BLOCKCHAINS IN THE PHYSICAL WORLD

CARS, WINE AND HORSEMEAT

Dr. Reuben Binns, Department of Computer Science, University of Oxford, UK.

reubenbinns.com

r@reubenbinns.com

Twitter: @RDBinns

OVERVIEW

- What is a blockchain?
- What are they good for?
- Do they have useful applications in the physical world?

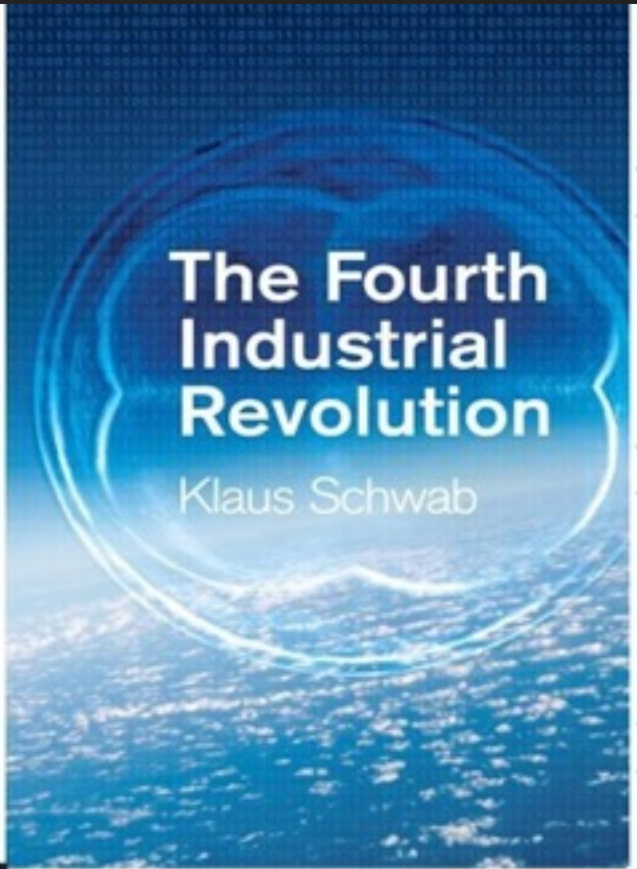
WHY IS EVERYONE SO EXCITED?

O'REILLY

Blockchain

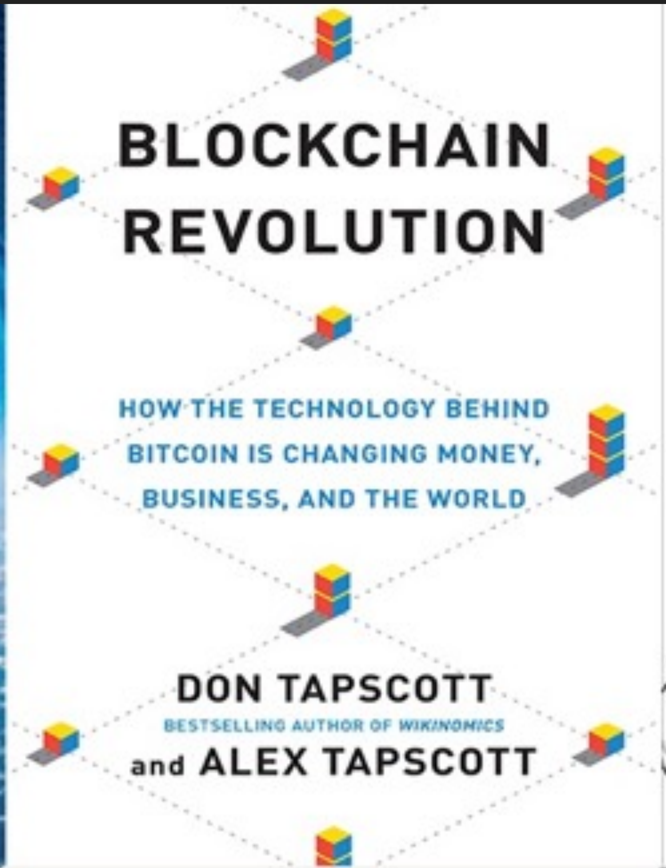
BLUEPRINT FOR A NEW ECONOMY

Melanie Swan



The Fourth Industrial Revolution

Klaus Schwab



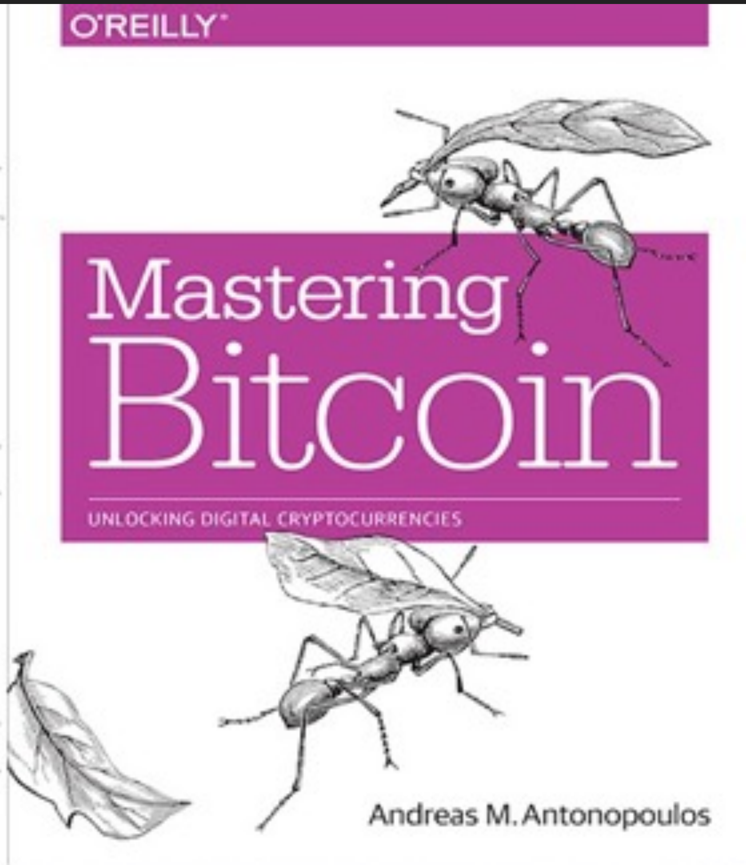
BLOCKCHAIN REVOLUTION

HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD

DON TAPSCOTT

BESTSELLING AUTHOR OF *WIKINOMICS*

and ALEX TAPSCOTT



O'REILLY

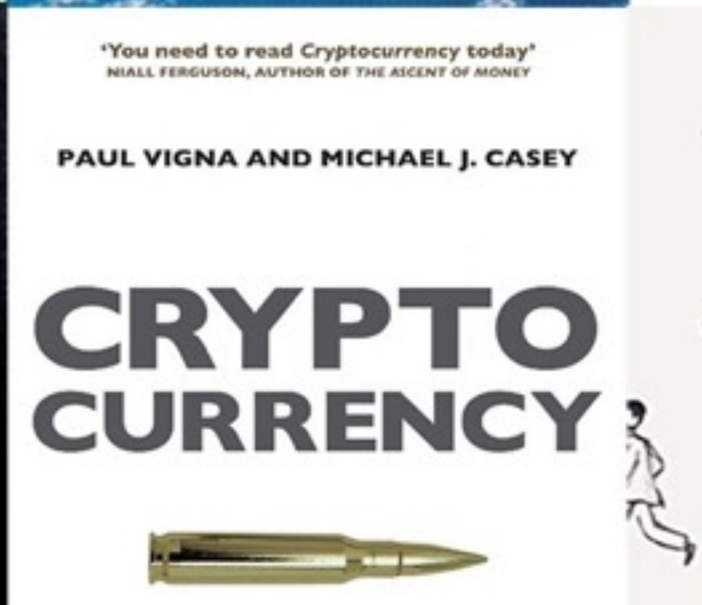
Mastering Bitcoin

UNLOCKING DIGITAL CRYPTOCURRENCIES

Andreas M. Antonopoulos

VALUE WEB

How FinTech firms are using mobile and blockchain technologies to create the Internet of Value



'You need to read *Cryptocurrency* today'

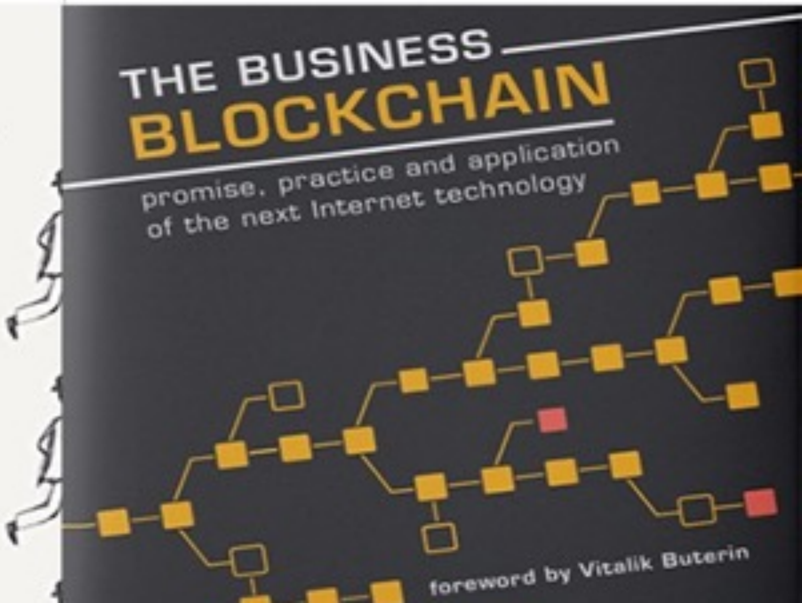
NIALL FERGUSON, AUTHOR OF *THE ASCENT OF MONEY*

PAUL VIGNA AND MICHAEL J. CASEY

CRYPTO CURRENCY

BYE BYE BANKS?

How retail banks are being displaced, diminished and disintermediated by tech startups – and what they can do to survive.



THE BUSINESS BLOCKCHAIN

promise, practice and application of the next Internet technology

foreword by Vitalik Buterin

Government
Office for Science

Distributed Ledger Technology:
beyond block chain

A report by the UK Government Chief Scientific Adviser

‘THESE TECHNOLOGIES [MAY] REFORM OUR FINANCIAL MARKETS, SUPPLY CHAINS, CONSUMER AND B2B SERVICES’

UK Government Chief Scientific Advisor

WHAT ISN’T A BLOCKCHAIN?

