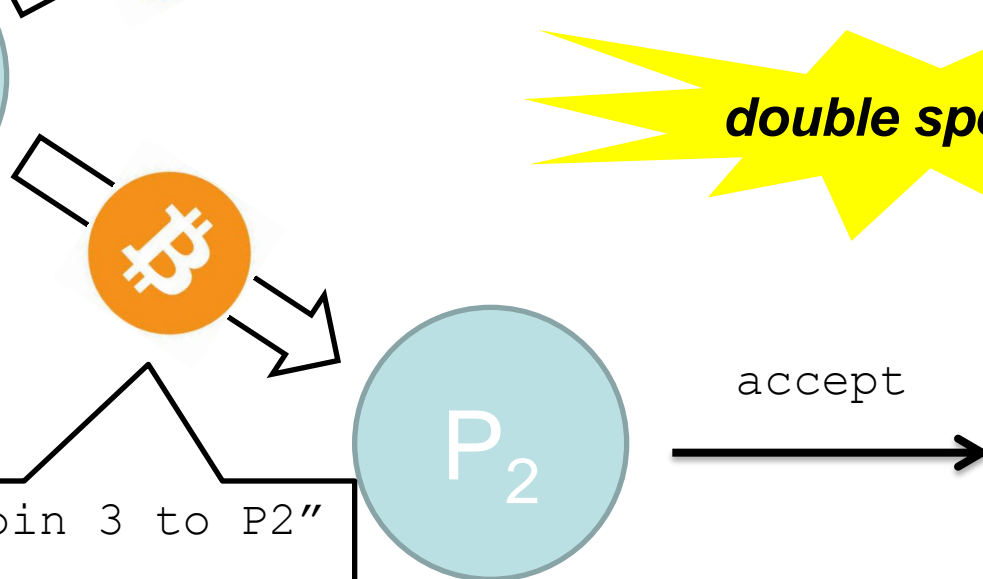
Risk of double spending



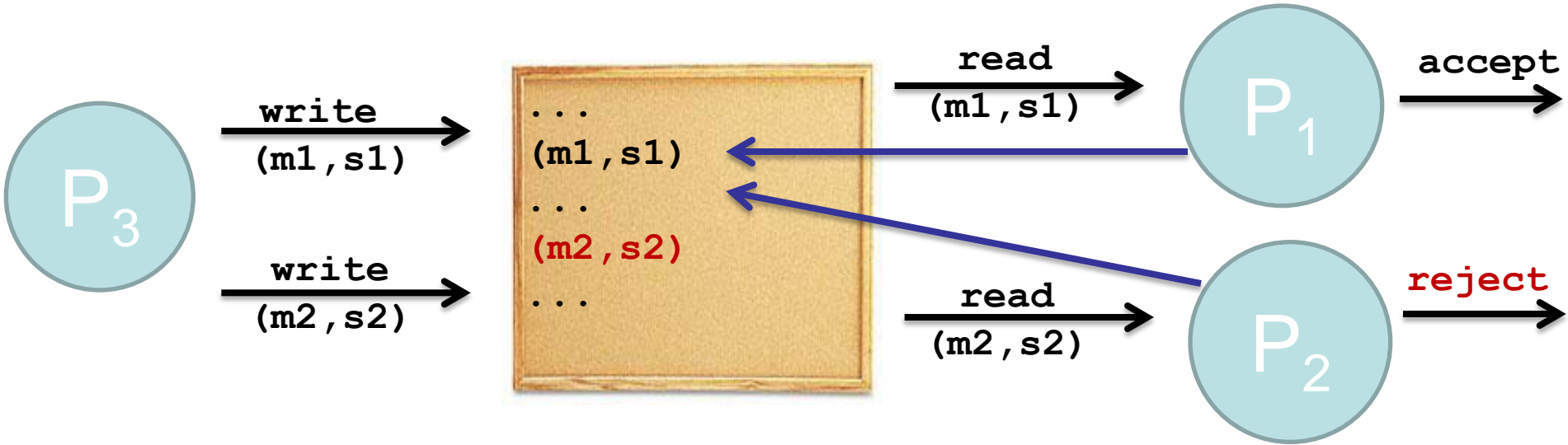
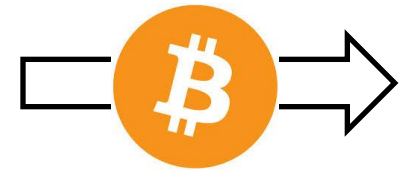
`m1="P3 gives coin 3 to P1"`
`s1=Sig(sk3,m1)`



