The blockchain: what, why, and how

Target audience: aspiring billionaires

Benny Michielsen
Hans Peeters

Solid Innovator

Benny Michielsen

bennym@infosupport.com
@bennymichielsen

Less talk more code
Programming, Zbgureshpxre

Hans Peeters

hansp@infosupport.com
@hspeeters

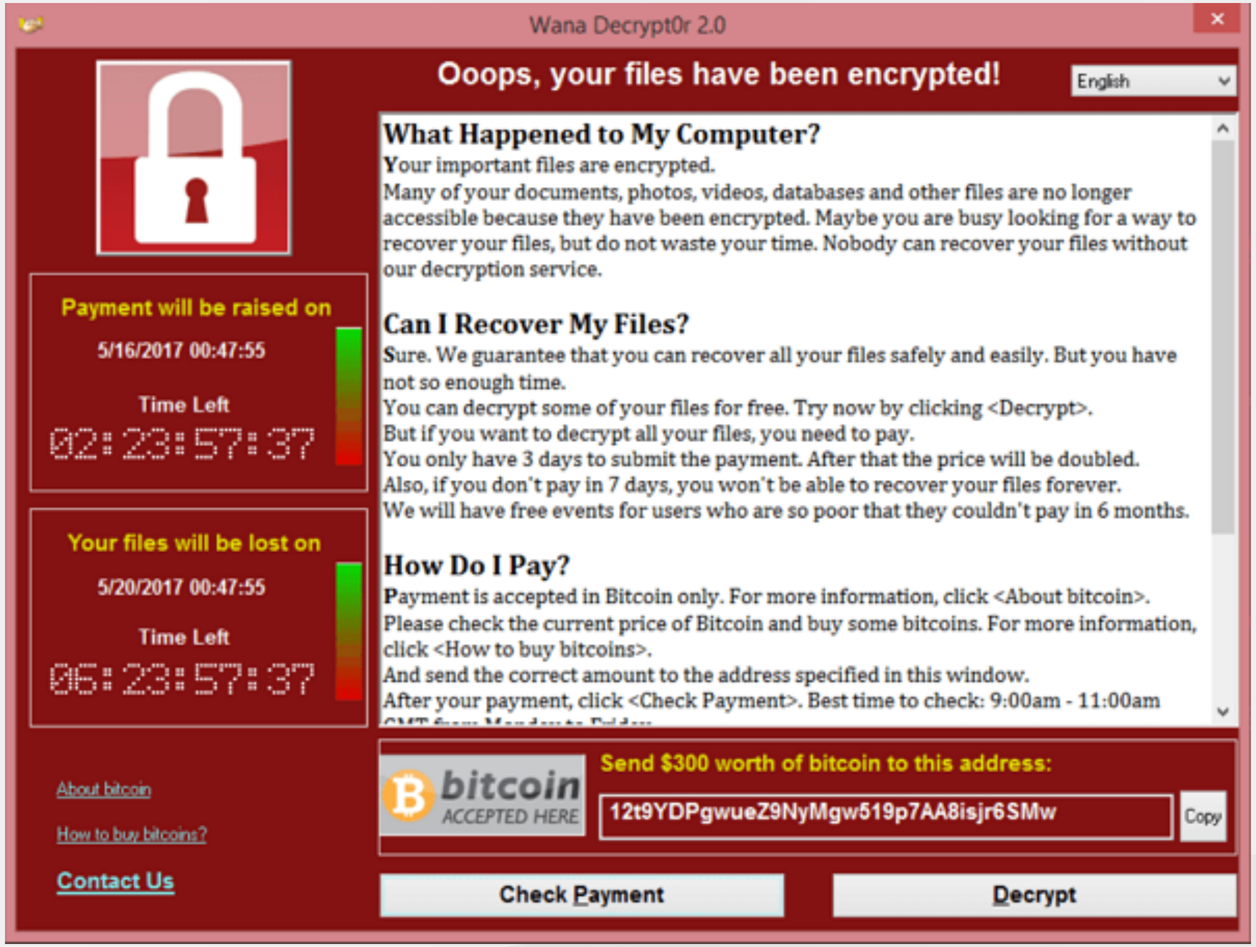
Lean
Mean

- Identity
- Integrity
- Transactions
- Miners

Bitcoin

- DApp architecture
- Smart contracts
- JS & .NET

Ethereum



Ooops, your files have been encrypted!

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

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?