> “EVERYTHING'S A ****ING BLOCKCHAIN”

David Birch

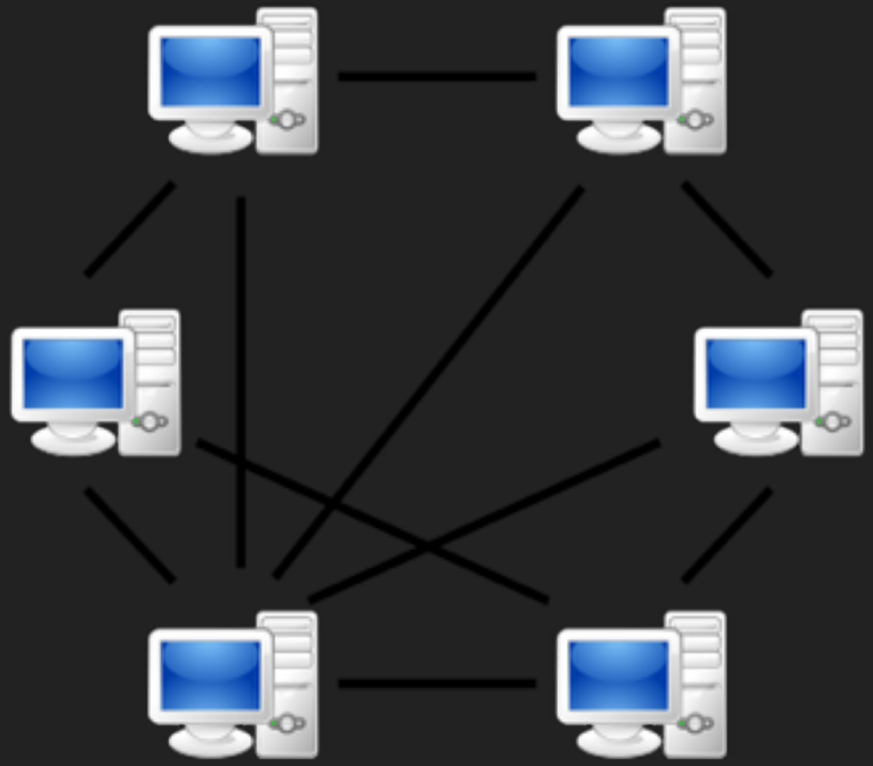
http://www.slideshare.net/15Mb/everythings-a-ing-blockchain

THE BITCOIN BLOCKCHAIN?

- First proposed as part of the bitcoin protocol
- Invented by ‘Satoshi Nakamoto’
- Builds on other technologies:
  - Peer-to-peer network
  - Cryptographic hash functions
  - Asymmetric key cryptography

P2P, DISTRIBUTED, DECENTRALISED SYSTEMS

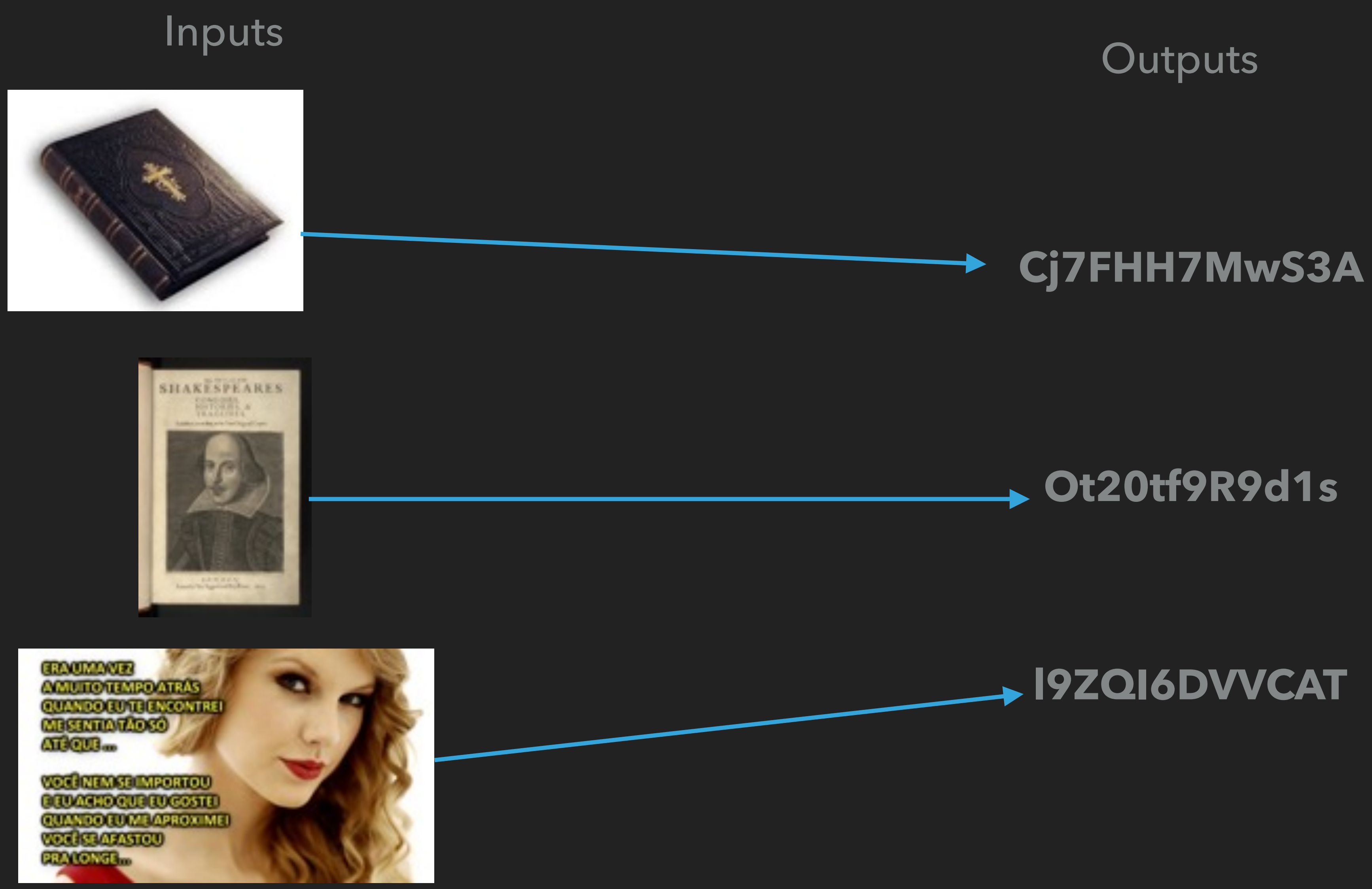
- Anyone is allowed to run a node
- All nodes follow the same protocol
- All nodes are equal
- Examples: file-sharing, the internet, the web



CRYPTOGRAPHIC HASH FUNCTION

- Cryptographic hash function:
  - input (any size), efficiently computes a particular output (fixed size)
  - Input can’t be guessed from output
  - Can’t find two distinct inputs with same output
  - All outputs are equally likely

CRYPTOGRAPHIC HASH FUNCTION



Inputs

Outputs

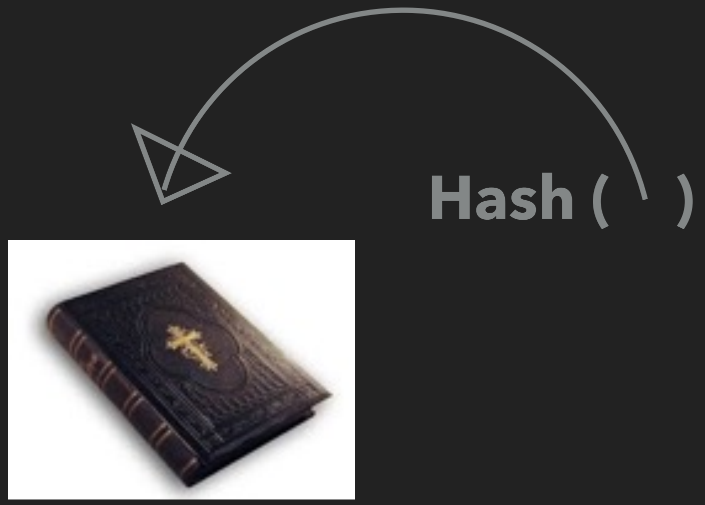
Cj7FHH7MwS3A

Ot20tf9R9d1s

I9ZQI6DVVCAT

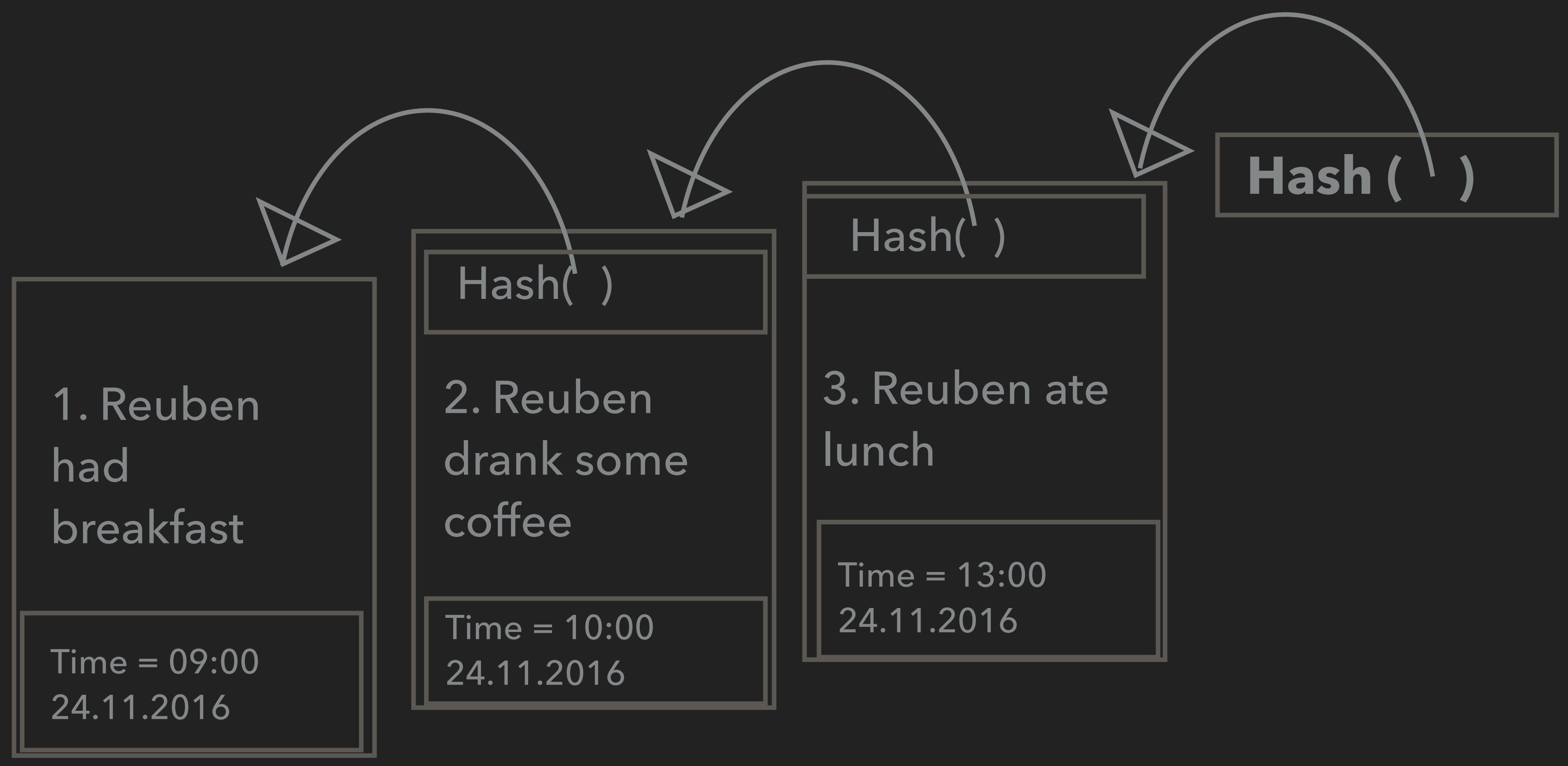
HASH POINTERS

- Point to some data, and a hash of it



Hash ( )