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



Preventing double spending



$m1 = \text{"P3 gives coin 3 to P1"}$

$s1 = \text{Sig}(sk3, m1)$

$m2 = \text{"P3 gives coin 3 to P2"}$

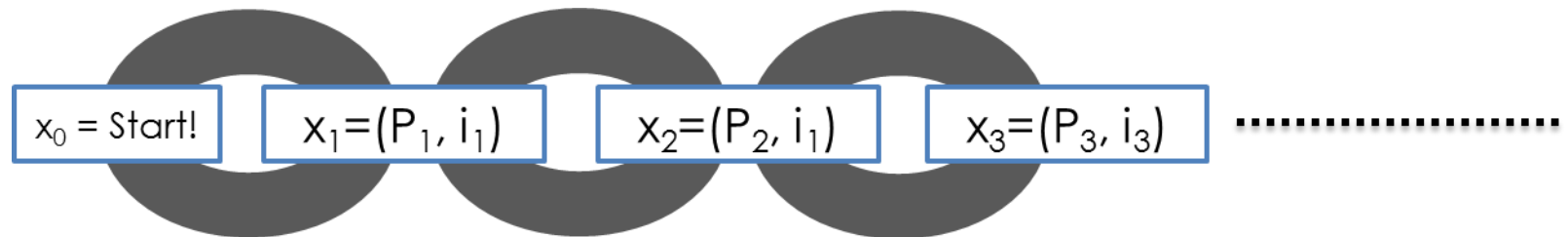
$s2 = \text{Sig}(sk3, m2)$

How to confirm Bitcoin transactions



Main Idea:

- Record **transfers** in the **blockchain ledger**
- **Sign** by including **proof of work**
 - Makes it computationally impossible to change ledger
 - Generates new Bitcoins to party who gave proof of work



How to confirm Bitcoin transactions



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



(m, s)

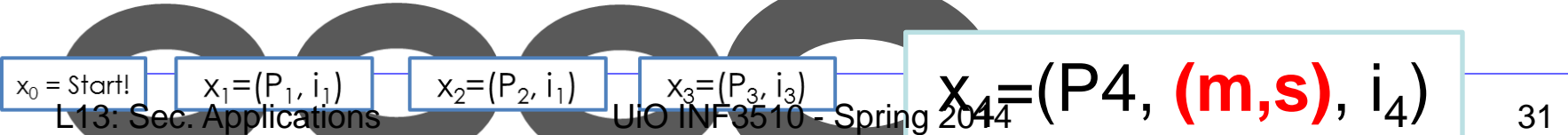
```
SolvePuzzle(L) {
  repeat{
    R = my_name || i++
    T = H(L,R)
  }while(T ≠ 0d)
  return R
}
```

