The blockchain: what, why & how

Target audience: aspiring billionares

Play on the chain

Benny Michielsen
Info Support

TOPCONF
Duesseldorf

Rock Paper Scissor Lizard Spock

- http://bbbg.azurewebsites.net/

Play on the chain

- Keep the browser open for ”*faster*” gameplay
- Don’t clear your history

Benny Michielsen

benny.michielsen@infosupport.com

Tech aficionado

Programming, Zbgureshpxre

Identity
Integrity
Transactions
Miners

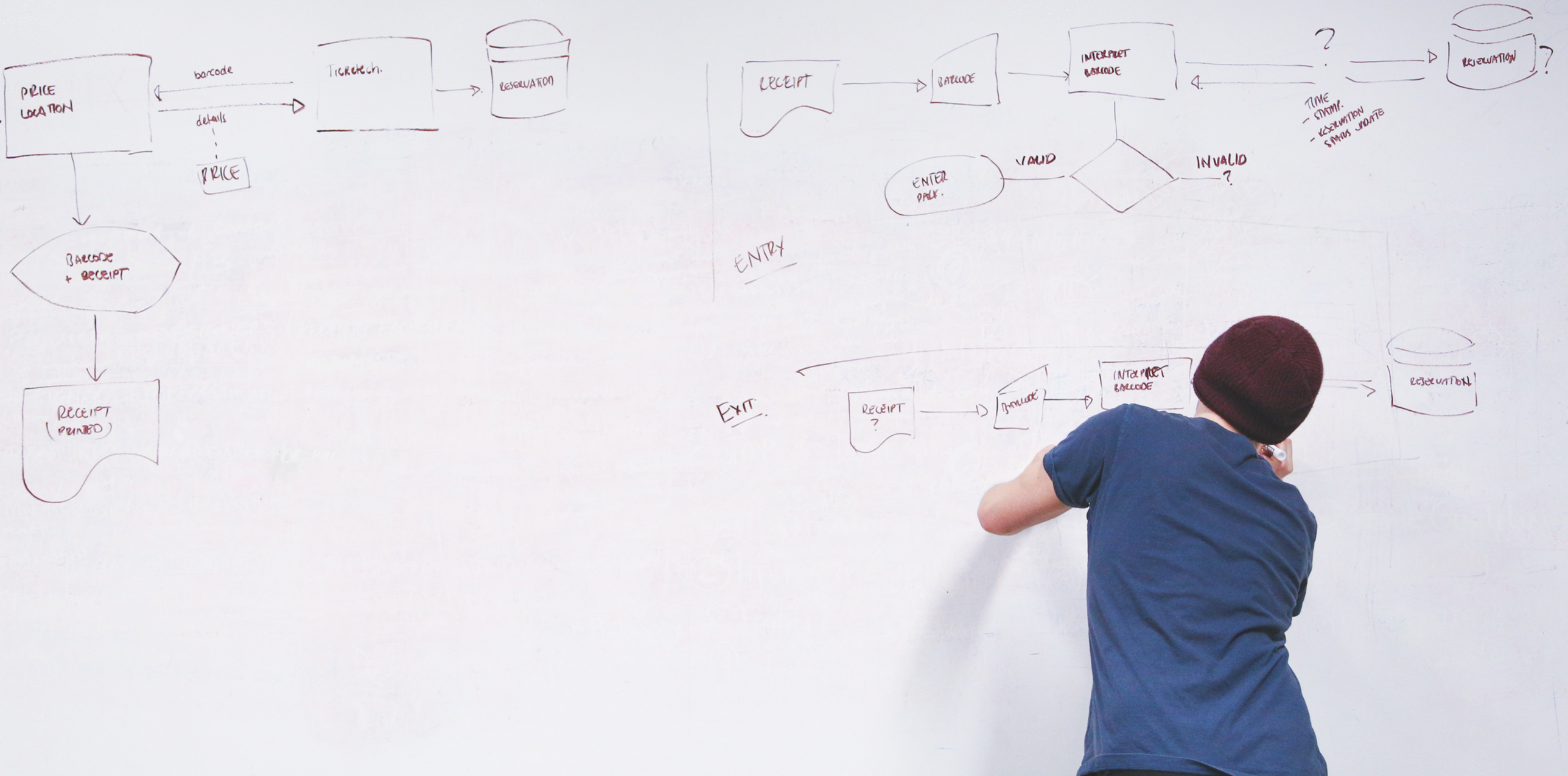
Bitcoin