HASH POINTER DATA STRUCTURES



Hash (   )

1. Reuben had breakfast

Time = 09:00 24.11.2016

Hash(   )

2. Reuben drank some coffee

Time = 10:00 24.11.2016

Hash(   )

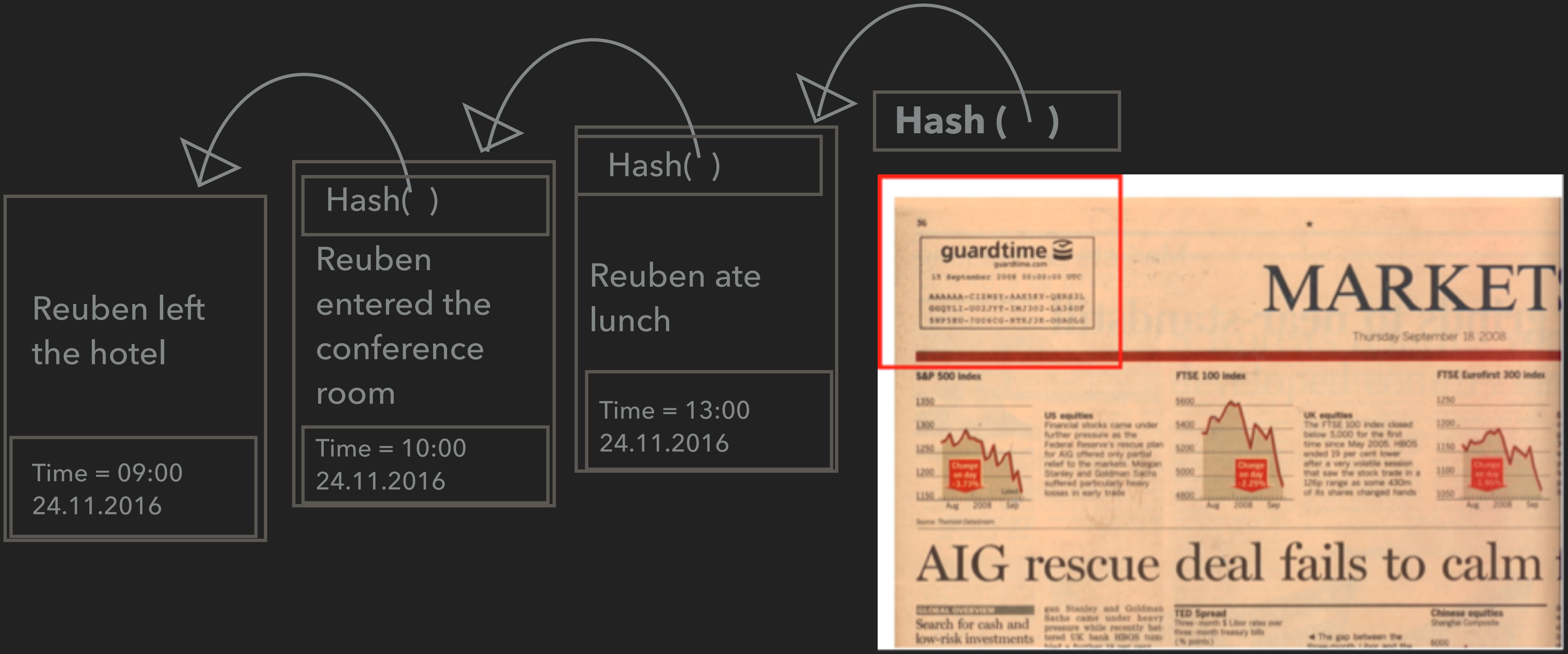
3. Reuben ate lunch

Time = 13:00 24.11.2016

Hash (   )

HASH POINTER DATA STRUCTURES

- Hashes can be published in multiple public places (e.g. GuardTime)



Reuben left the hotel

Time = 09:00 24.11.2016

Hash( )

Reuben entered the conference room

Time = 10:00 24.11.2016

Hash( )

Reuben ate lunch

Time = 13:00 24.11.2016

Hash ( )

36

guardtime
guardtime.com
15 September 2008 00:00:00 UTC
AAAAAA-CIIWSY-AAKSKY-QRR63L
GGQYLI-UO2JYT-IMJ302-LA340F
SHPSEU-7O06CG-RTRJ3R-OOAOLG

MARKETS

Thursday September 18 2008

S&P 500 index

Source: Thomson Datastream

US equities
Financial stocks came under further pressure as the Federal Reserve's rescue plan for AIG offered only partial relief to the markets. Morgan Stanley and Goldman Sachs suffered particularly heavy losses in early trade

FTSE 100 index

UK equities
The FTSE 100 index closed below 5,000 for the first time since May 2005. HBOS ended 19 per cent lower after a very volatile session that saw the stock trade in a 126p range as some 430m of its shares changed hands

FTSE Eurofirst 300 index

AIG rescue deal fails to calm

GLOBAL OVERVIEW
Search for cash and low-risk investments

gan Stanley and Goldman Sachs came under heavy pressure while recently battered UK bank HBOS tumbled a further 19 per cent

TED Spread
Three-month $ Libor rates over three-month treasury bills (% points)

◄ The gap between the three-month Libor and the

Chinese equities
Shanghai Composite

Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." Conference on the Theory and Application of Cryptography. Springer Berlin Heidelberg, 1990. https://www.anf.es/pdf/Haber_Stornetta.pdf

DIGITAL SIGNATURES

- Only you can make your signature
- Anyone who looks at it can see it is valid
- Each signature is only valid for the document it signs

28

VISAS

10 PIASTRES 10
SUDAN POSTAGE
S.G.

SUDAN GOVERNMENT
Passports & Permits
Sudan Agency, Cairo
Visa No. 2936 27-12-44
Valid for single entry into
the Sudan,
SUDAN AGENT.

Valid for departure within
-30- days from date of
issue.

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

DIGITAL SIGNATURE SCHEME

- Generate a secret key and a public key
- Your secret key allows you to put your signature on a document
- Anyone can verify the signature on a document belongs to you, using your public key

© CEphoto, Uwe Aranas

Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22.6 (1976): 644-654.

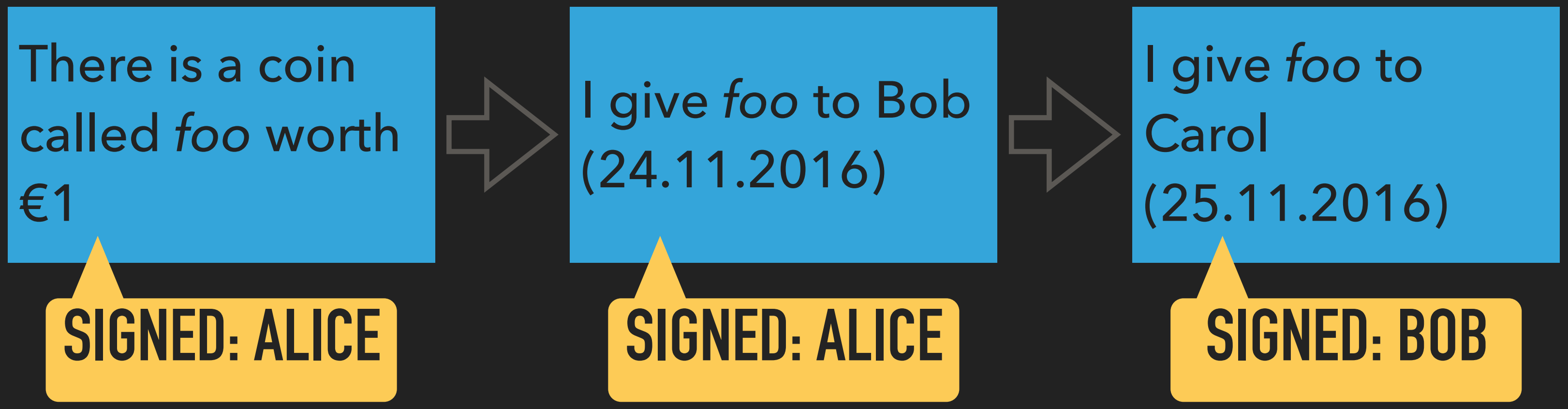
HOW TO BUILD A DECENTRALISED DIGITAL CURRENCY

- The blockchain relies on P2P, hash functions and PKI to create a secure decentralised digital currency

DIGITAL CURRENCY

- Cash is a promise with a signature from someone we trust

DIGITAL CURRENCY



There is a coin called *foo* worth €1

SIGNED: ALICE

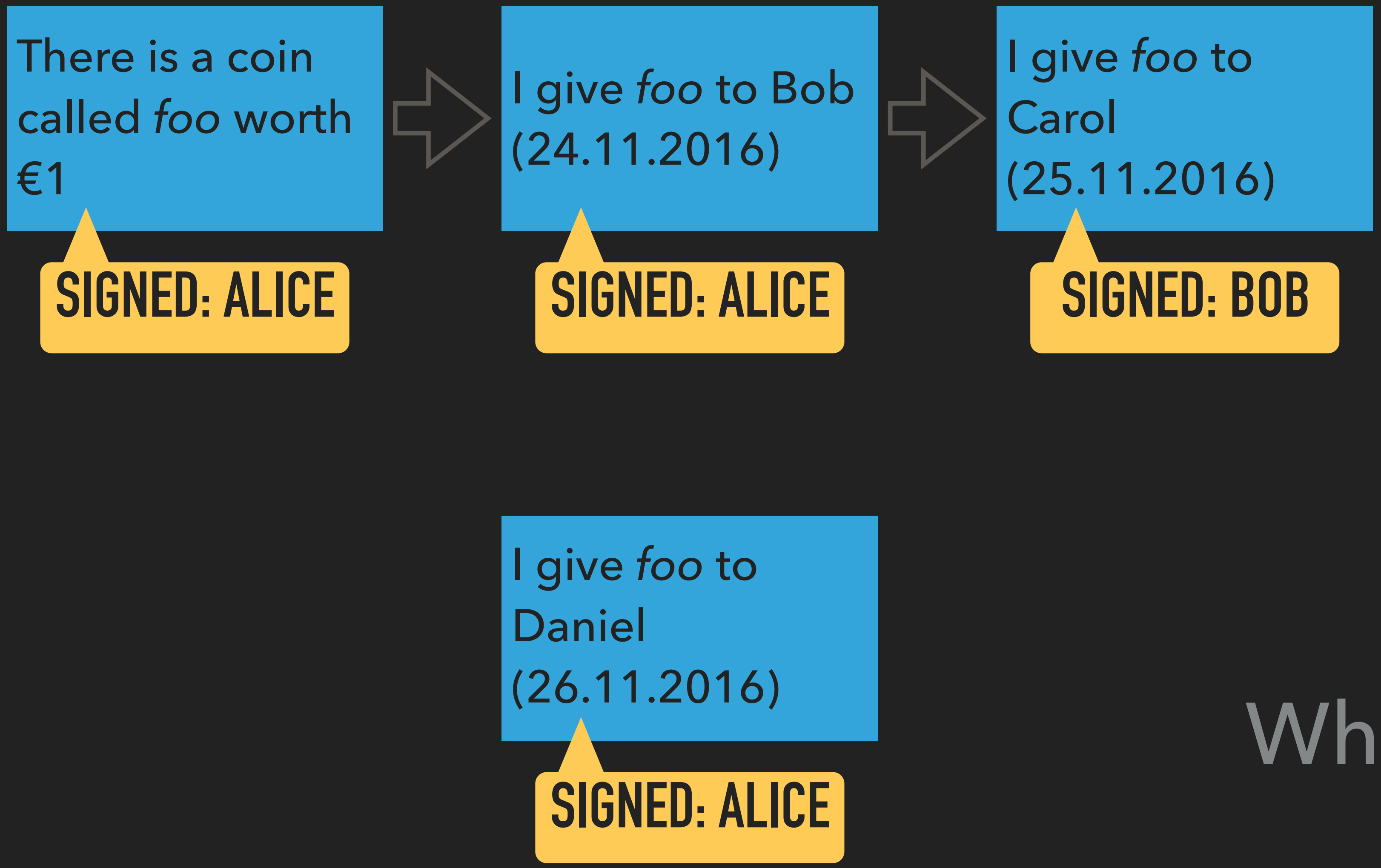
I give *foo* to Bob (24.11.2016)

SIGNED: ALICE

I give *foo* to Carol (25.11.2016)

SIGNED: BOB

DIGITAL CURRENCY: DOUBLE SPEND ATTACK!



