The blockchain: what, why & how

Target audience: aspiring billionares

Play on the chain

Benny Michielsen

TOPCONF TALLINN

Info Support Solid Innovator

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

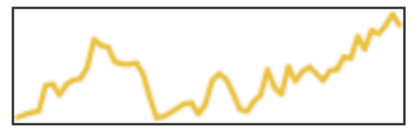
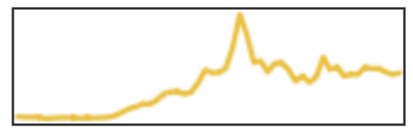
Programming, Zbgureshpxre

Identity
Integrity
Transactions
Miners

Bitcoin

DApp architecture
Smart contracts
JS & .NET

Ethereum

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	€96,538,010,991	€5787.59	€2,856,362,778	16,680,162 BTC	2.58%	
2	Ethereum	€27,213,885,858	€284.27	€899,383,067	95,733,690 ETH	4.64%	
3	Bitcoin Cash	€18,287,458,029	€1088.36	€1,322,396,296	16,802,825 BCH	3.68%	
4	Ripple	€6,814,766,845	€0.176444	€68,078,541	38,622,870,411 XRP *	0.00%	
5	Litecoin	€2,862,843,374	€53.18	€140,148,613	53,832,257 LTC	2.36%	

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

?

TIME
- STAMP.
- RESERVATION
STATUS UPDATE

RESERVATION

?

ENTER
PARK.

VALID

INVALID
?

ENTRY

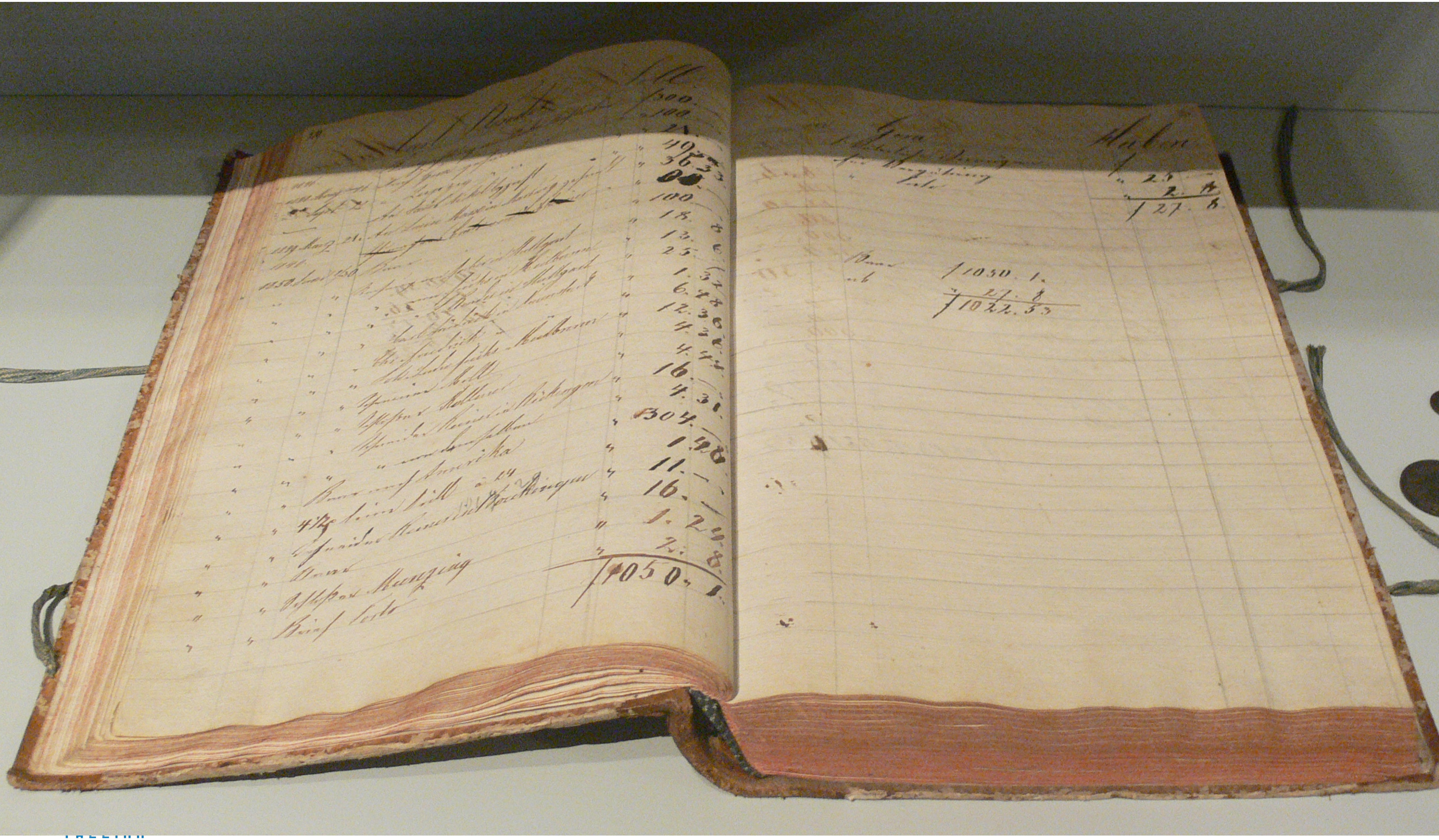
EXIT.