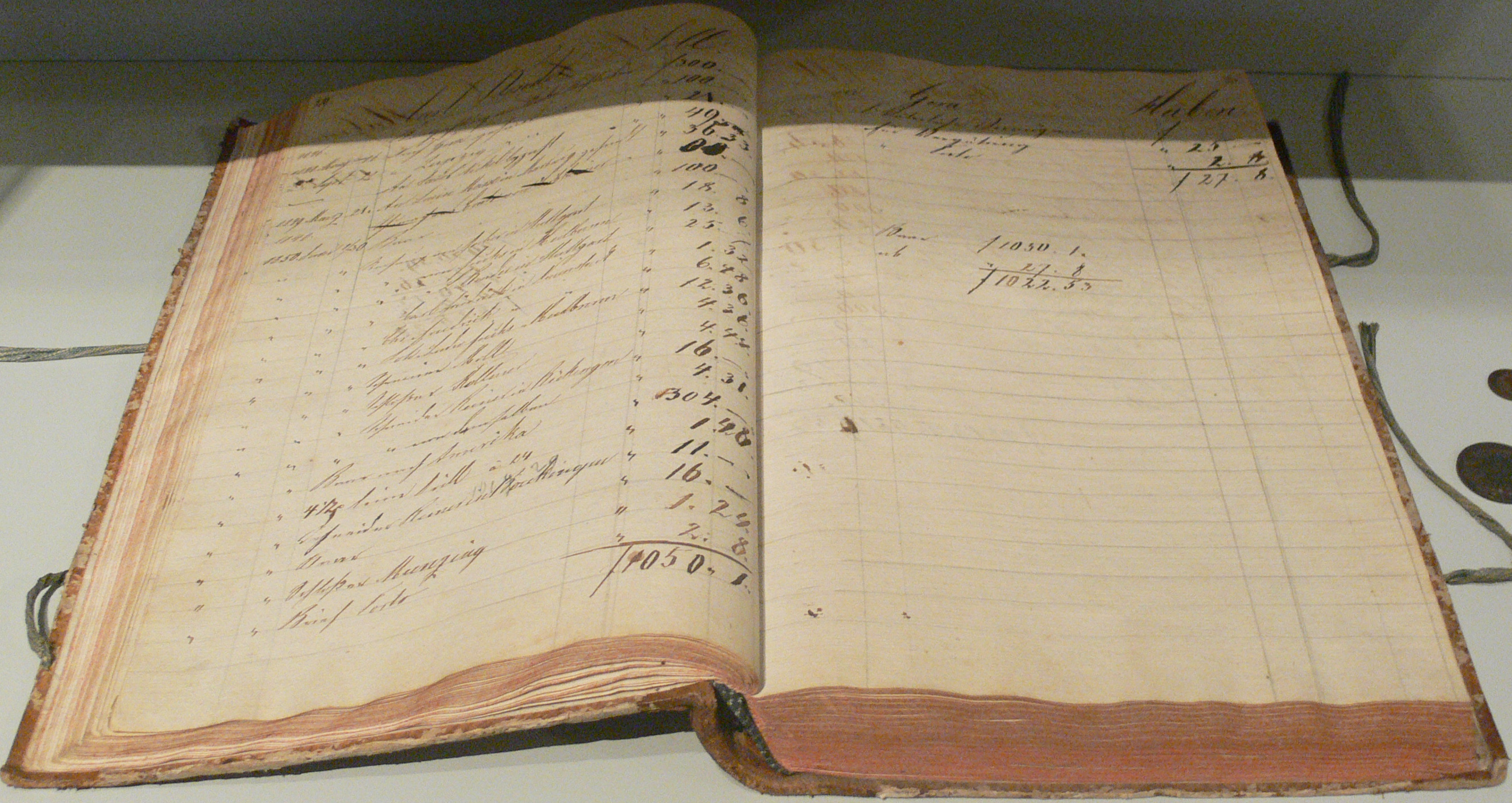
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WESTERN
UNION
®

PRICE LOCATION
barcode
details
PRICE
Ticketech.
RESERVATION
BARCODE + RECEIPT
RECEIPT (PRINTED)
RECEIPT
BARCODE
INTERPRET BARCODE
?
RESERVATION
?
TIME - STAMP.
- RESERVATION STATUS UPDATE
ENTER PARK.
VALID
INVALID
?
ENTRY
EXIT.
RECEIPT ?
BARCODE
INTERPRET BARCODE
RESERVATION



[illegible]	100.
[illegible]	100.
[illegible]	21.
[illegible]	49.
[illegible]	36.33
[illegible]	00.
[illegible]	100.
[illegible]	18.
[illegible]	13. 8
[illegible]	25. 6
[illegible]	1.37
[illegible]	6.48
[illegible]	12.36
[illegible]	4.28
[illegible]	4.42
[illegible]	16.—
[illegible]	4.31
[illegible]	1304.—
[illegible]	1.48
Baar nach Amerika	11.—
4½ [illegible] à 24	16.—
[illegible]	1.24
Baar	2.8
	f 1050.1

[illegible]	25.—
Saldo	2.8
	f 27.8

Baar	f 1030.1.
ab	27.8
	f 1022.53

Identify

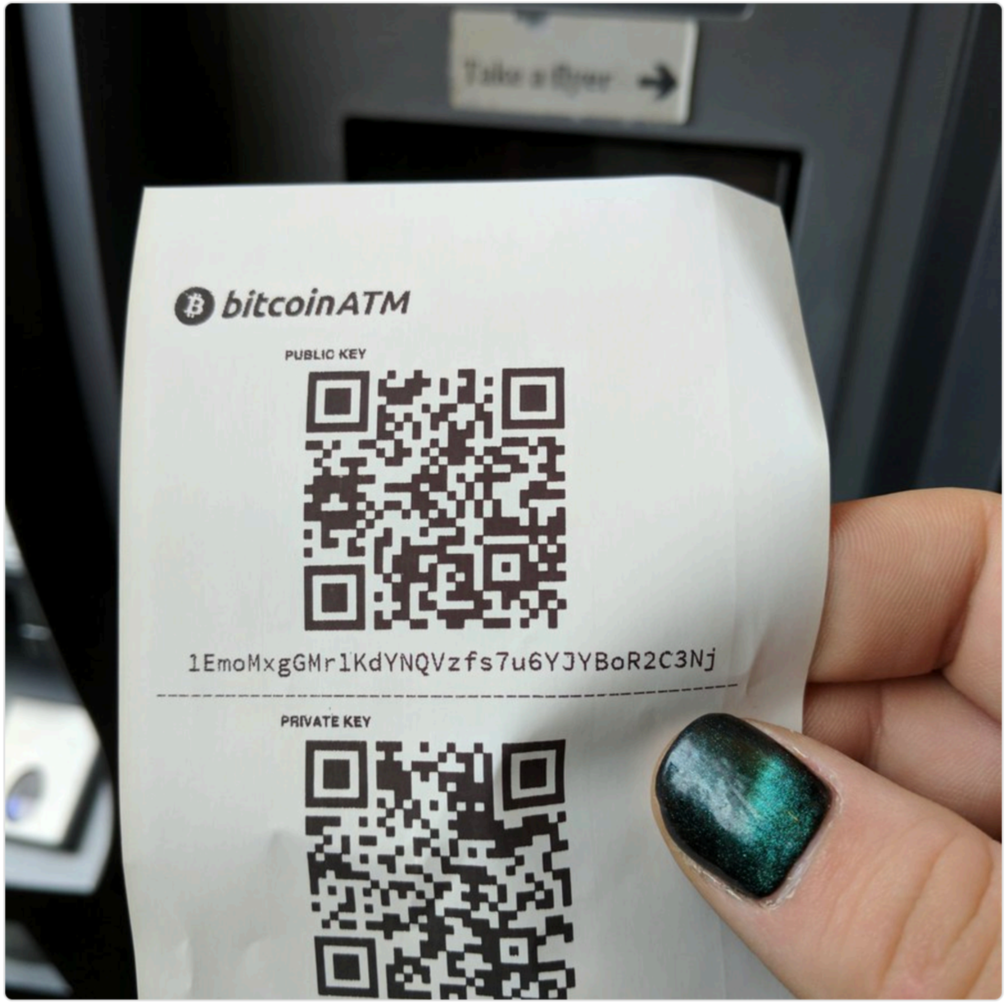
- Where do I need to register?
- Where can I send funds to?