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



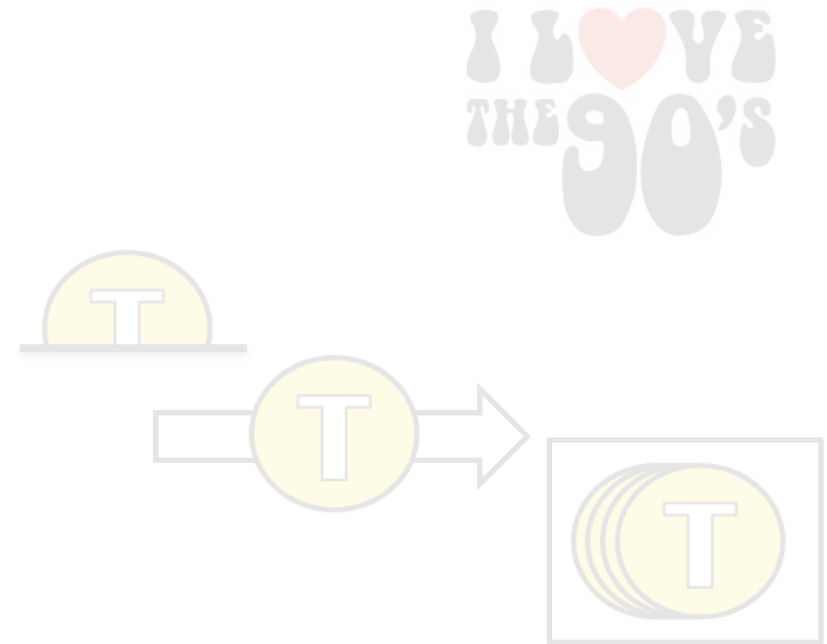
```
SolvePuzzle(L, ...) {
  repeat{
    R = my_name || (m, s) || i++
    T = H(L, R)
  }while(T ≠ 0d)
  return R
}
```

(m, s)





Outline

- Part 0: a little history
- Part 1: TheoryCoin
 - How to *create* coins
 - How to *transfer* coins
 - How to *store* coins



I LOVE
THE 90'S

- Part 2: diff( , )
- Part 3: Problems and issues

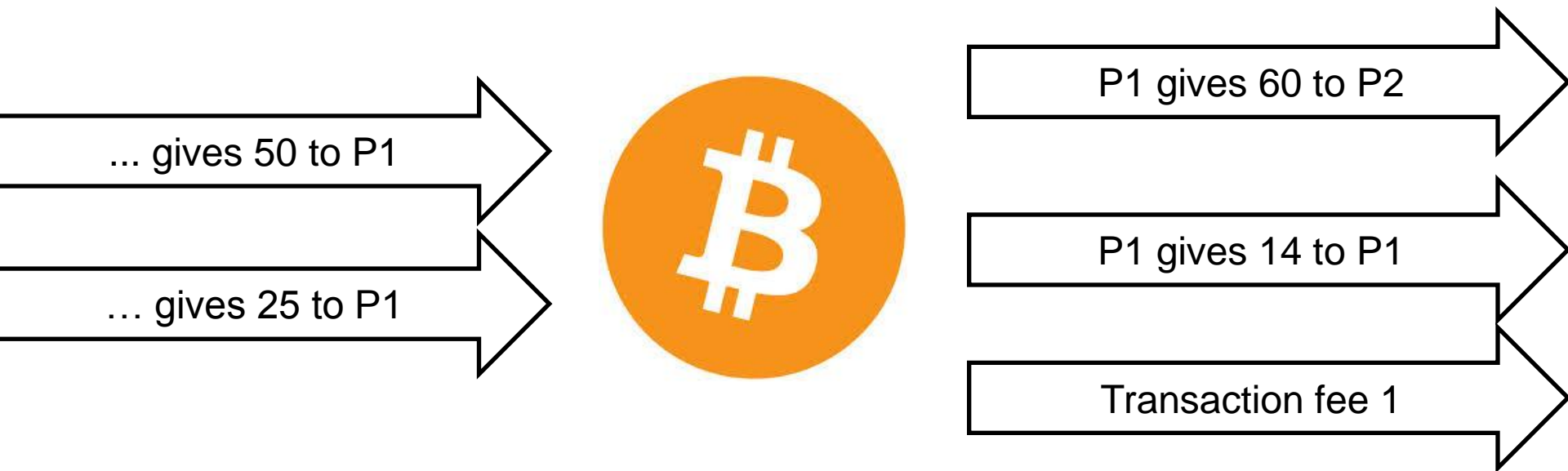


Bitcoin characteristics

- New block of transactions signed **every ~10 mins**
- **Difficulty** of proof of work adjusted every ~2000 blocks
- Initial reward: **50 BTC**
- Halved every ~4 years (now **25 BTC**)