RECEIPT
?

BARCODE

INTERPRET
BARCODE

REJECTION


Haben
Amerika
1050. 1.

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

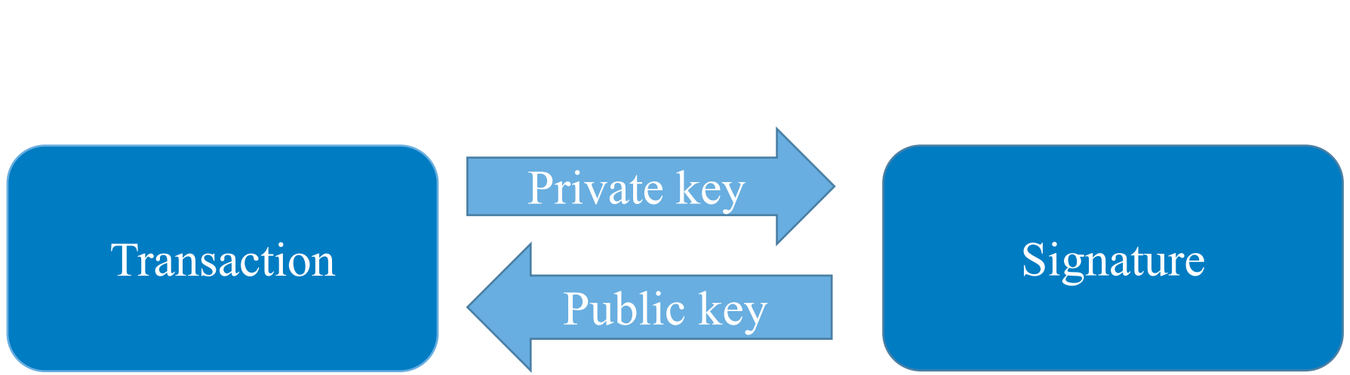
- Unlikely to create private key twice 10^{48}
  - All atoms in the earth: 10^{50}