- 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}

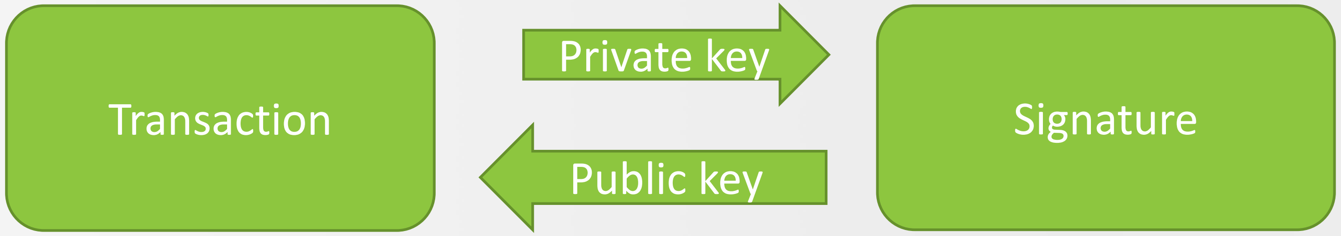
- Important to keep your private key safe!

I bought some Bitcoin at an atm 😃



Signing Transactions

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



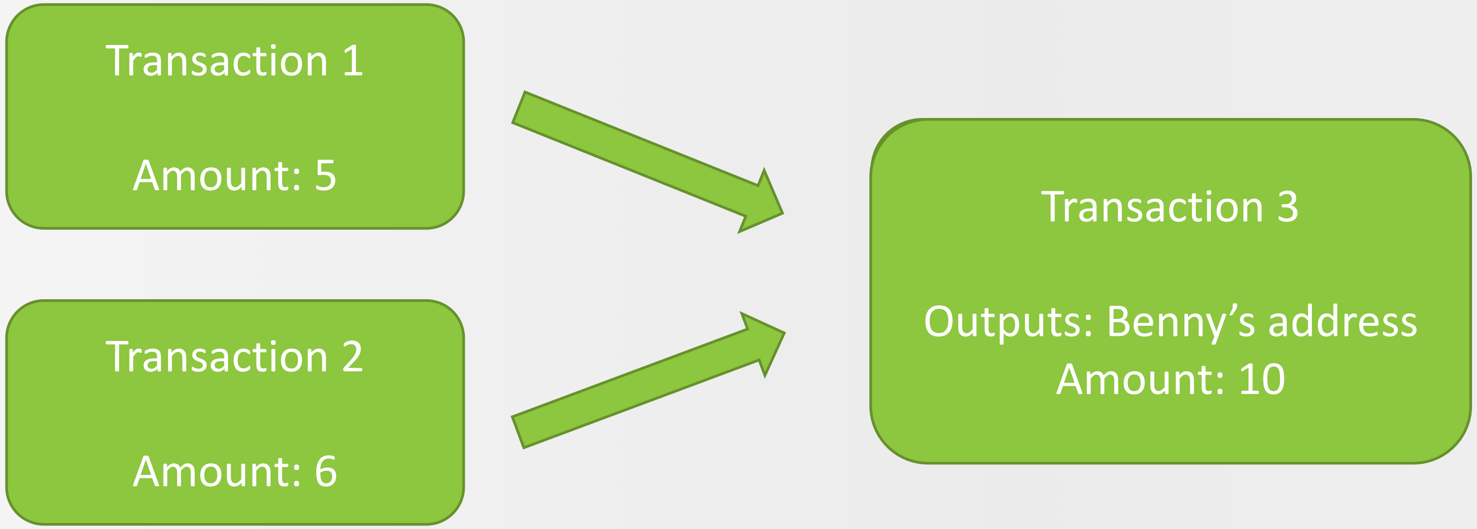
Transactions

Transactions

Transaction 3

Outputs: Benny’s address
Amount: 10

Transactions



Transaction 1

Amount: 5

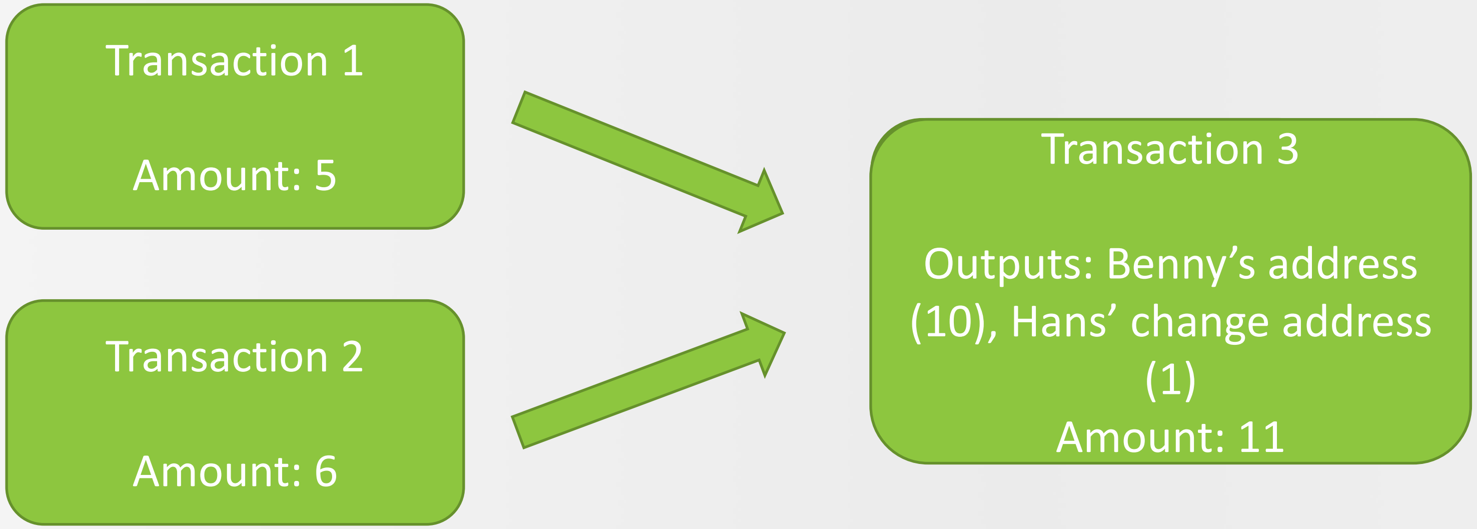