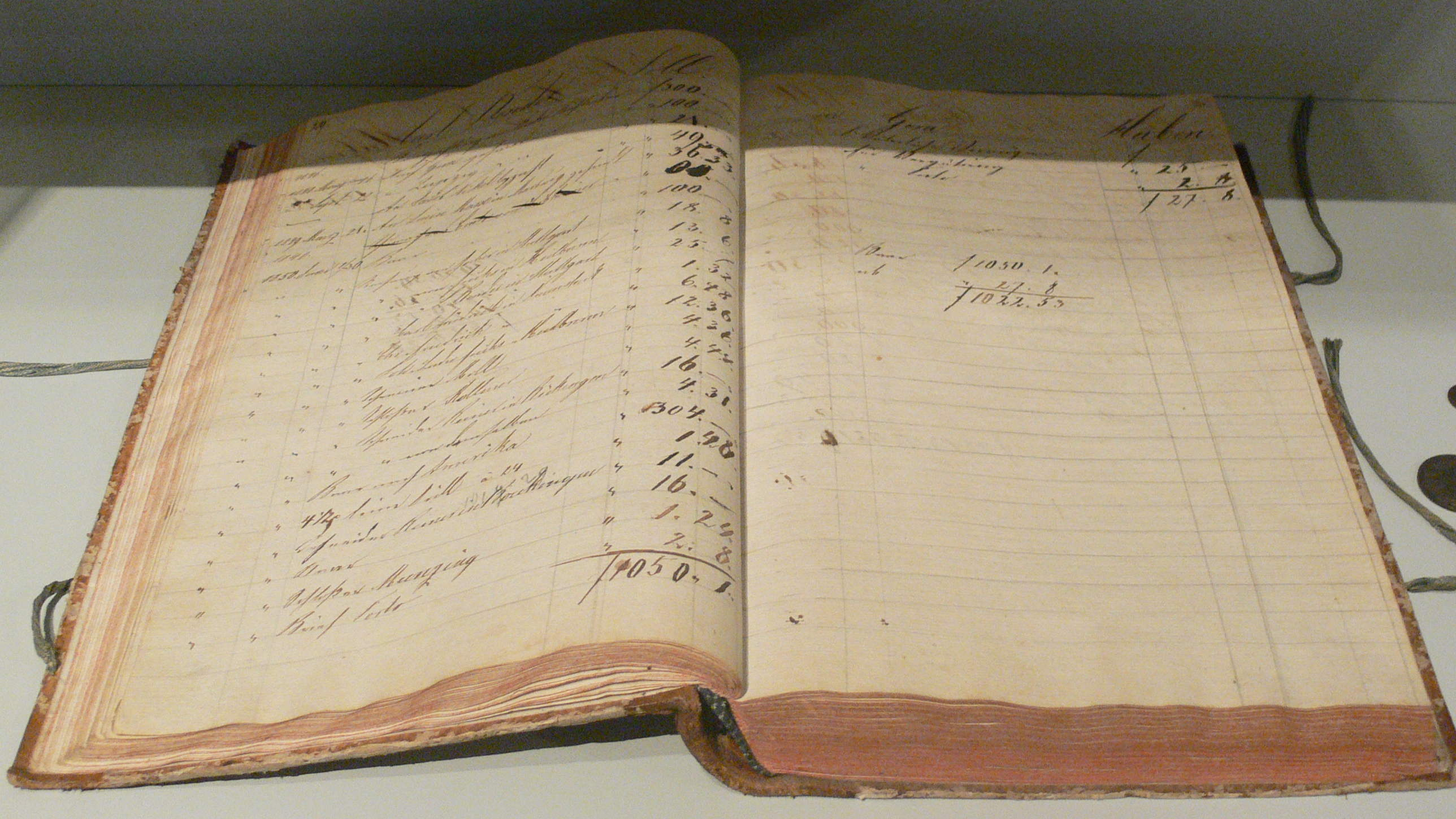
DApp architecture
Smart contracts
JS & .NET

Ethereum


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


WESTERN
UNION
®


PRICE
LOCATION
barcode
details
PRICE
Ticketch.
RESERVATION
BARCODE
+ RECEIPT
RECEIPT
PRINTED
RECEIPT
BARCODE
INTERPRET
BARCODE
RESERVATION
TIME
- STAMP.
- RESERVATION
STATUS UPDATE
ENTER
PACK.
VALID
INVALID
ENTRY
EXIT
RECEIPT
?
INTERPRET
BARCODE
RESERVATION



Identify

- Where do I need to register?
- Where can I send funds to?