- 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



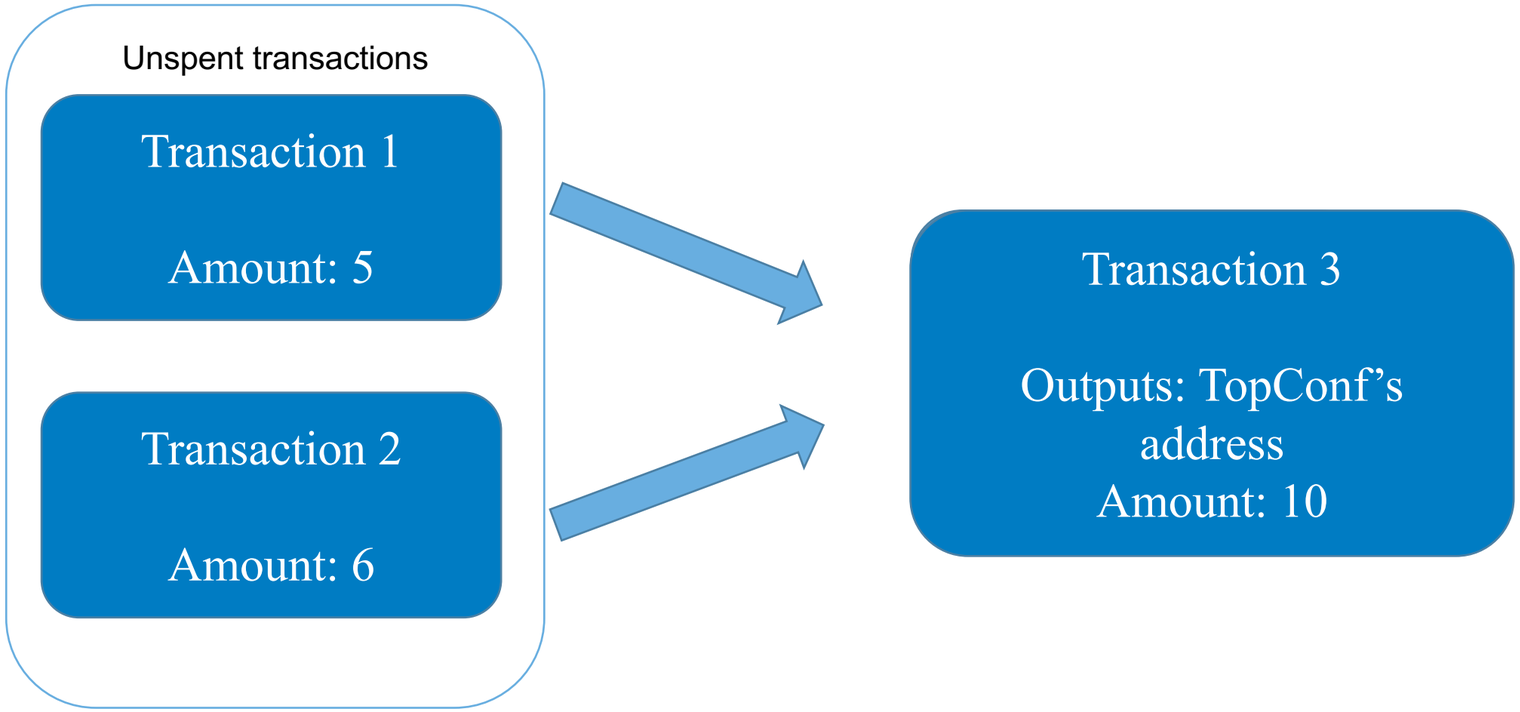
Transactions

Transactions

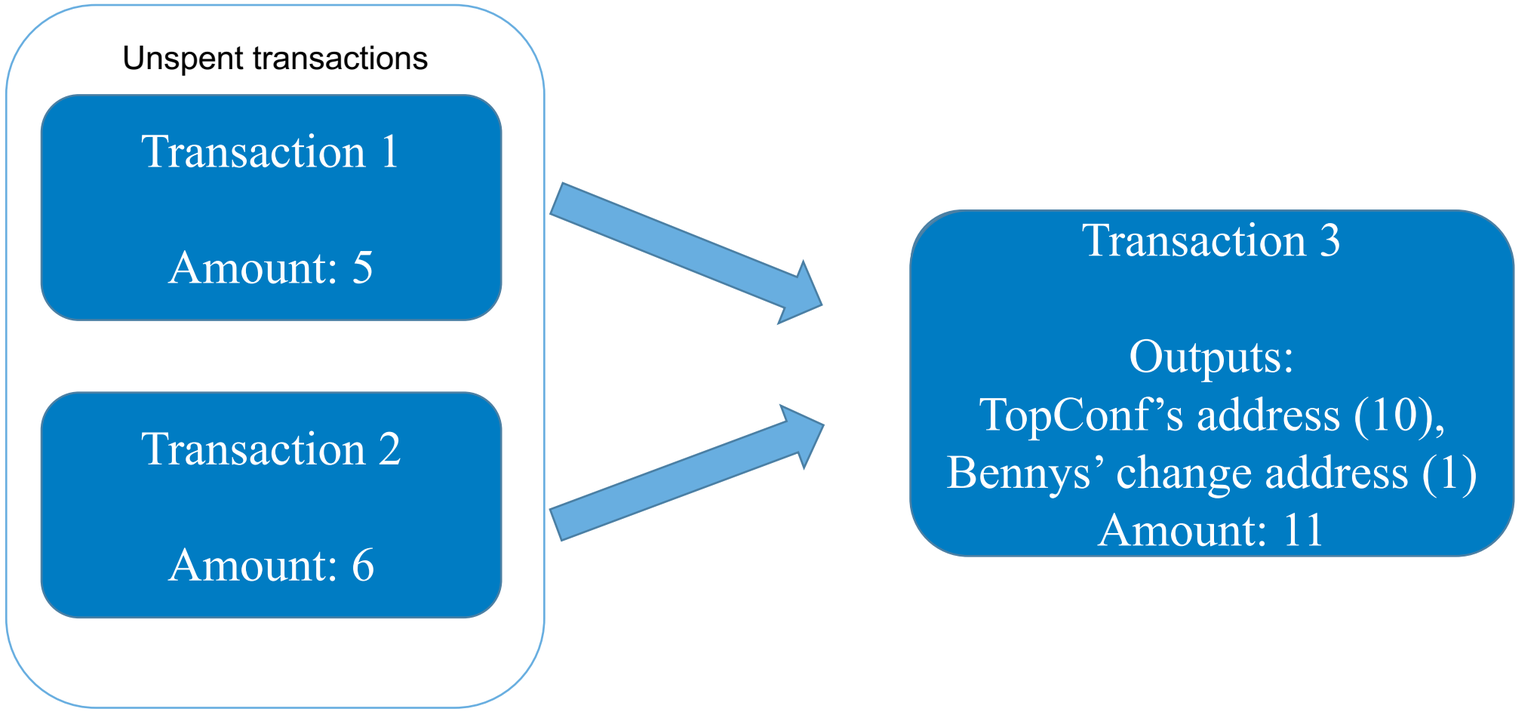
Transaction 3

Outputs: TopConf's address
Amount: 10

Transactions