Transaction 2

Amount: 6

Transaction 3

Outputs: Benny’s address
Amount: 10

Transactions



Transaction 1

Amount: 5

Transaction 2

Amount: 6

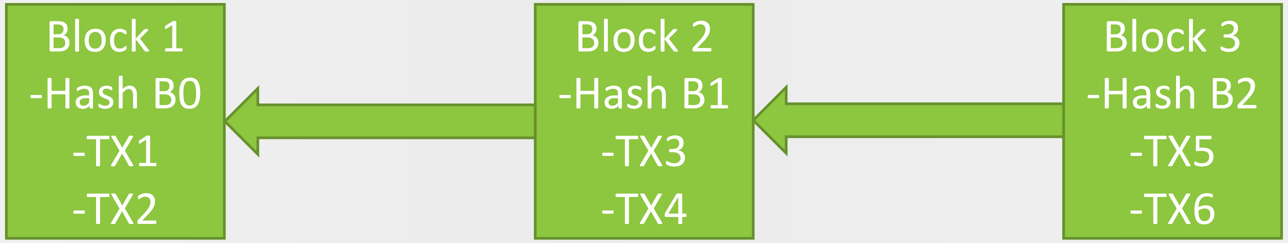
Transaction 3

Outputs: Benny’s address (10), Hans’ change address (1)
Amount: 11

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

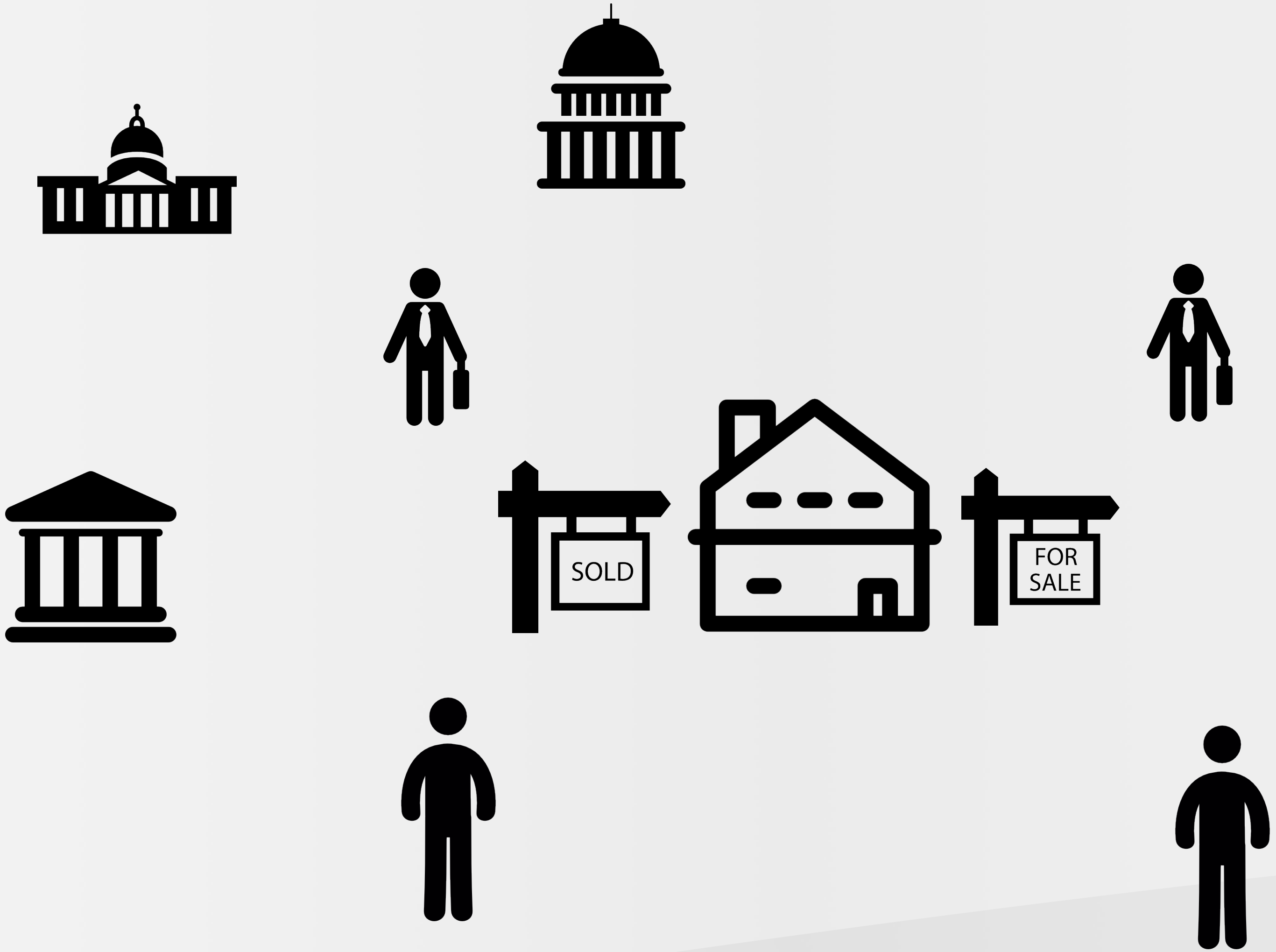
- Data can not be tampered with
- Hashing previous block makes the network secure