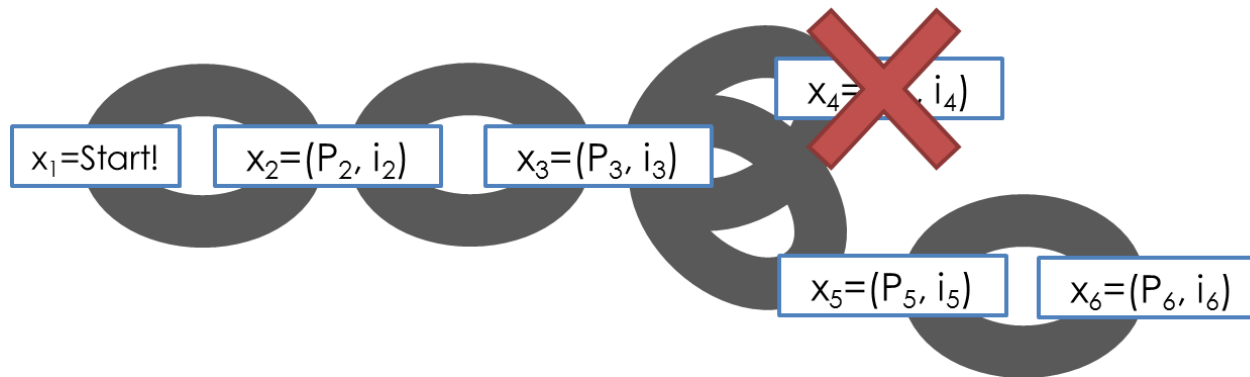
Transactions and fees

Example: P1 wants to give 60 to P2



Failed Bitcoin transactions


- Transaction in **orphaned blocks** are invalid
 - **Wait 6 blocks** (~1 hour) before accepting transaction.
 - **Checkpoints** to prevent complete history rollback.



- **All transaction** are stored in the blockchain
 - (Currently ~14 GB)

Future of Bitcoin ?



- Does not satisfy requirements for currency
 - Not a reliable store of value
 - Not adequate for accounting
 - Only practical for transferring value
- Bitcoin is a virtual commodity 
- Similarly to virtual commodities in games
- The size of wallets keep growing
 - Is it a problem
- Many alternative types of virtual cash



New DigiCash without privacy is mCASH



3D Secure

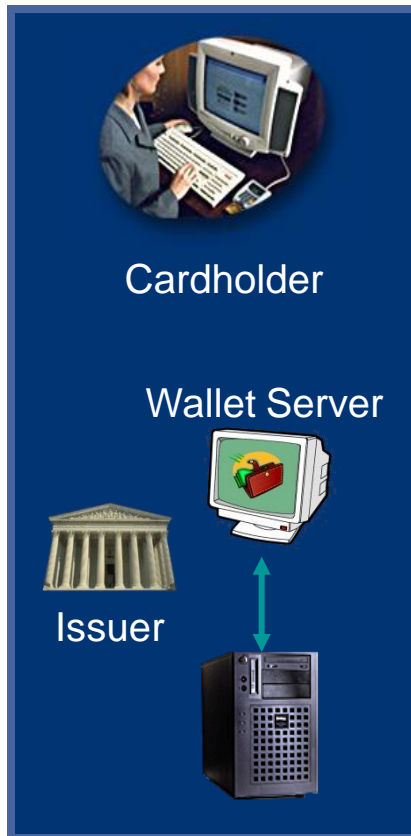


3D Secure
Verified by **VISA** MasterCard.
SecureCode.