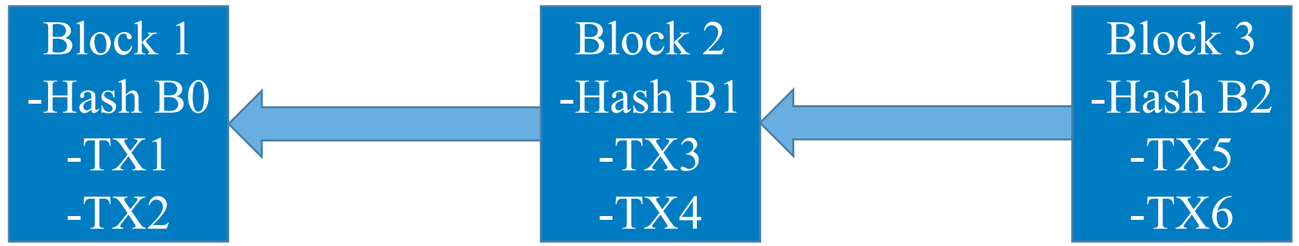
Transactions



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

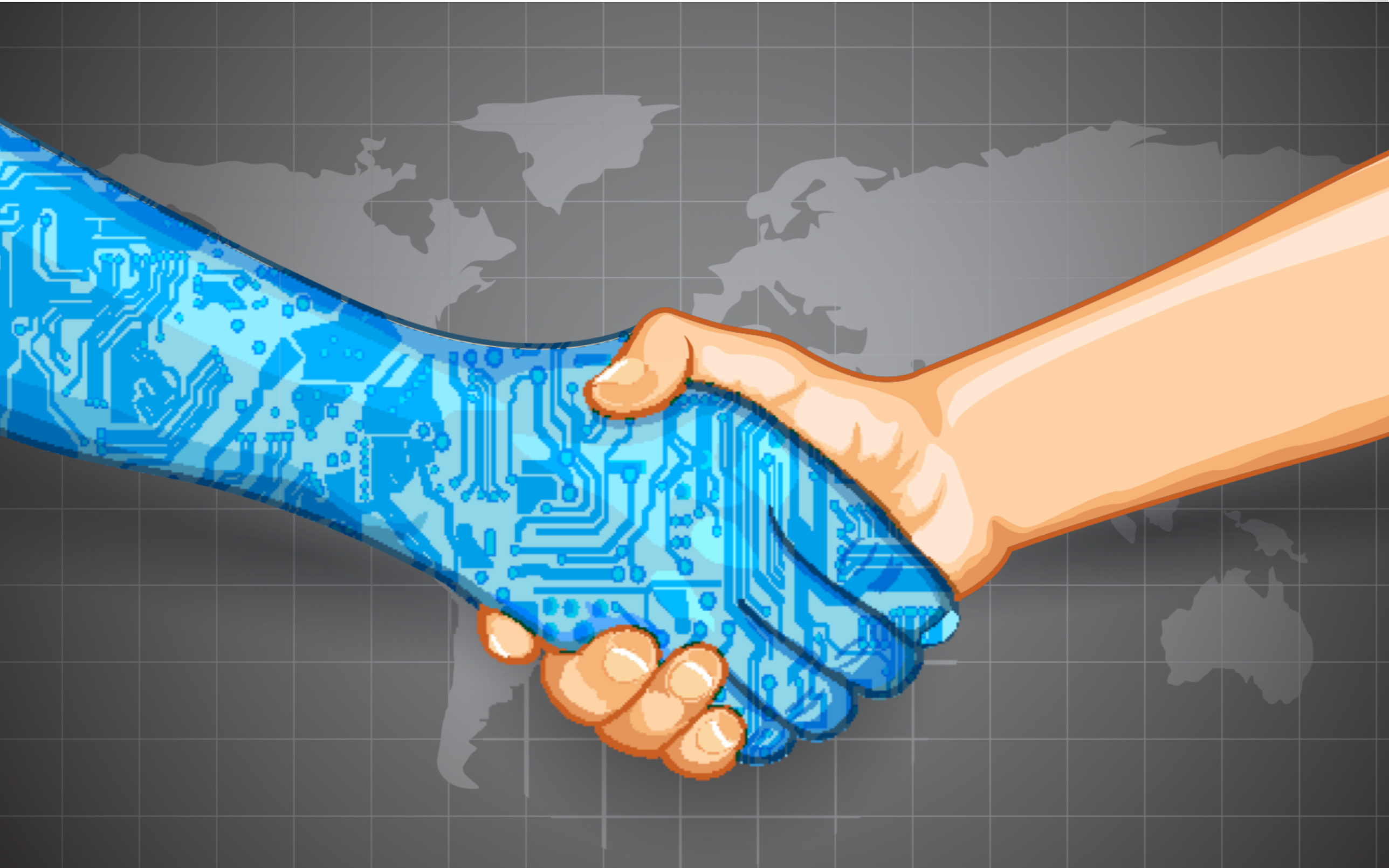
Single distributed ledger	• Single ledger • Everyone has a copy
Immutable	• Data can not be tampered with • Hashing previous block makes the network secure
Trust(less)	• Miners keep track of transactions • Signatures and hashes provide integrity
Automated	• Miners work continuously

Andreas Brekken Follow
Sep 4 · 10 min read

OpenBazaar: What Happened to Bitcoin's eBay Killer App?