Trust(less)

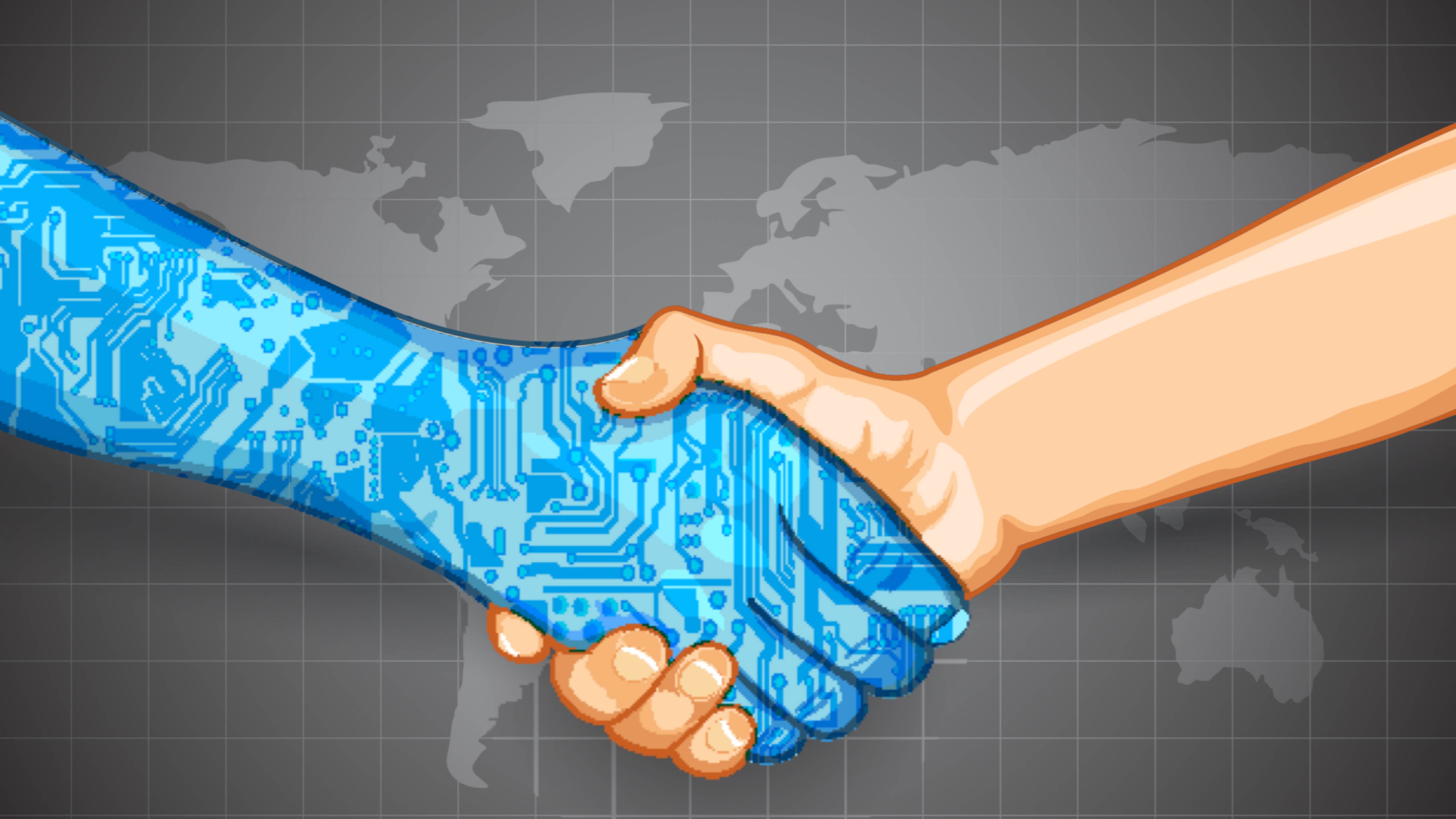
- Miners keep track of transactions
- Signatures and hashes provide integrity