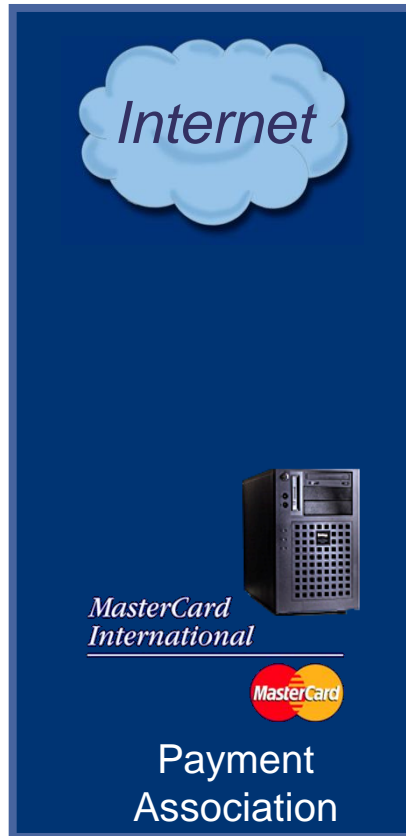
Idea:

- authenticate user without a certificate
- Requires the user to answer a challenge in real-time
- Challenge comes from the issuing bank, not from the merchant
- Issuing bank confirms user identity to merchant