- Public Key Cryptography
- Random number to create a private key
- No central registry

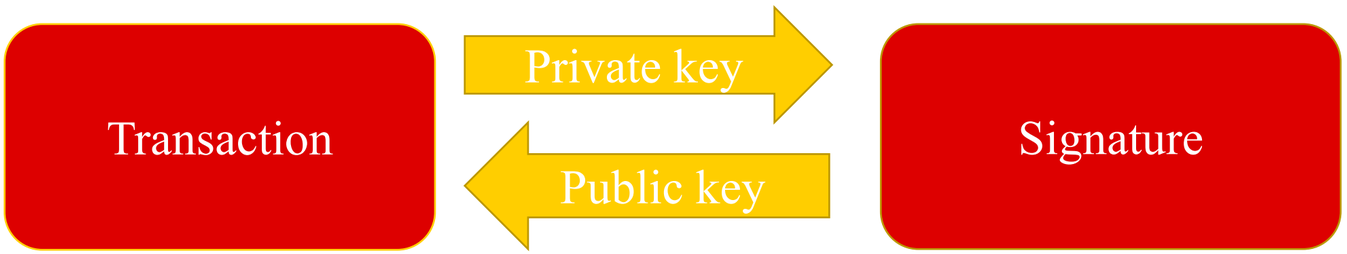
- Unlikely to create private key twice 10^{48}
  - All atoms in the earth: 10^{50}

- Important to keep your private key safe!

I bought some Bitcoin at an atm 😃

Signing Transactions

- How to validate integrity and source of a transaction?
- Public Key Cryptography