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



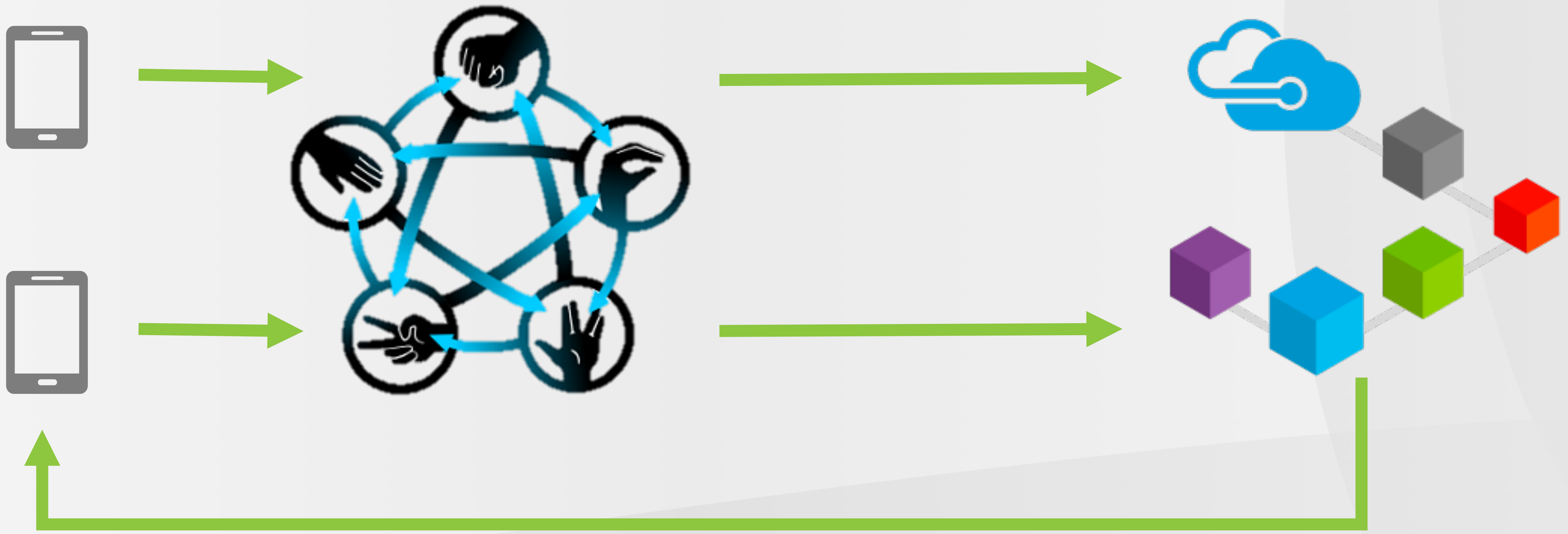
Ethereum

- Bitcoin has limited possibilities to program against

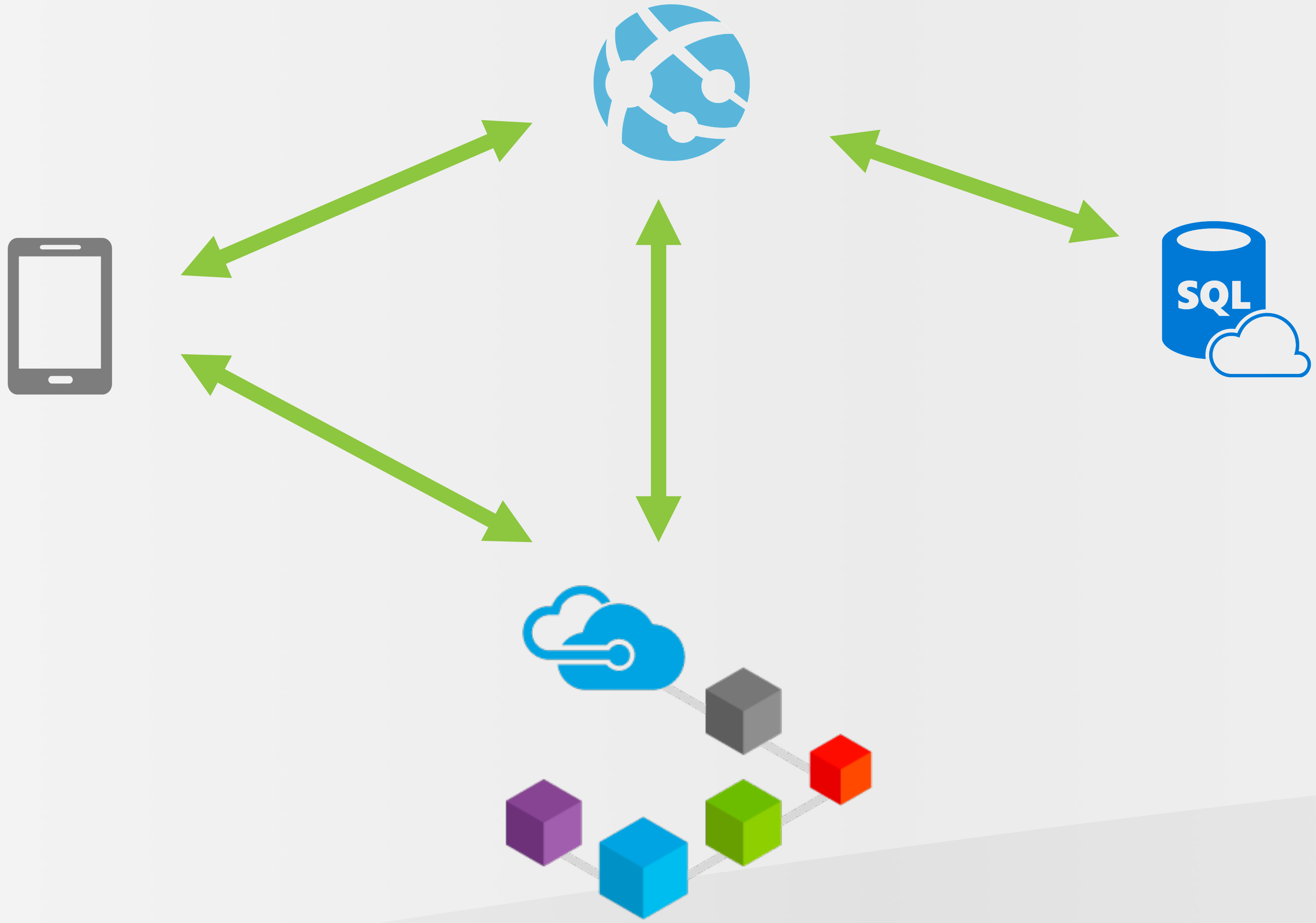
- Ethereum blockchain
  - Programmable by design
  - Distributed “computer”
  - Develop smart contracts/dapps
  - Most popular development blockchain

- 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 sending ether to that address