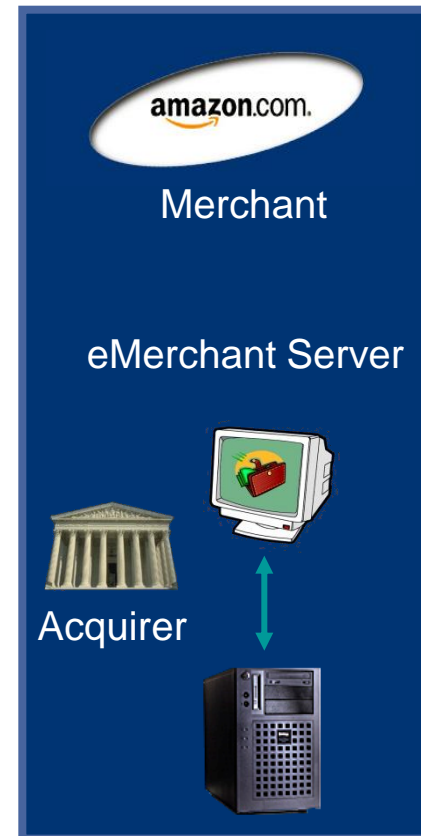
3D Secure parties



Cardholder and card issuer

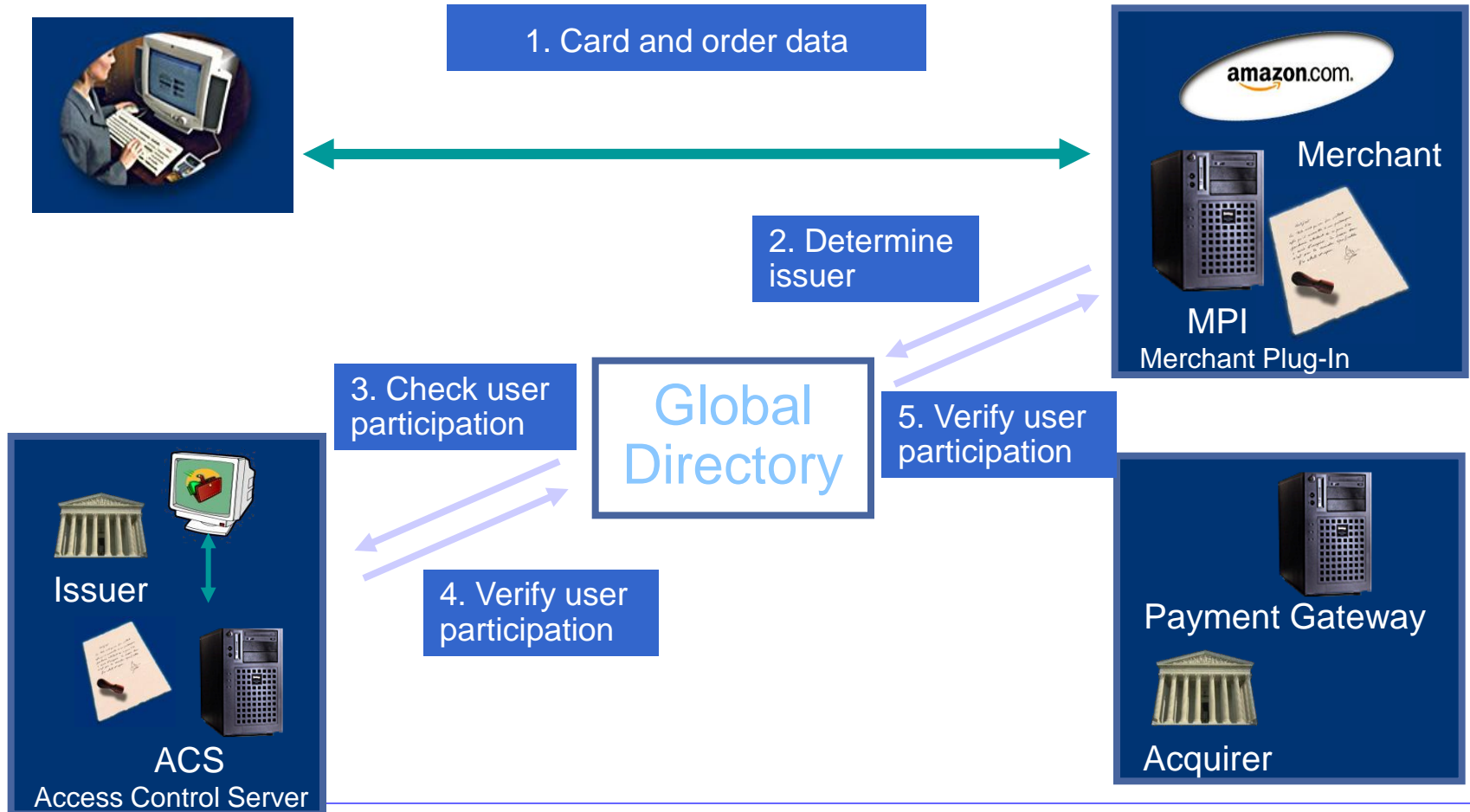


Credit Card Companies

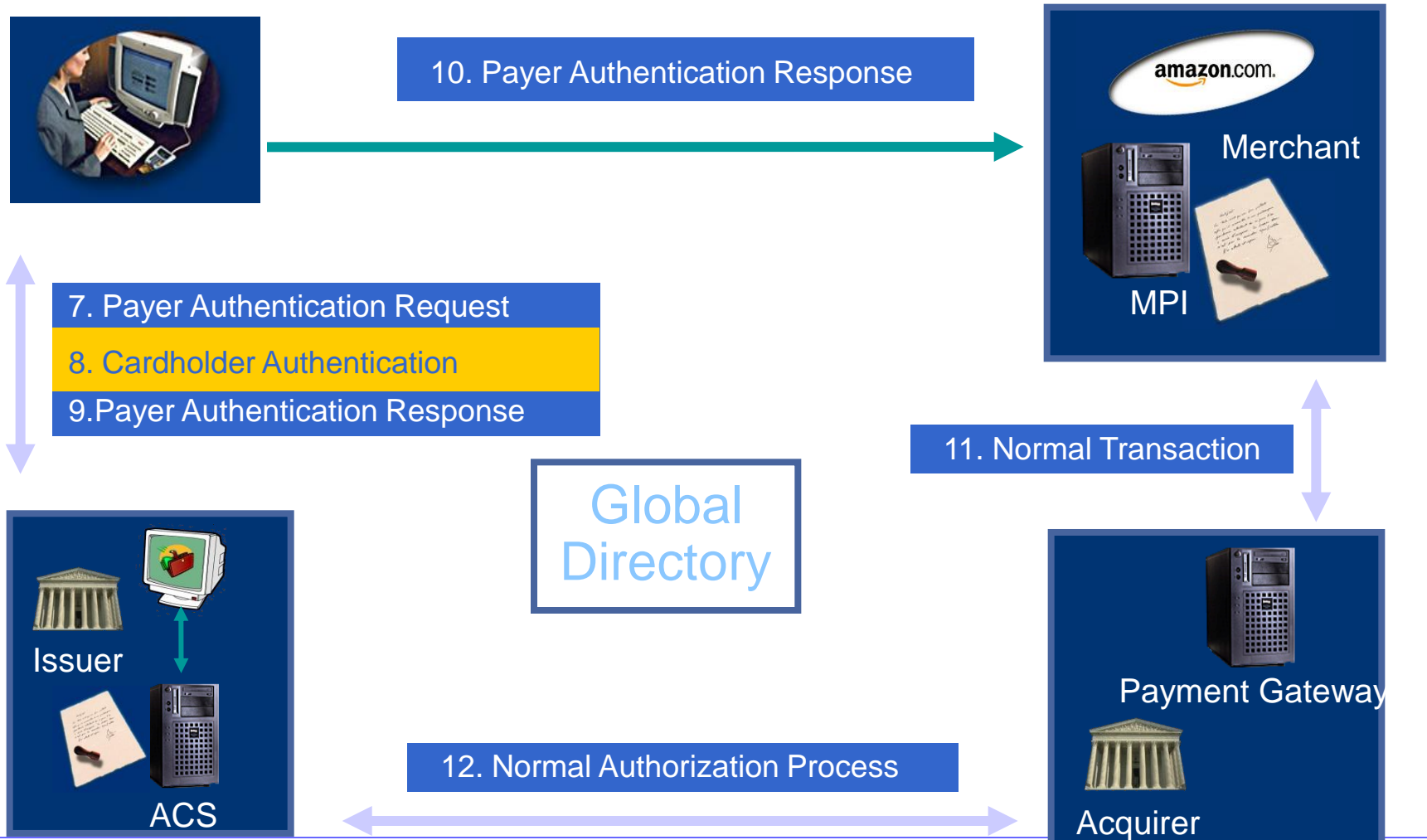


Merchants and their banks

3D-Secure protocol (1)



3D-Secure protocol (2)



Purchase Transaction, cont.

- Step 1 Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase. Merchant now has all necessary data, including PAN and user device information.
- Step 2 Merchant Server Plug-in (MPI) sends PAN (and user device information, if applicable) to Directory Server.
- Step 3 Directory Server queries appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the PAN and device type. If no appropriate ACS is available, the Directory Server creates a response for the MPI and processing continues with Step 5.
- Step 4 ACS responds to Directory Server.

Purchase Transaction, cont.

- Step 5 Directory Server forwards ACS response (or its own) to MPI. If neither authentication nor proof of authentication attempt is available, 3-D Secure processing ends, and the merchant, acquirer, or payment processor may submit a traditional authorization request, if appropriate.
- Step 6 MPI sends Payer Authentication Request to ACS via shoppers device. The Payer Authentication Request message may be **PAReq** (for cardholders using PCs) or **CPRQ** (for cardholders using mobile Internet devices - see 3-D Secure: Protocol Specification - Extension for Mobile Internet Devices).
- Step 7 ACS receives Payer Authentication Request.
- Step 8 ACS authenticates shopper using processes applicable to PAN (password, chip, PIN, etc.). Alternatively, ACS may produce a proof of authentication attempt. ACS then formats Payer Authentication Response message with appropriate values and signs it. The Payer Authentication Response message is **PARes** if **PAReq** was received, or **CPRS** if **CPRQ** was received. (**CPRS** is created using values from the **PARes**.)