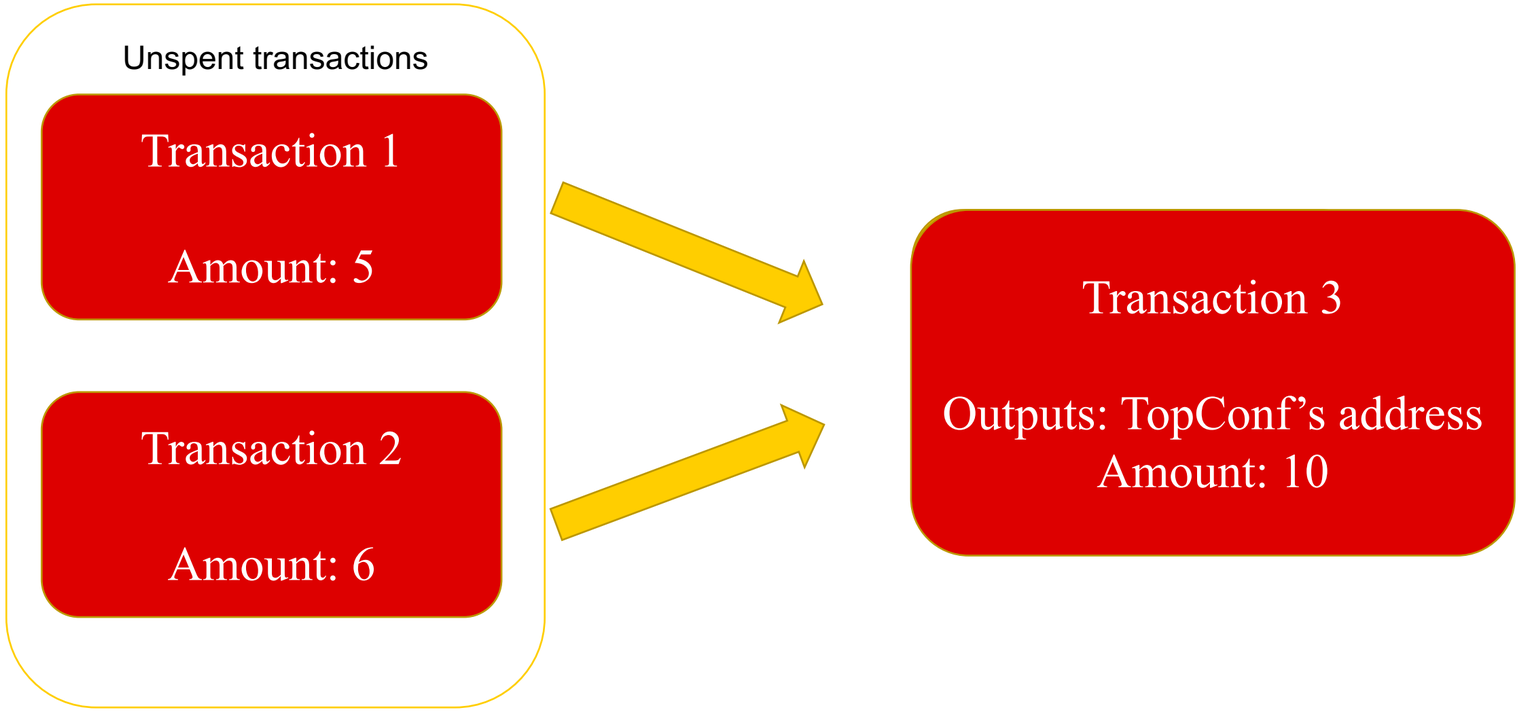
Transactions

Transactions

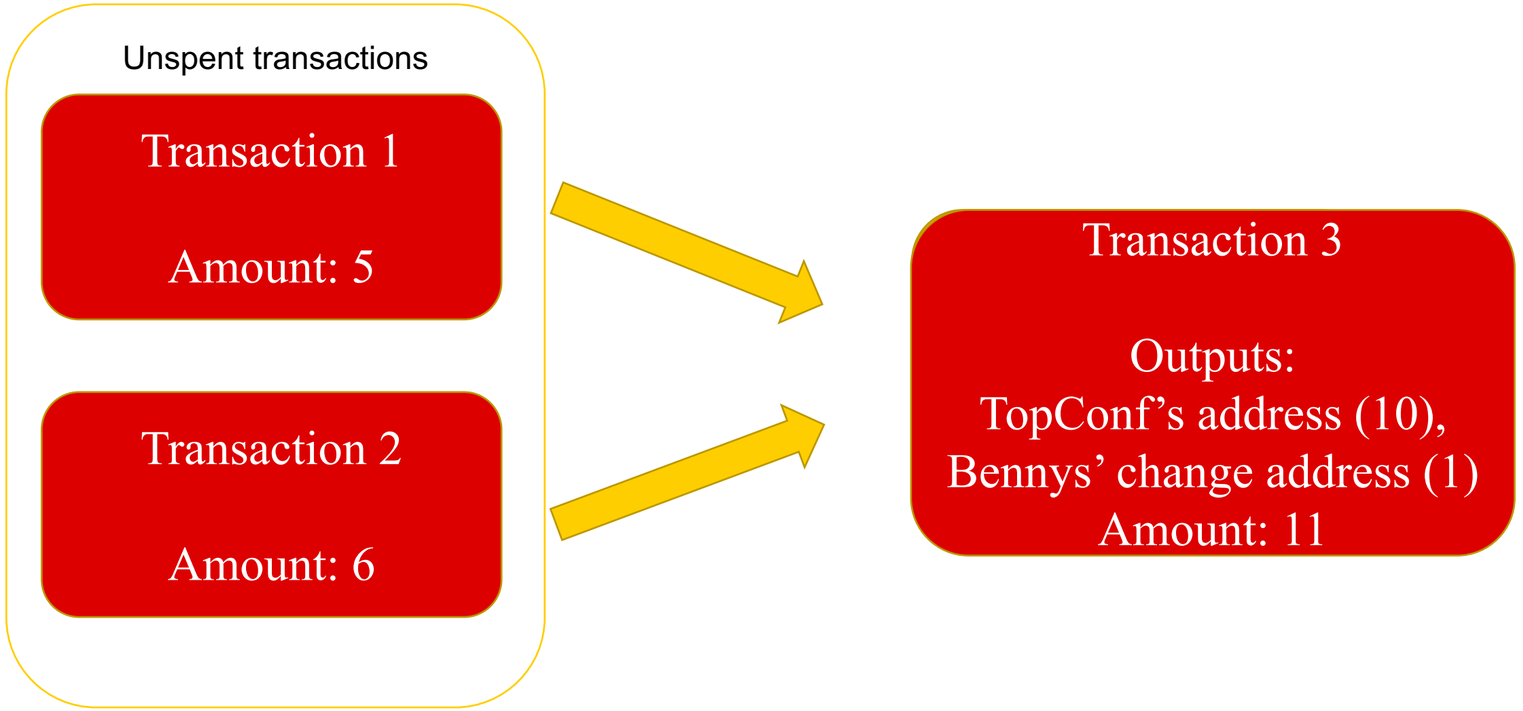
Transaction 3

Outputs: TopConf's address
Amount: 10

Transactions



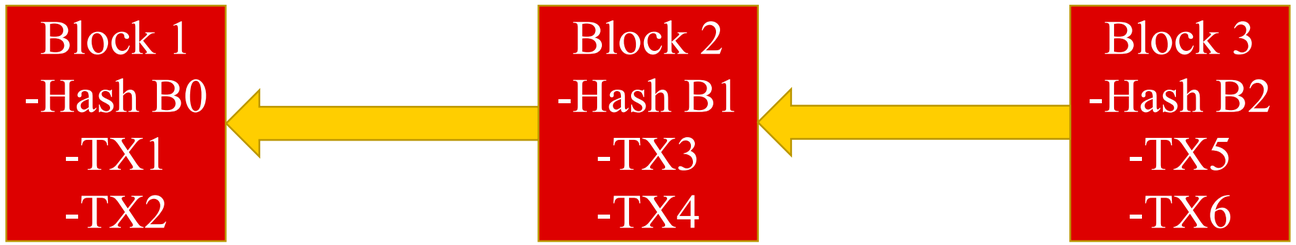
Transactions



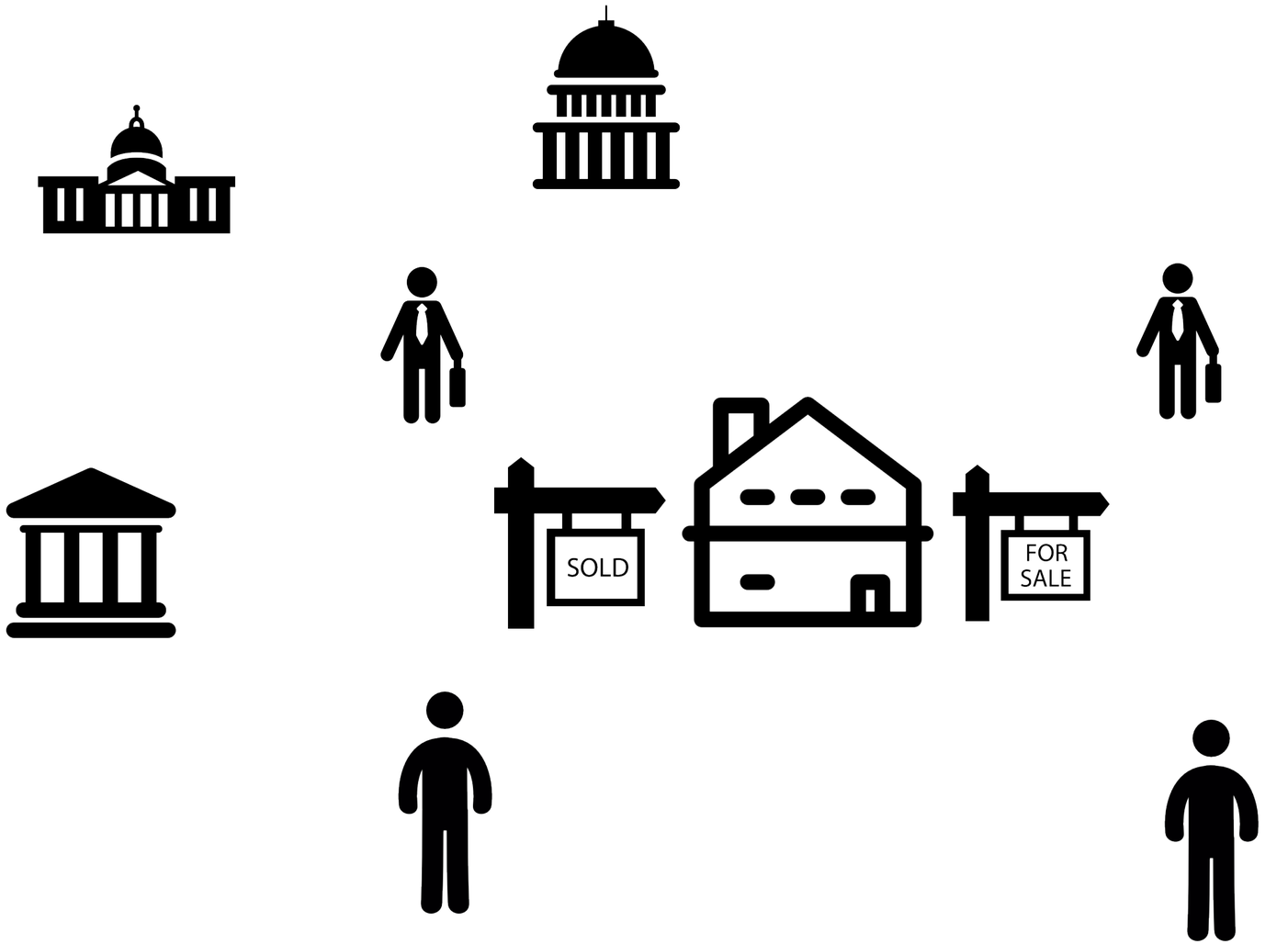
Miners / Bookkeepers

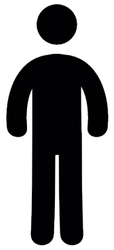
- Who keeps track of the transactions?

- Miners
  - Receive transactions
  - Group transactions to form a new block
  - Hash previous block + hash new block + random number < puzzle hash
    - HASH & HASH & ? < 100
  - Goal: guess random number
    - Very compute intensive
    - Are rewarded for finding the number
  - One quintillion hashes per second


Block 1
-Hash B0
-TX1
-TX2
Block 2
-Hash B1
-TX3
-TX4
Block 3
-Hash B2
-TX5
-TX6

Single distributed ledger	• Single ledger • Everyone has a copy
Immutable	• Data can not be tampered with • Hashing previous block makes the network secure
Trust(less)	• Miners keep track of transactions • Signatures and hashes provide integrity
Automated	• Miners work continuously