Game

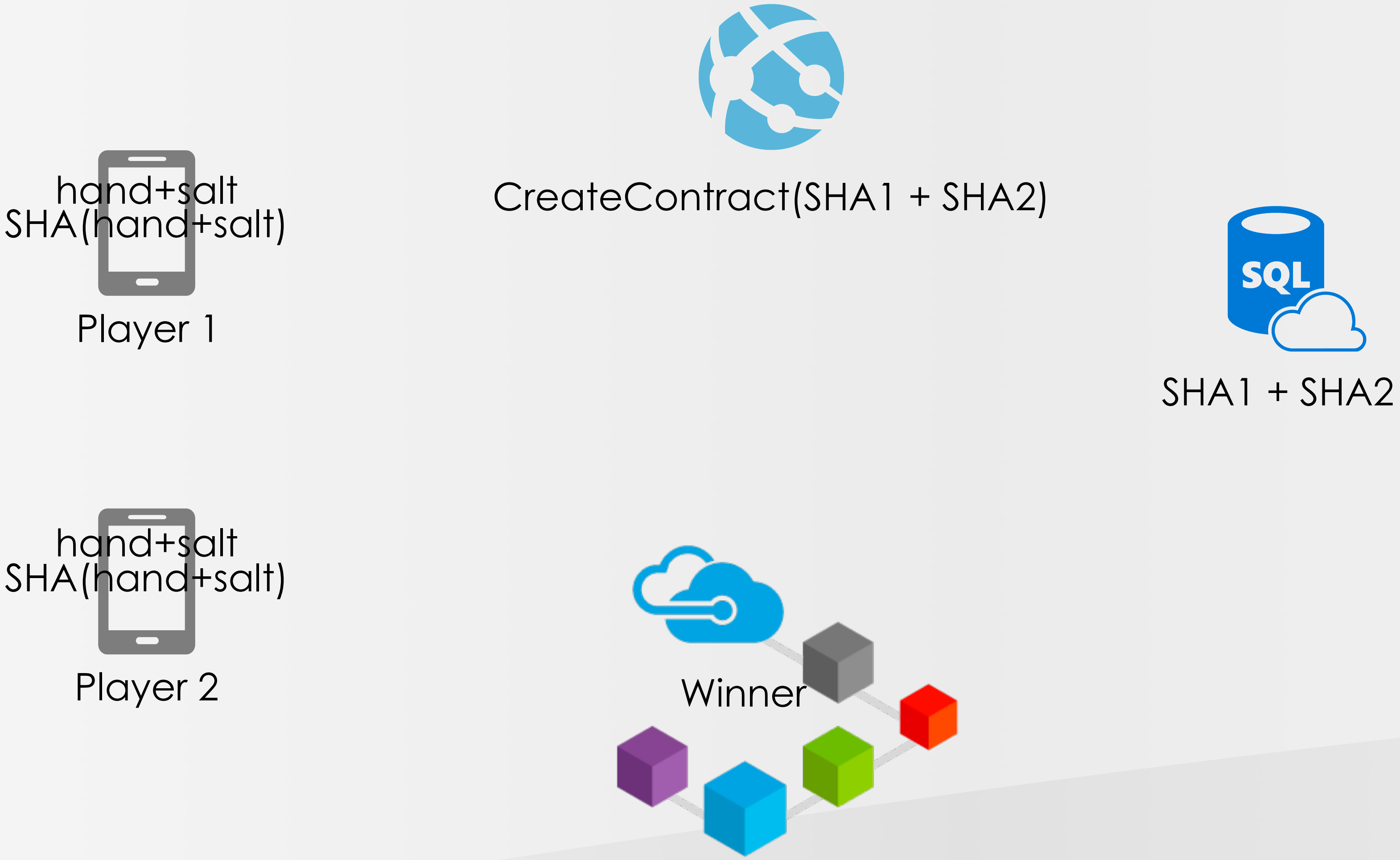


Demo


SQL

.NET
Core
TRUFFLE
HTML
5

Flow



hand+salt
SHA(hand+salt)

Player 1

CreateContract(SHA1 + SHA2)

SHA1 + SHA2

hand+salt
SHA(hand+salt)