There is a coin called *foo* worth €1

SIGNED: ALICE

I give *foo* to Bob (24.11.2016)

SIGNED: ALICE

I give *foo* to Carol (25.11.2016)

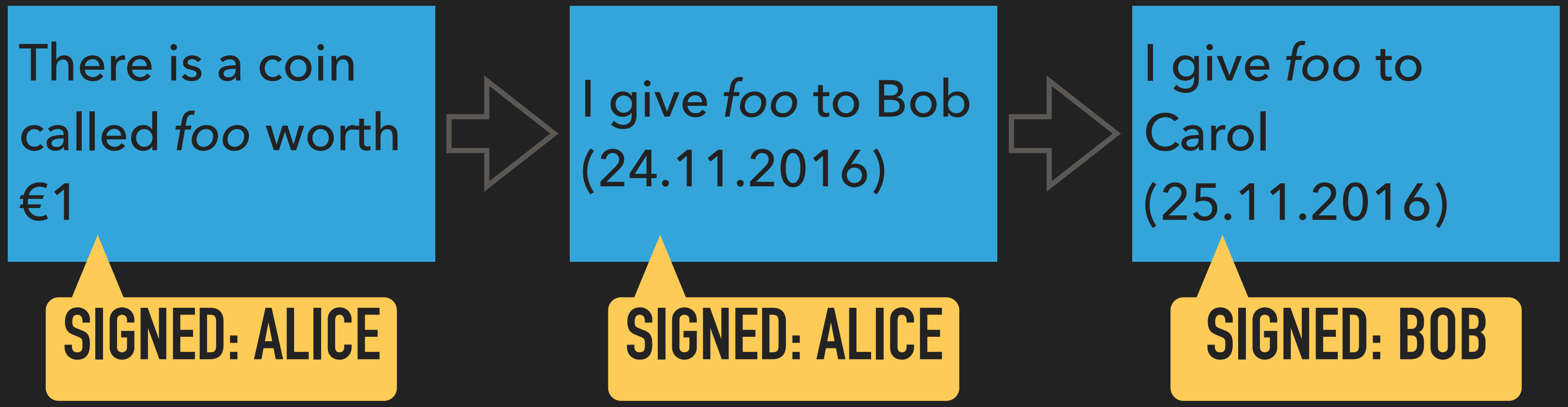
SIGNED: BOB

I give *foo* to Daniel (26.11.2016)

SIGNED: ALICE

Who owns *foo* now?

DIGITAL CURRENCY: CENTRALISED



There is a coin called *foo* worth €1

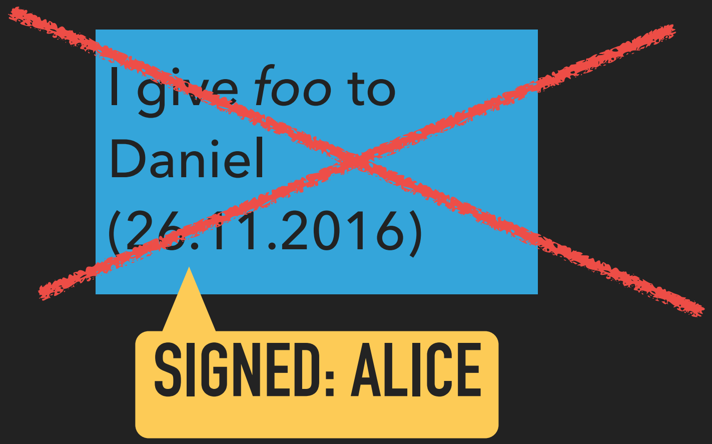
SIGNED: ALICE

I give *foo* to Bob (24.11.2016)

SIGNED: ALICE

I give *foo* to Carol (25.11.2016)

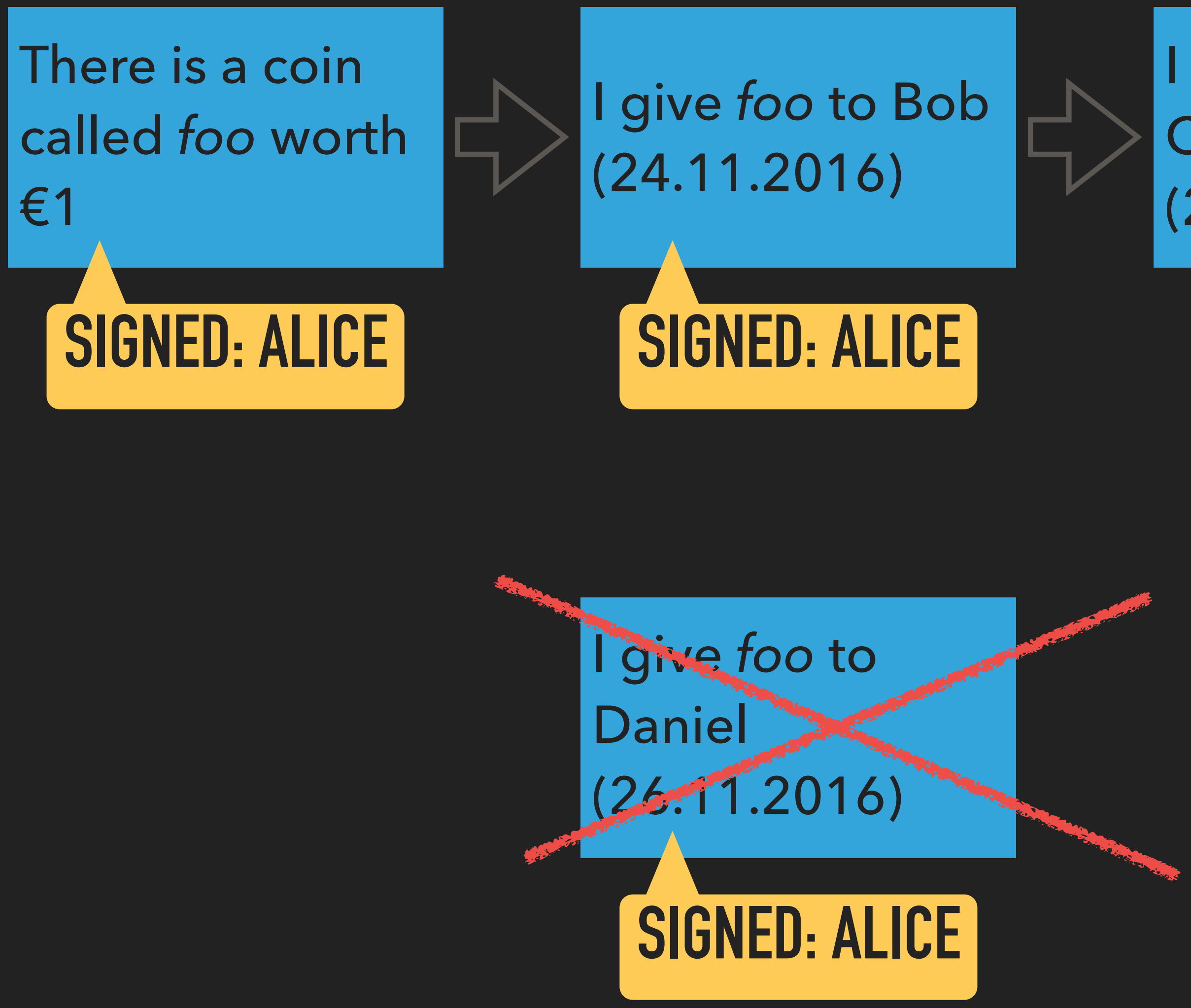
SIGNED: BOB



~~I give *foo* to Daniel (26.11.2016)~~

SIGNED: ALICE

DIGITAL CURRENCY: DECENTRALISED



There is a coin called *foo* worth €1

SIGNED: ALICE

I give *foo* to Bob (24.11.2016)

SIGNED: ALICE

I give *foo* to Carol (25.11.2016)

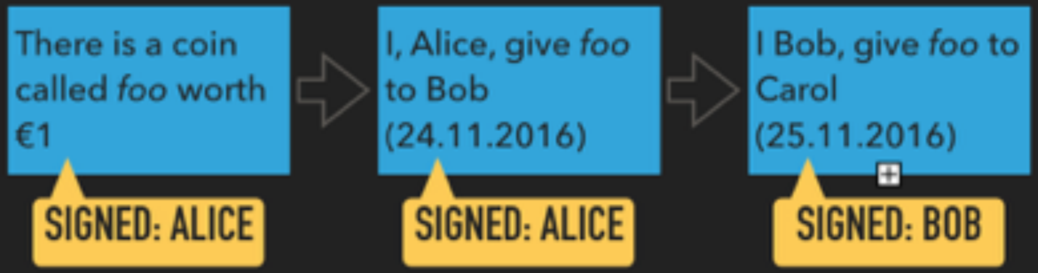
SIGNED: BOB

~~I give *foo* to Daniel (26.11.2016)~~

SIGNED: ALICE

We all agree, *foo* belongs to Carol

DIGITAL CURRENCY: DECENTRALISED SOLUTION



There is a coin called *foo* worth €1

SIGNED: ALICE

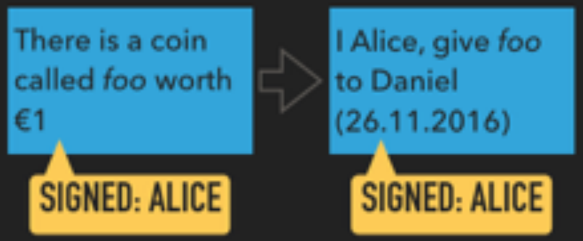
I, Alice, give *foo* to Bob (24.11.2016)

SIGNED: ALICE

I Bob, give *foo* to Carol (25.11.2016)

SIGNED: BOB

"Looks to me like *foo* belongs to Carol"



There is a coin called *foo* worth €1

SIGNED: ALICE

I Alice, give *foo* to Daniel (26.11.2016)

SIGNED: ALICE

"I disagree: *foo* belongs to Daniel"

DIGITAL CURRENCY: DECENTRALISED SOLUTION

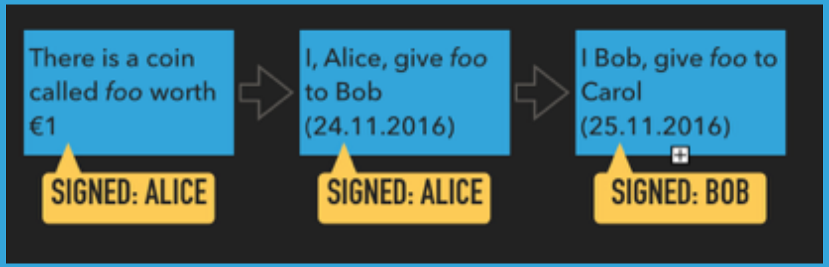
We need to settle on one version of the truth

How? Nodes *race against each other* to solve computationally expensive puzzles. The winner gets to propose their version of the truth!