OpenBazaar is eBay on the blockchain, promoted as the "killer app" for Bitcoin since 2014. Has OpenBazaar's $4.3M in VC funding made eBay obsolete with world-wide open trade?

> *TL;DR: OpenBazaar is unstable and has no listings. I was unable to use it to buy or sell online.*



Ethereum

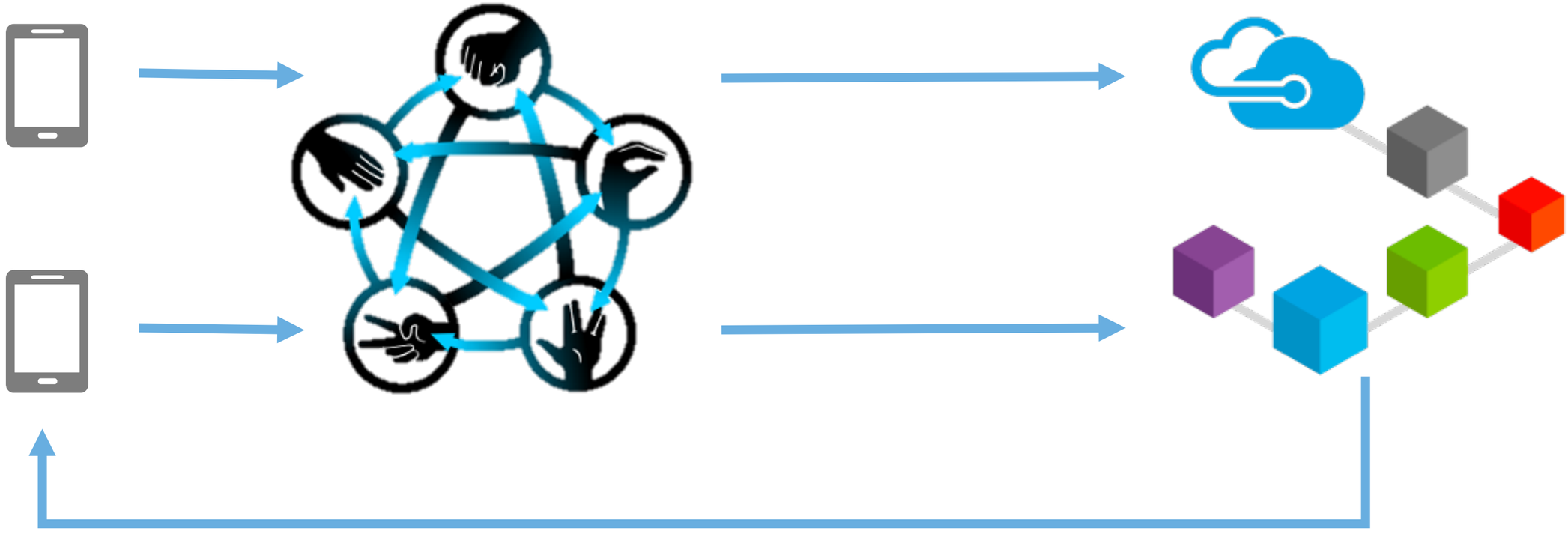
- Bitcoin has limited possibilities to program against