SOLD
FOR
SALE



Single distributed ledger

- Property information stored in a blockchain

Immutable

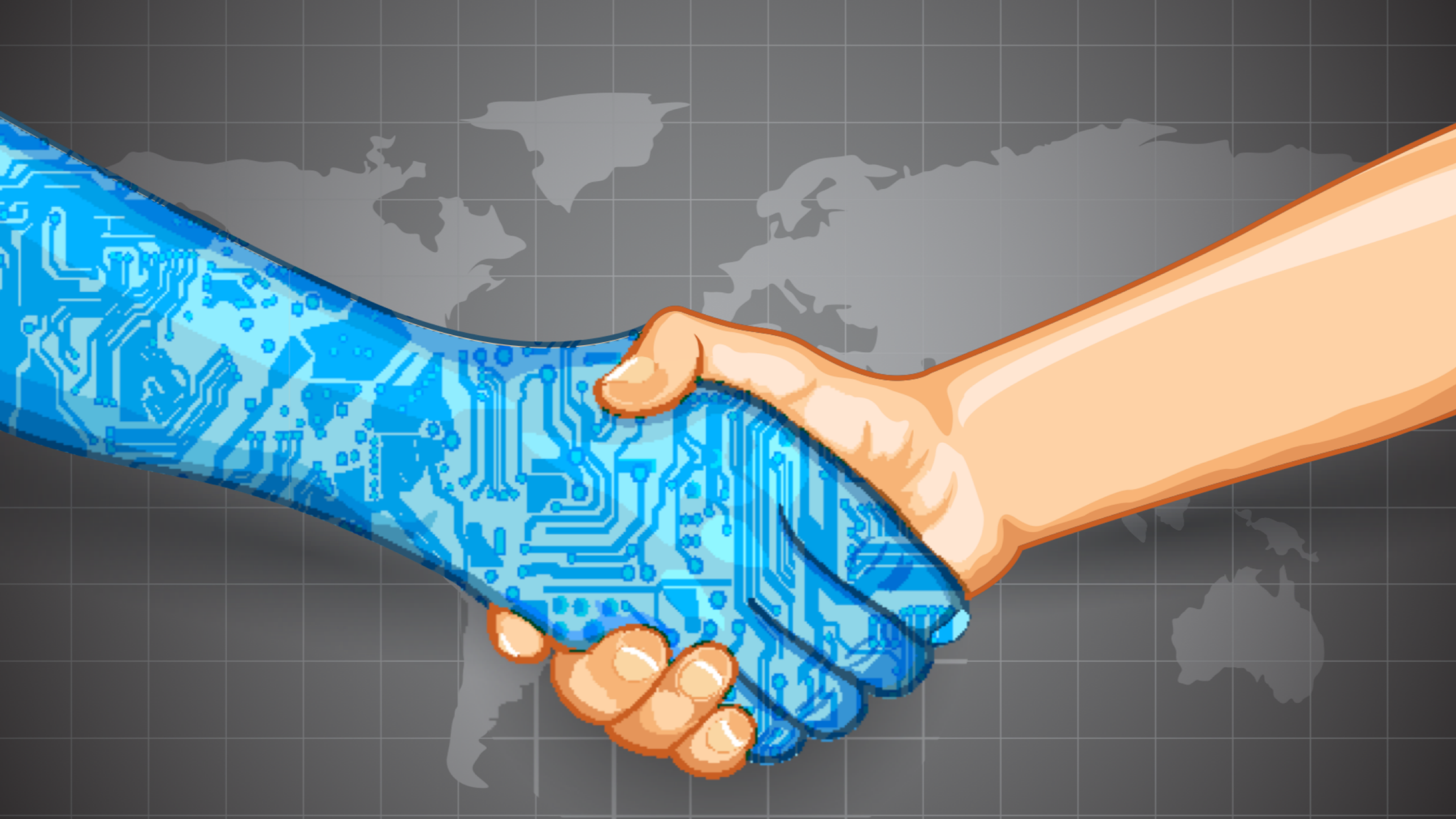
- Data can not be tampered with

Trust(less)

- Intermediaries no longer needed
- Identity is inherently verified

Automated

- Paper process can become a digital process
- Reduce in cost
- Increase in speed