Wellcome Images

DIGITAL CURRENCY: DECENTRALISED SOLUTION

"I won the race, and this is what the transactions look like to me:"



There is a coin called *foo* worth €1

SIGNED: ALICE

I, Alice, give *foo* to Bob (24.11.2016)

SIGNED: ALICE

I Bob, give *foo* to Carol (25.11.2016)

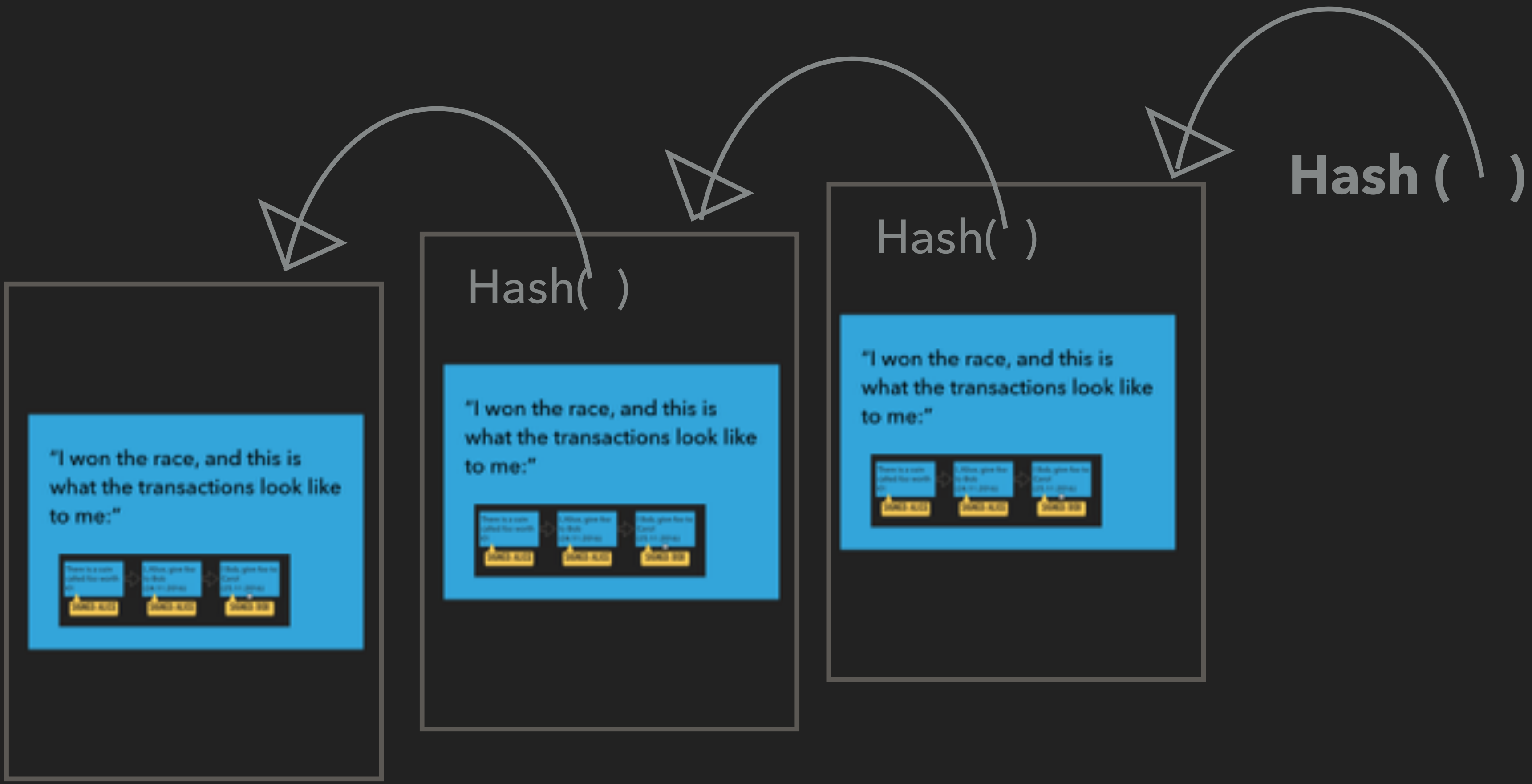
SIGNED: BOB

Wellcome Images

The winner collects together all the transaction claims in a *block* and broadcasts it to the other nodes…

DIGITAL CURRENCY: DECENTRALISED SOLUTION

If winner 2 accepts winner 1's block, they will include a hash of it in their new block. If not, they will start from the previous block.



"I won the race, and this is what the transactions look like to me:"

"I won the race, and this is what the transactions look like to me:"

"I won the race, and this is what the transactions look like to me:"

DIGITAL CURRENCY: DECENTRALISED SOLUTION

- If puzzle winners are honest, then they won’t allow double spending or accept invalid signatures
- We are assuming that winners will generally be honest.
- But what incentive does the winning node have to be honest?

MINING INCENTIVES

- Miners who win the race get to award themselves 12.5 BTC per block, automatically, and to collect fees on the transactions they process
- If their block ends up being rejected by later race-winning miners, then the version of the blockchain where they get a reward is ignored

51% ATTACK

- A majority of the miners collude with each other to allow invalid blocks
- But once discovered, faith in the currency would collapse, and BTC's gained would be worthless

Bundesarchiv, Bild 183-R1215-506
Foto: o.Ang. | Oktober 1923

OTHER USES

- We’ve seen how the blockchain solves a core security challenge of decentralised digital currencies. It can also:
- *Set rules*: What code will be executed
- *Provenance*: tell us where a coin came from

SETTING RULES WITH SMART CONTRACTS

- A way for untrusting parties to agree on what code will run
- Bitcoin transactions are simple agreements:
  - e.g. ‘Transfer 1BTC from Alice to Bob’
  - Escrow - allow third-party arbitration if there is a conflict
- Once we’ve agreed, nobody can back out or change the terms, and they will be executed by the bitcoin network

SETTING RULES WITH SMART CONTRACTS

- *Ethereum* (ethereum.org) is an alternative system with a smart contract language at its core
- Betting
- Loans, stocks, shares
- Subscription
- Crowdfunding

PROVENANCE: EVERY COIN HAS A STORY TO TELL

- Every coin (or fraction of a coin) has a unique, tamper-proof history recorded in the blockchain.
- Coloured coins: let coins represent something that can be redeemed (tokens, tickets, vouchers, passes)
- This allows the coin to change hands, but it cannot be copied

PROVENANCE: EVERY COIN HAS A STORY TO TELL

- Warning: the owner of the token has to trust that the token issuer will allow him/her to redeem the thing it represents (unless it can be written in a smart contract!)

RULES AND PROVENANCE FOR THE PHYSICAL WORLD?

- Rules: how could a blockchain stop me from physically picking up property and running away with it?
- Provenance: how could a blockchain guarantee that my burger is 100% beef?
- Do we *need* a blockchain for these things?

SMART PROPERTY

- Physical property can be stolen and lost, and then used or sold illegitimately
- What if a seller disappears after taking your money, without delivering the goods?
- Control over property could be determined by the blockchain?

SMART PROPERTY

- Something which requires a computer to work
- E.g. a smart car

SMART PROPERTY

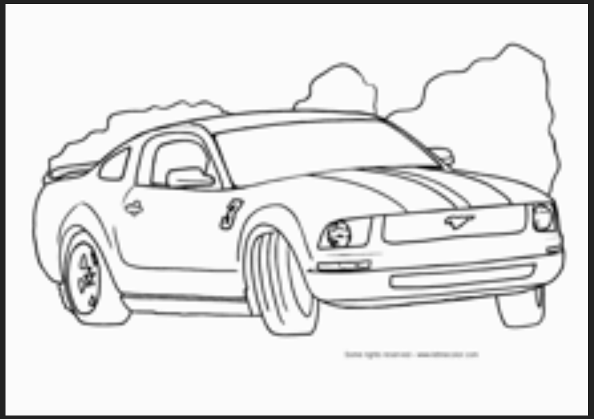
- Car won’t start without the computer
- Computer is unlocked by a key fob