Purchase Transaction, cont.

- Step 9 ACS returns Payer Authentication Response to MPI via shoppers device. ACS sends selected data to Authentication History Server.
- Step 10 MPI receives Payer Authentication Response.
- Step 11 MPI validates Payer Authentication Response signature (either by performing the validation itself or by passing the message to a separate Validation Server).
- Step 12 Merchant proceeds with authorization exchange with its acquirer. Following Step 12, acquirer processes authorization with issuer via an authorization system such as VisaNet, then returns the results to merchant.

Criticism against 3D Secure

- Verifiability of site identity
 - The "Verified by Visa" system has drawn some criticism, since it is hard for users to differentiate between the legitimate Verified by Visa pop-up window or inline frame, and a fraudulent phishing site.
- Lack of support on many Mobile devices

Information warfare

- The term information warfare refers to peace time activities
 - psychological operations (psyop)
 - cyber war/net war
- In wartime the term is Command, Control, Communications, Computers, Intelligence, Sensors, Reconnaissance Warfare (C4ISRW)
 - military operations, like bombing communications infrastructure, throwing metallic fibre trash on radars
 - jamming radio communications
 - largely targeted to military command systems
 - and to communication system infrastructure
 - airplanes, trains, telecommunications

4 Fundamental Changes

New Geostrategic Context

- Cyberspace: new operational realm/battlespace
 - Dominant in business, politics, warfare
- Convergence
 - Digital: 1110101110001010 = lingua franca
 - Information mediums (radio, TV, phone, etc)
- Global Omnilinking
 - Electronic digital connectivity of people, organizations, governments...globally & instantly
- Critical Infrastructure Protection
 - Opportunity....and vulnerability
 - Critical to advanced societies, but public/private links poorly understood
 - Roles and missions; what does “interagency” mean?

Impact of information society

- Global Economy
 - Dependent on interlinked networks
 - Information as critical as energy and capital
- Global Audience
 - Real-time 24-hour cycle
 - Waning controllability of information
- Global Society
 - Contact anyone, anywhere, anytime
- Strategic Impact: Diplomatic, Economic, Military

Potential for information operations

- Information content and information technology
 - Strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis
 - affects the global behavior of governments, supra-governmental organizations, and societies
 - affects national security”

U.S. Cyber Operations Policy, Presidential Policy Directive

- Cyber operations as consisting of:
 - *Cyber Collection,*
 - *Defensive Cyber Effects Operations (DCEO)*
 - *Offensive Cyber Effects Operations (OCEO)*

US Cyber Collection

- *“Operations and related programs or activities conducted [...] for the primary purpose of collecting intelligence - including information that can be used for future operations - from computers, information or communications systems, or networks with the intent to remain undetected. Cyber collection entails accessing a computer, information system, or network without authorization from the owner or operator of that computer, information system, or network or from a party to a communication or by exceeding authorized access. [...].”*

US Defensive Cyber Operations

- Defensive Cyber Effects Operations (DCEO): Operations and related programs or activities - other than network defense or cyber collection - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks for the purpose of defending or protecting against imminent threats or ongoing attacks or malicious cyber activity against U.S. national interests from inside or outside cyberspace.

US Offensive Cyber Operations

- Offensive Cyber Effects Operations (OCEO): Operations and related programs or activities - other than network defense, cyber collection, or DCEO - conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks.

Which countries have info warfare strategies ?

- All countries with a defence strategy also have information operations strategies
- Only the USA has official Information Operations Policy
 - Other countries might think that since information operations are invisible, they can pretend that they don't have a strategy.

End of Lecture