Ethereum

- Bitcoin has limited possibilities to program against

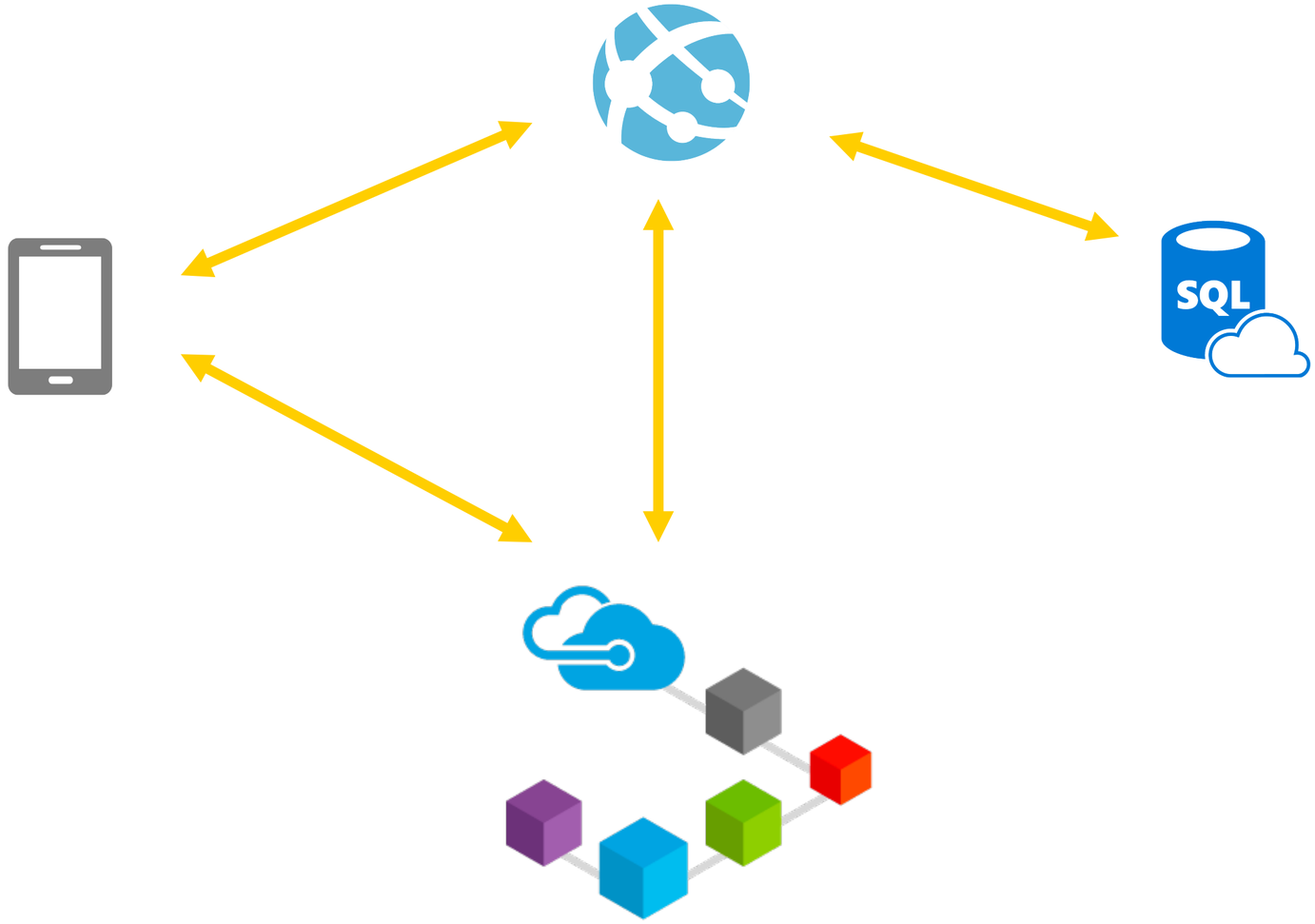
- Ethereum blockchain
  - Programmable by design
  - Distributed “computer”
  - Develop smart contracts/dapps
  - Most popular development blockchain

ethereum

- Each node runs contracts and verifies result
  - Calculation costs gas (payed for with Ether)
- Not fast, but very reliable
- Deploy contract to address
- Trigger contract by calling functions and sending ether

Rock, Paper, Scissor, Lizard, Spock!

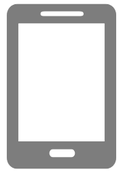

Demo


SQL


.NET
Core
HTML
TRUFFLE

Signup

SendEther



Player 1

Nickname

Address

Playing a game

Player 1

CreateContract(SHA1 + SHA2)

SHA1 + SHA2

Player 2

Winner

Enough talking, show me the code

Lessons learned

- Cutting edge
- UX
  - Speed
  - Cost
- Potential


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
E-mail: SCOTTADAMS@AOL.COM
© 1995 United Feature Syndicate, Inc.(NYC)

PAPERCHASE

Sweden's blockchain-powered land registry is inching towards reality

By Joon Ian Wong | April 03, 2017

Jong VLD komt met voorstel om huis te kopen zonder notaris

21-09-17, 10.24u - Bewerkt door: ESA - Bron: Belga

© photo_news 1

TOPCONF Duesseldorf


Welcome to the digital vault of the future.
Everledger is a global startup that uses the best of emerging technology including blockchain, smart contracts and machine vision to assist in the reduction of risk and fraud for banks, insurers and open marketplaces.

Benny Michielsen

Info Support

blog.bennymichielsen.be

bennym@infosupport.com

@bennymichielsen

TOPCONF
Duesseldorf