SMART PROPERTY: AUTHENTICATION

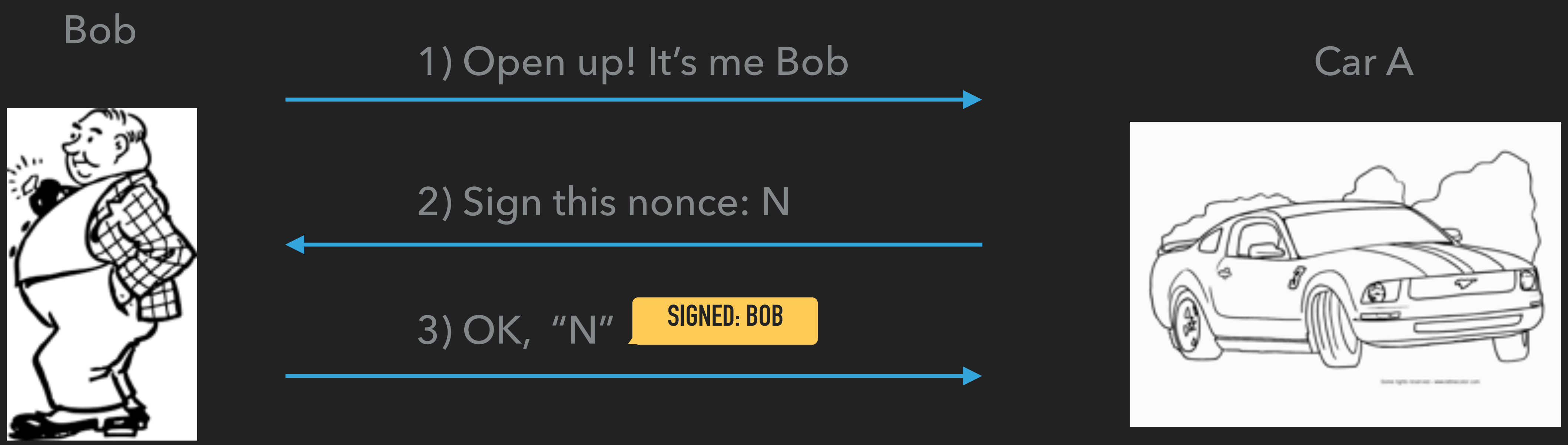
Bob

1) Open up! It's me Bob

Car A



SMART PROPERTY: AUTHENTICATION



Bob

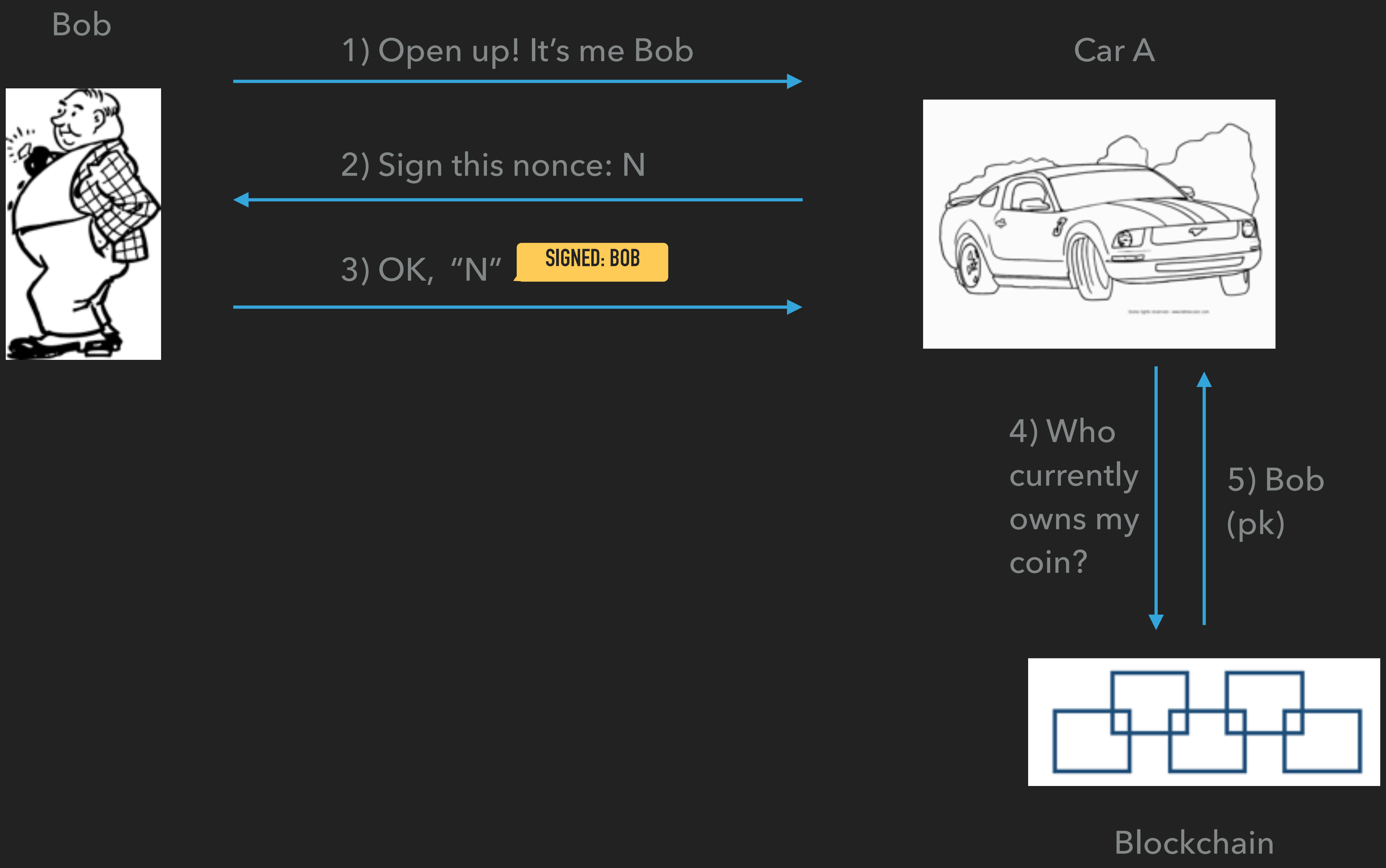
Car A

1) Open up! It's me Bob

2) Sign this nonce: N

3) OK, "N" SIGNED: BOB

SMART PROPERTY: AUTHENTICATION



Bob

1) Open up! It's me Bob

Car A

2) Sign this nonce: N

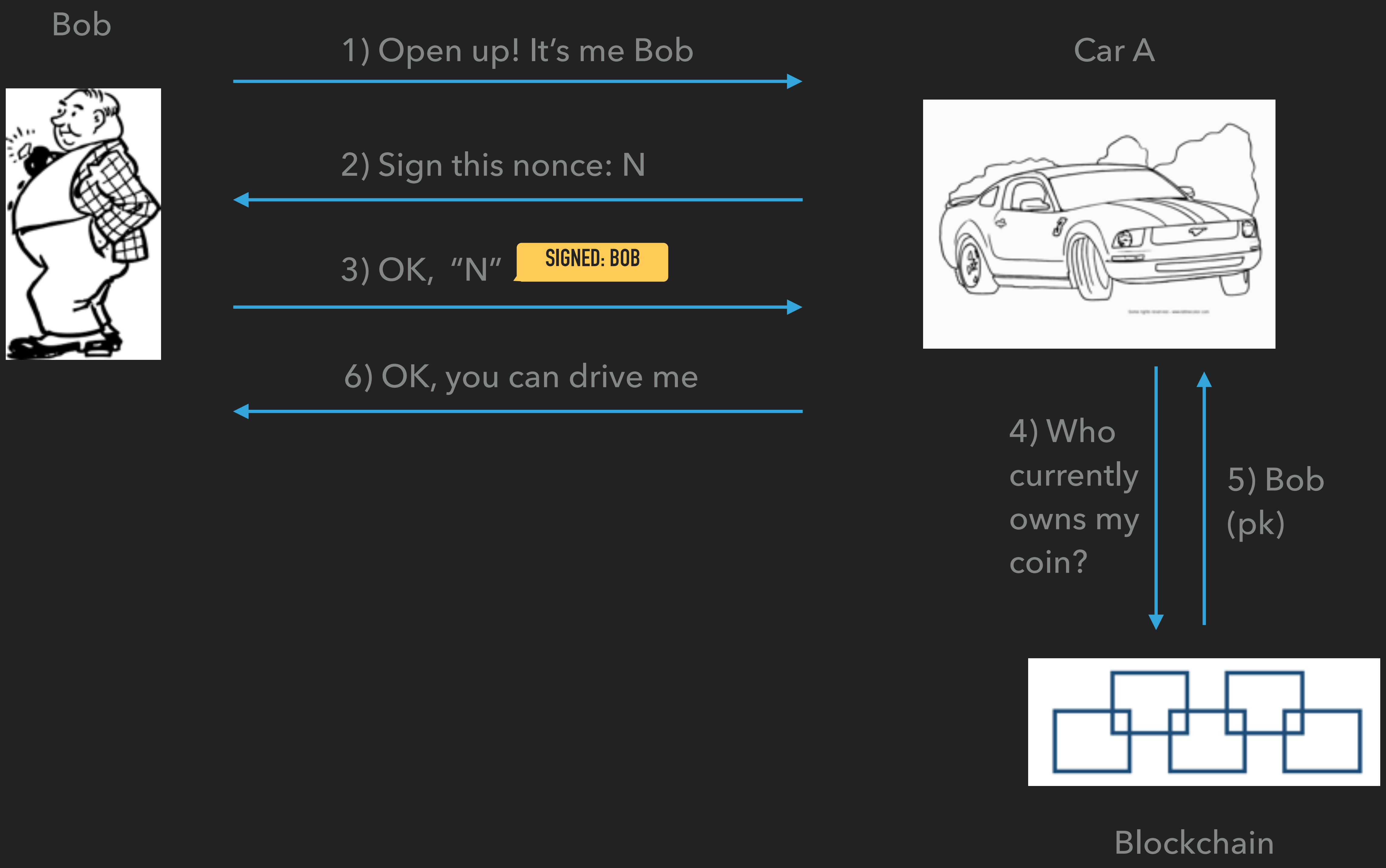
3) OK, "N" SIGNED: BOB

4) Who currently owns my coin?

5) Bob (pk)

Blockchain

SMART PROPERTY: AUTHENTICATION



Bob

1) Open up! It’s me Bob

Car A

2) Sign this nonce: N

3) OK, “N” SIGNED: BOB

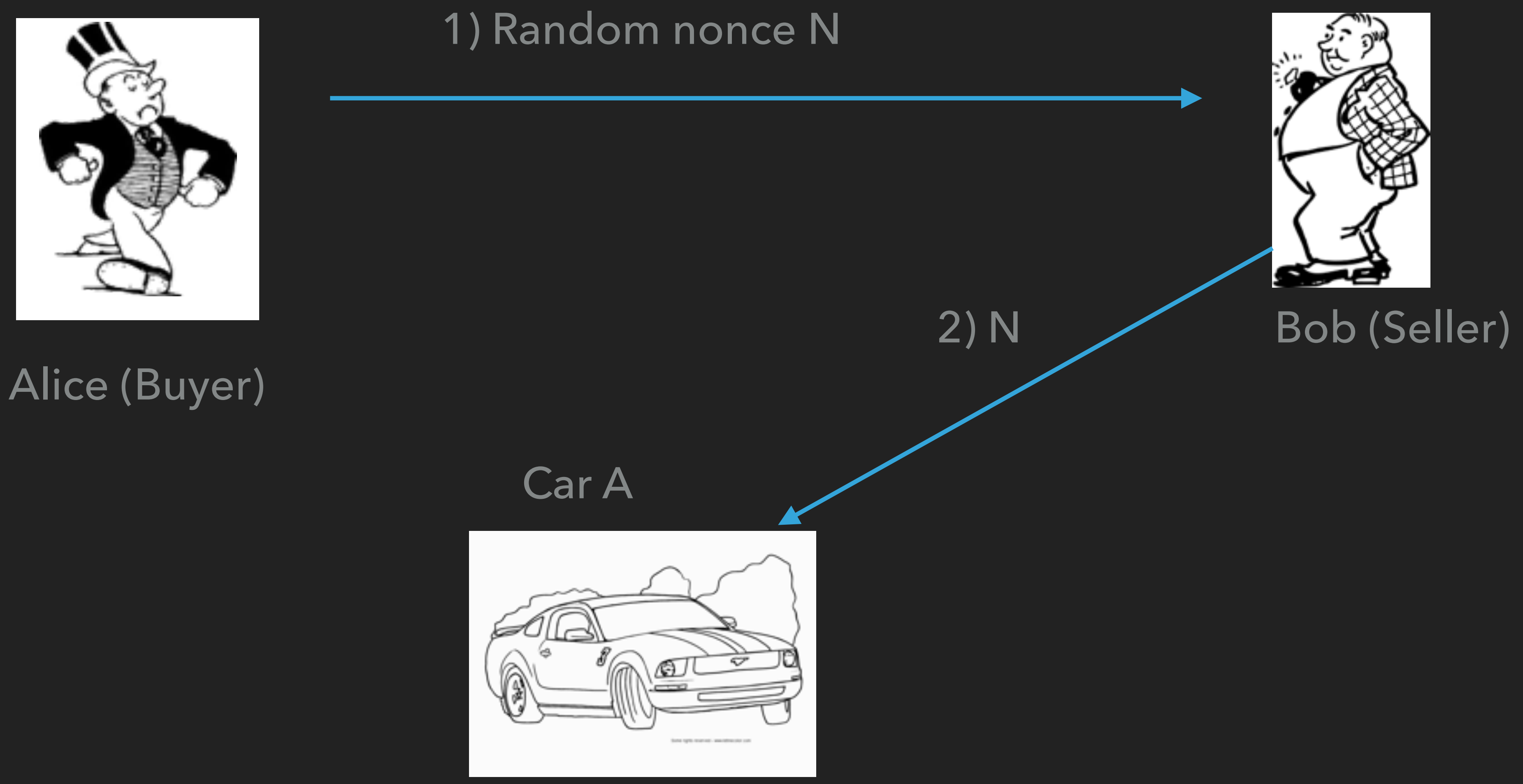
6) OK, you can drive me

4) Who currently owns my coin?