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

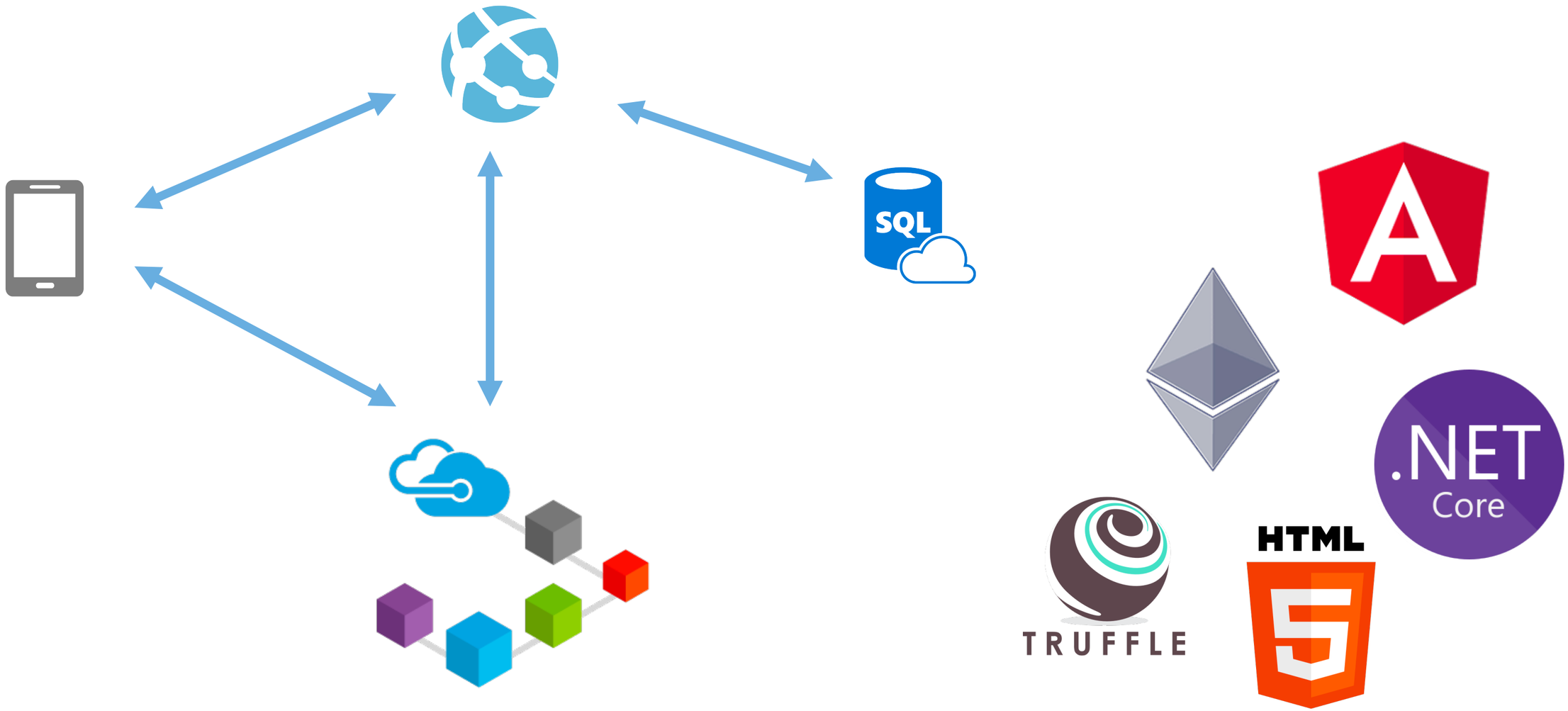
ethereum

- 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
TRUFFLE
HTML
.NET
Core

Signup

Player 1
Nickname
Address

SendEther

Playing a game

Player 1

CreateContract(SHA1 + SHA2)

SHA1 + SHA2

Player 2

Winner

PROGRAMMING, ZBGURESHPXRE

DO YOU SPEAK IT?

TOPCONF TALLIN

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
S. Adams
© 1995 United Feature Syndicate, Inc.(NYC)

KSI Blockchain

e-Law

e-Court

e-Police

ksi blockchain

KSI is a blockchain technology designed in Estonia and used globally to make sure networks, systems and data are free of compromise, all while retaining 100% data privacy.