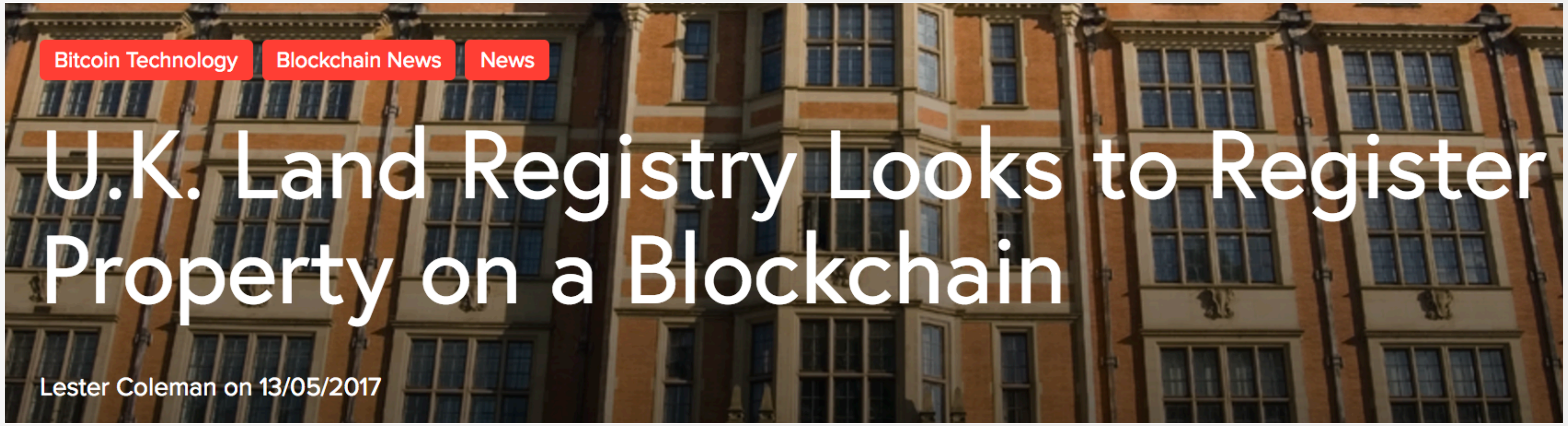
Player 2

Winner

Lessons learned

- Trust
  - Speed
  - Cost
- Cutting edge
- Potential

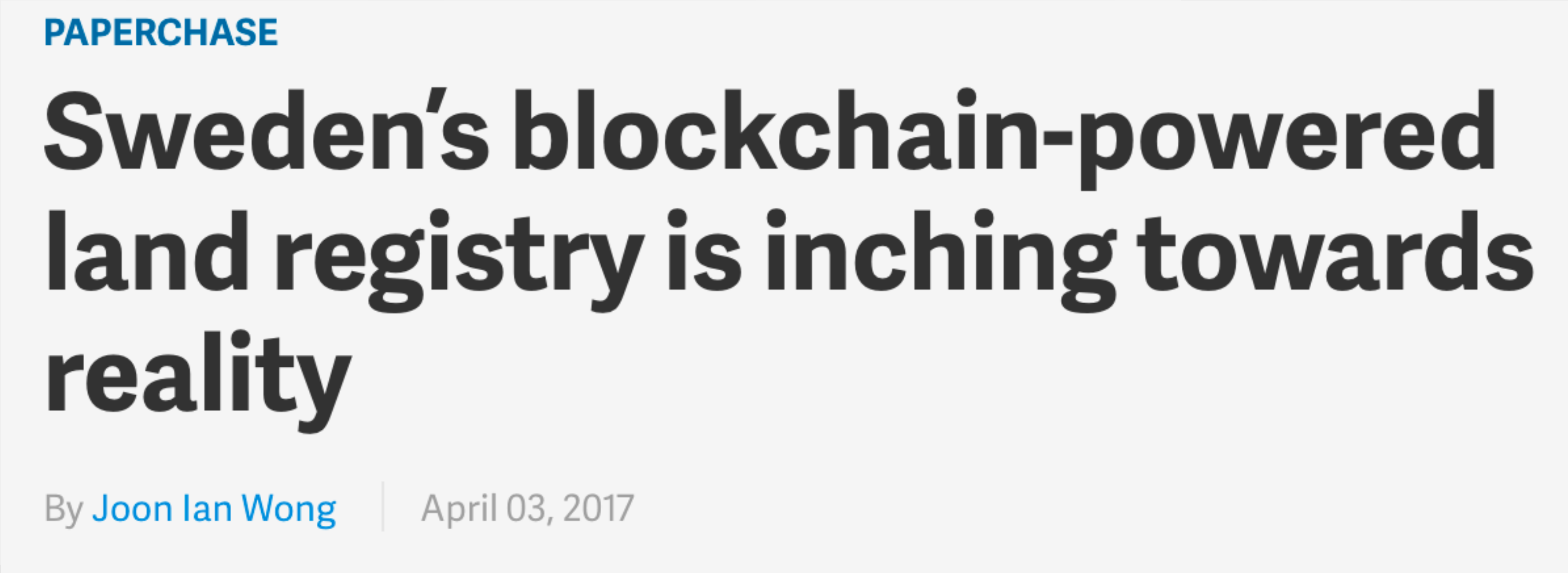
I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
E-mail: SCOTTADAMS@AOL.COM
S. Adams
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.



Bitcoin Technology | Blockchain News | News

U.K. Land Registry Looks to Register Property on a Blockchain

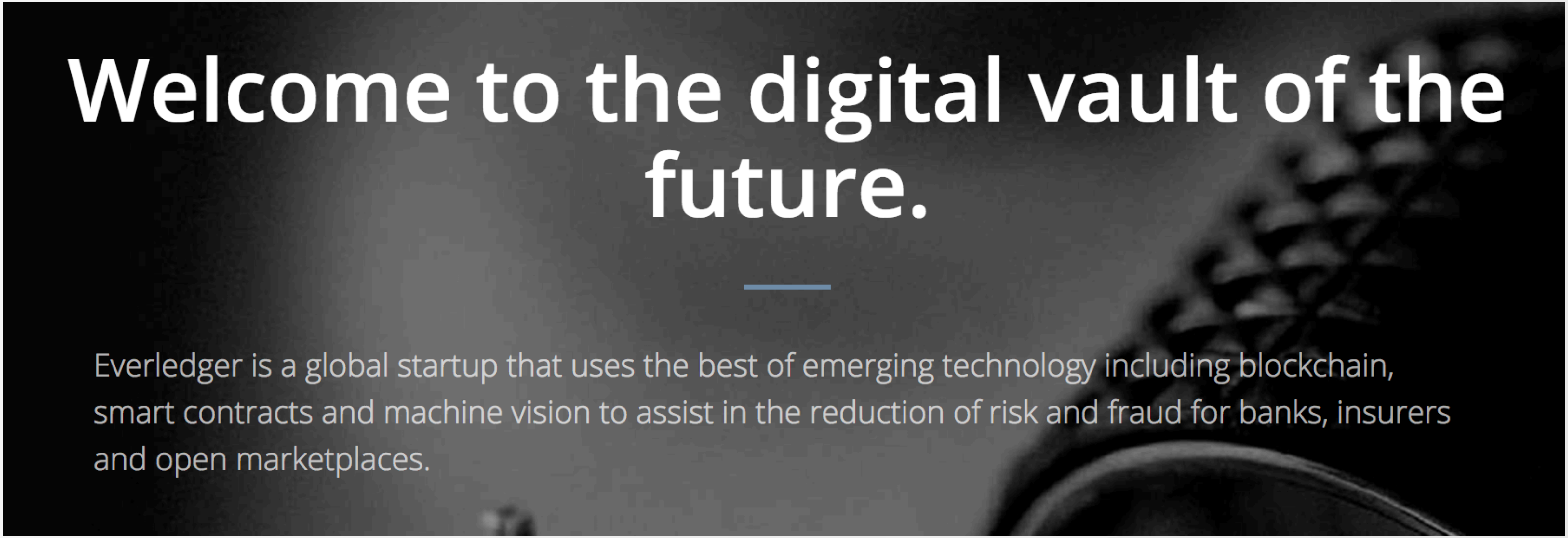
Lester Coleman on 13/05/2017



PAPERCHASE

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

By Joon Ian Wong | April 03, 2017



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
@bennymichielsen
bennym@infosupport.com

Hans Peeters
@hspeeters
hansp@infosupport.com

http://bbbg.azurewebsites.net

https://github.com/BennyM/bigbangblockchaingame