5) Bob (pk)

Blockchain

SMART PROPERTY: TRANSFERRING OWNERSHIP



1) Random nonce N

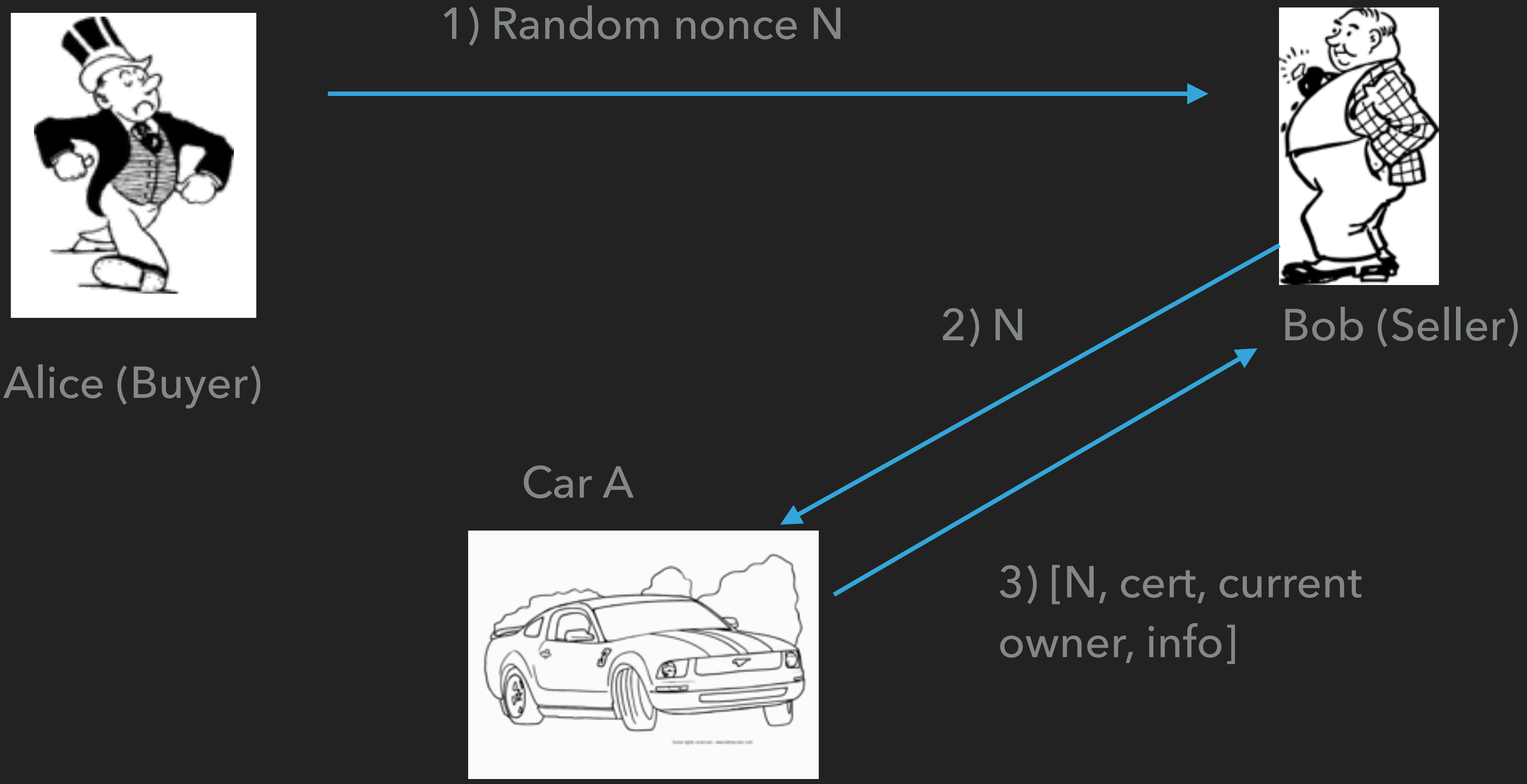
2) N

Alice (Buyer)

Bob (Seller)

Car A

SMART PROPERTY: TRANSFERRING OWNERSHIP



1) Random nonce N

Bob (Seller)

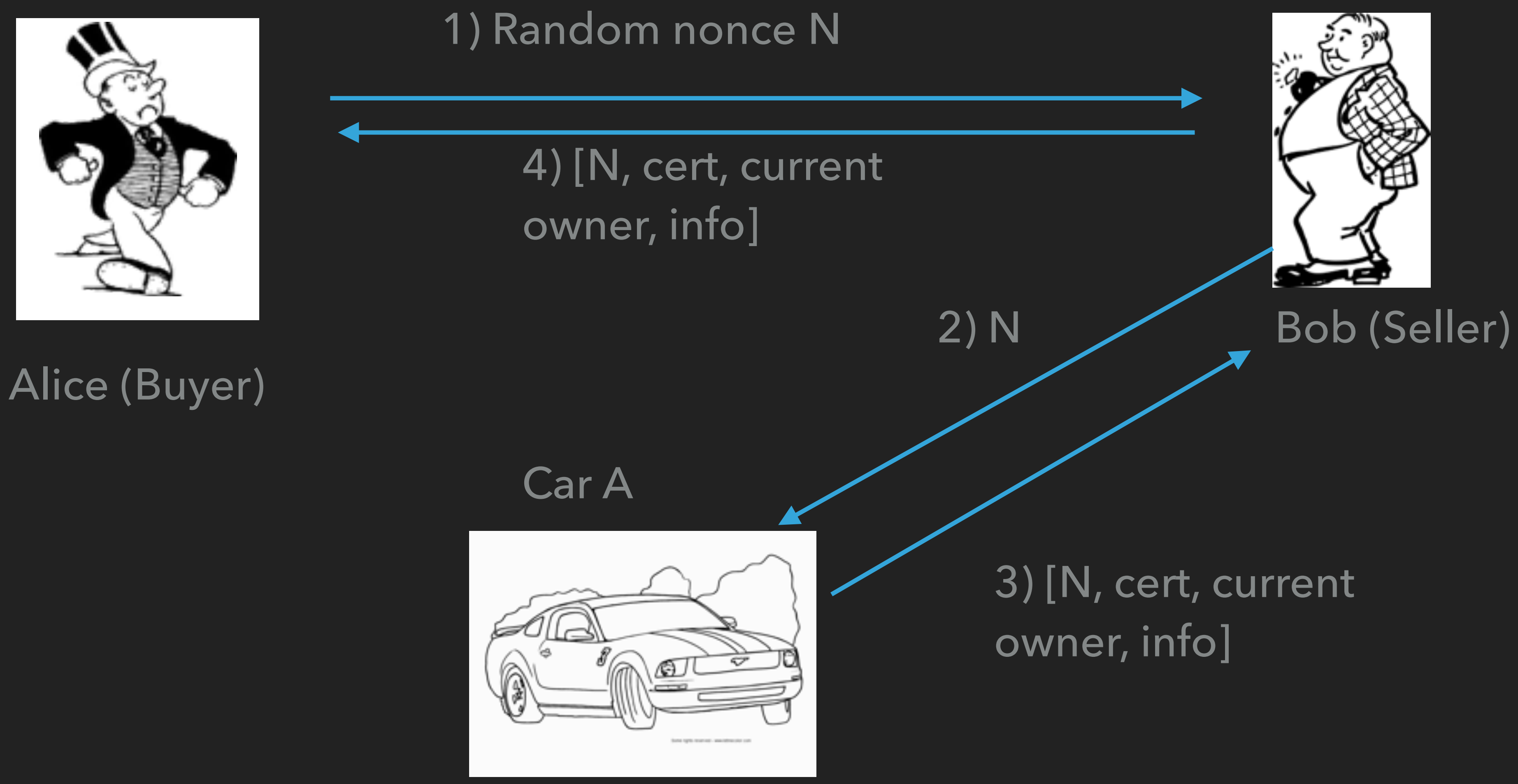
Alice (Buyer)

2) N

Car A

3) [N, cert, current owner, info]

SMART PROPERTY: TRANSFERRING OWNERSHIP



1) Random nonce N

4) [N, cert, current owner, info]

Alice (Buyer)

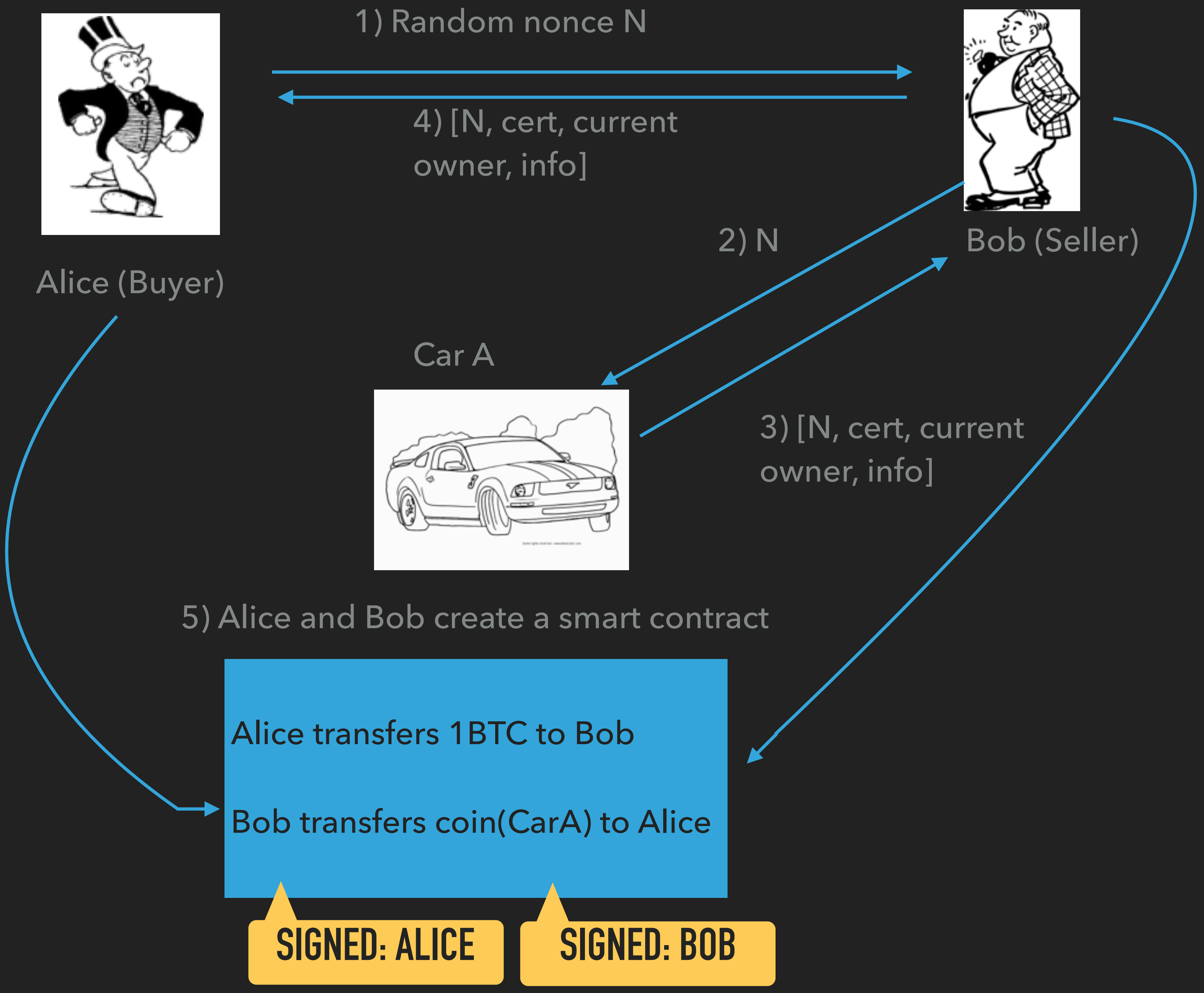
2) N

Bob (Seller)