The world reported on Estonia launching a national cryptocurrency — but it turned out to be fake news

Jill Bederoff, Business Insider Nordic

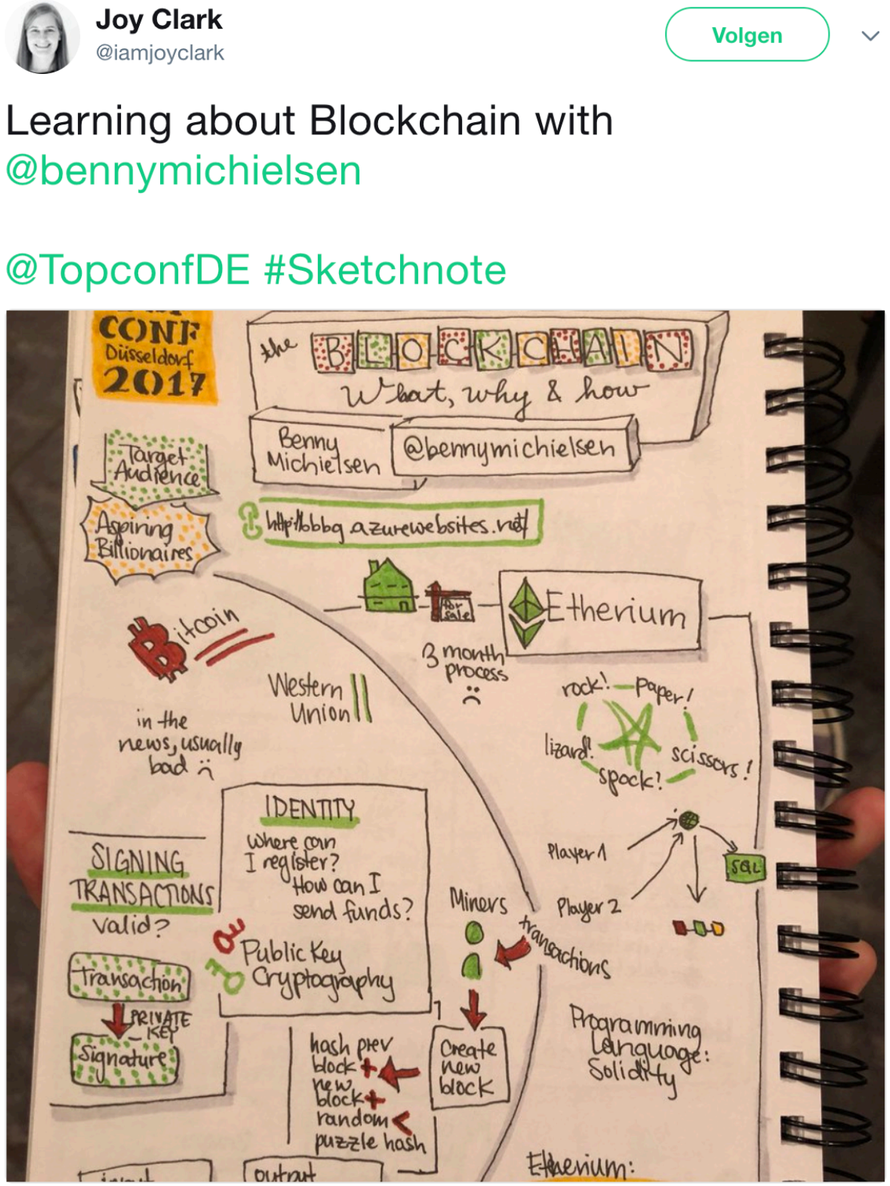
Benny Michielsen

@bennymichielsen

blog.bennymichielsen.be

bennym@infosupport.com

https://youtu.be/_dlKELBYgrw

https://github.com/BennyM/bigbangblockchaingame

TOPCONF TALLINN