Car A

3) [N, cert, current owner, info]

SMART PROPERTY: TRANSFERRING OWNERSHIP



Alice (Buyer)

Bob (Seller)

Car A

1) Random nonce N

2) N

3) [N, cert, current owner, info]

4) [N, cert, current owner, info]

5) Alice and Bob create a smart contract

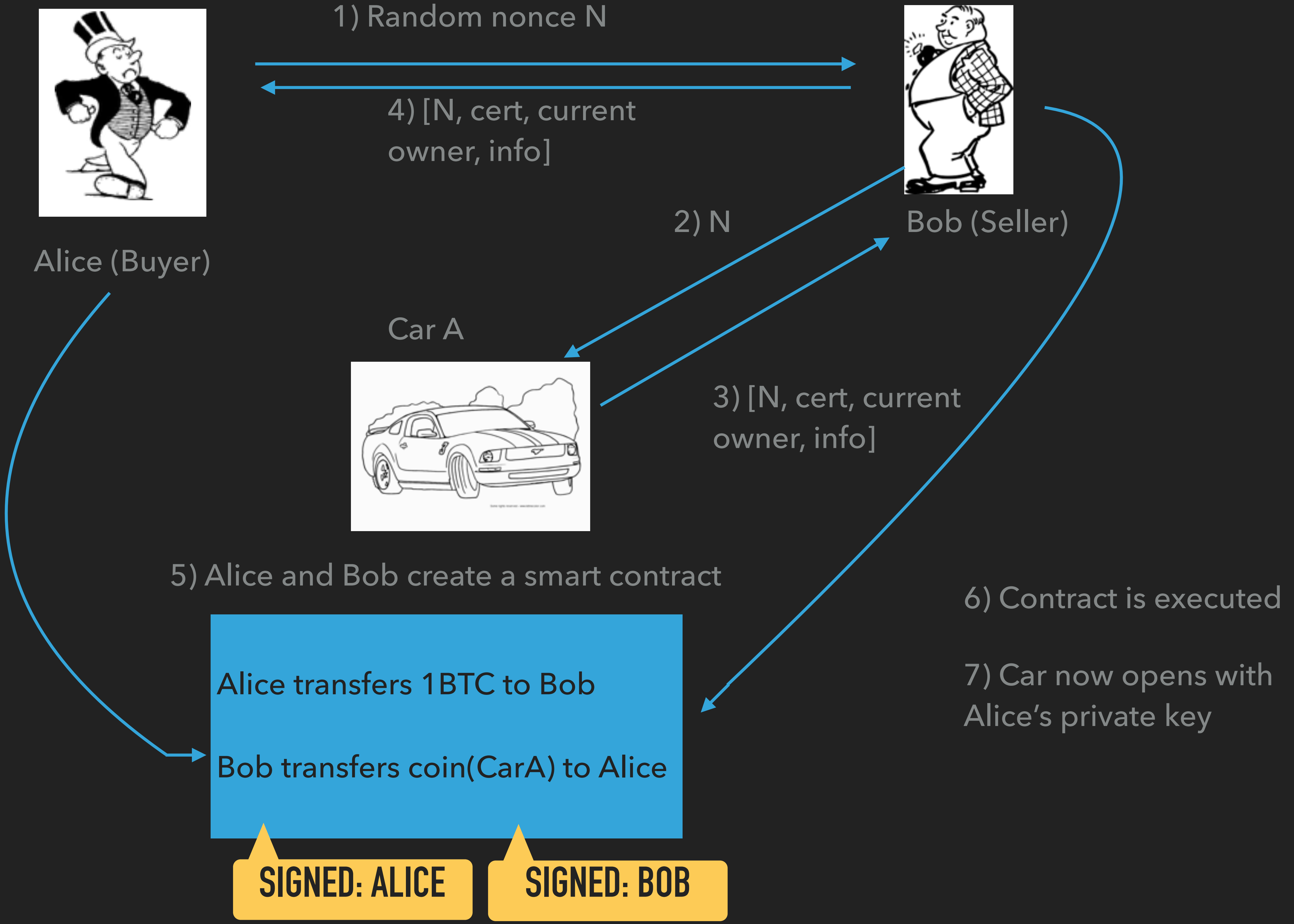
Alice transfers 1BTC to Bob

Bob transfers coin(CarA) to Alice

SIGNED: ALICE

SIGNED: BOB

SMART PROPERTY: TRANSFERRING OWNERSHIP



1) Random nonce N

4) [N, cert, current owner, info]

Alice (Buyer)

Bob (Seller)

2) N

Car A

3) [N, cert, current owner, info]

5) Alice and Bob create a smart contract

Alice transfers 1BTC to Bob

Bob transfers coin(CarA) to Alice

SIGNED: ALICE

SIGNED: BOB

6) Contract is executed

7) Car now opens with Alice's private key

SMART PROPERTY: ADVANTAGES

- Neither party can cheat the other
- Smart property can be used as collateral in a smart contract
- No need for centralised intermediary to track ownership

SMART PROPERTY: PROBLEMS

- Only works for things that rely on computers
- You need to trust the original manufacturer
- Requires trusted computing
- Makes everything easily re-possess-able
- Smart property transactions are worth more than normal BTC transactions: pollutes miner's incentives

PROVENANCE OF PHYSICAL OBJECTS?

- The blockchain provides provenance of coins
- Could it also provide provenance of physical stuff? Prove that it came from a certain place?

Is this wine really a 1985 Ponsot Burgundy?

Wine Spectator
www.winespectator.com
The Crusade Against Counterfeits
With Millions at Stake, Vintners and Collectors Take Action
BAROLO EXCELS IN 2005
GREAT VALUES FROM SPAIN
HOLIDAY GIFTS: CHEFS' PICKS
ARGENTINE MALBECS: WHAT TO BUY
Billionaire Bill Koch: "I plan to put people in jail."

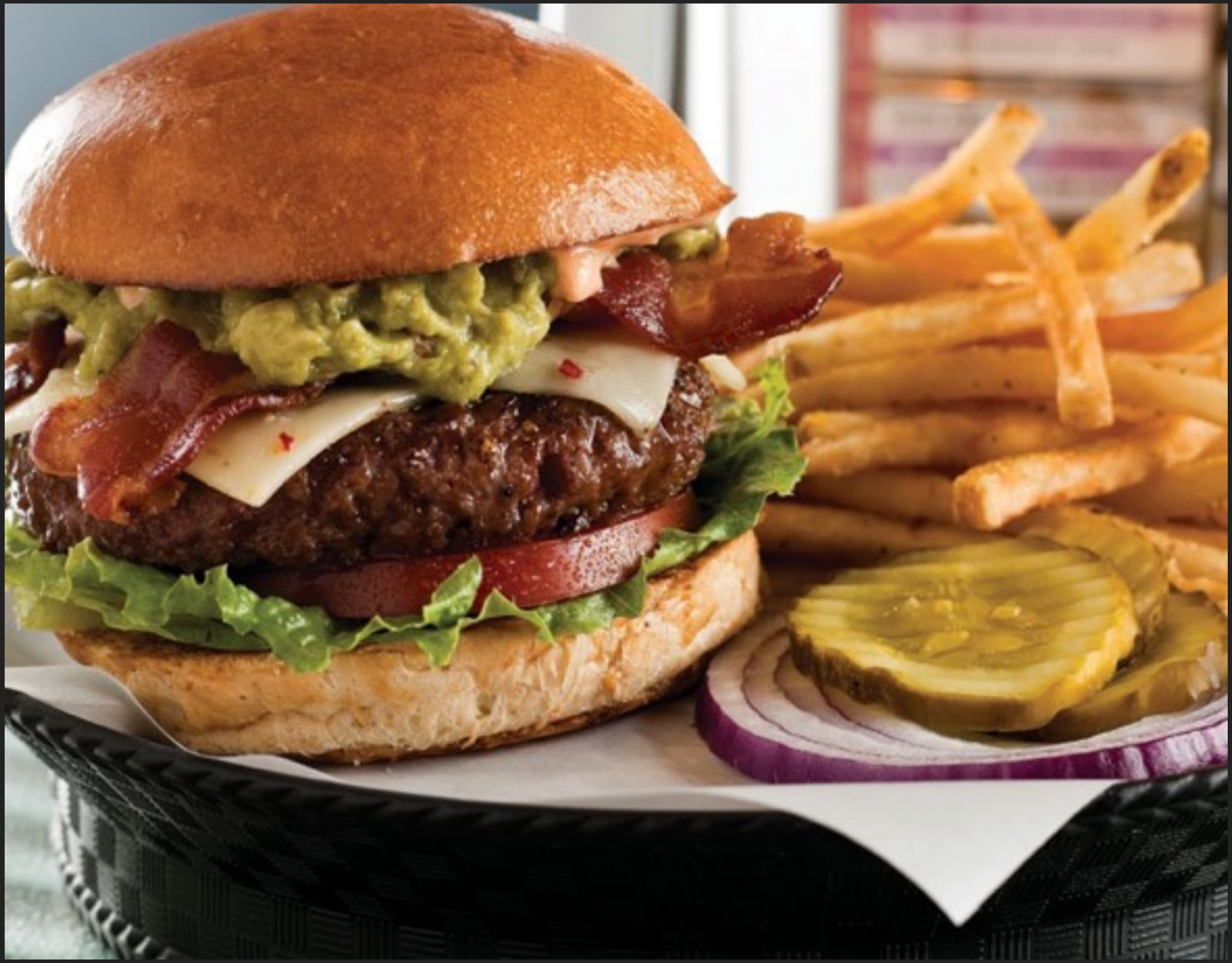
FIRST AID FOR
CHOKING

HR
217

GRAND VIN DE CHATEAU LATOUR
CHÂTEAU LATOUR A POMEROL
PREMIER GRAND CRU
GRAND VIN 1947
APPELLATION CONTRÔLÉE
Mis en Bouteilles au Château
GRAND VIN DE CHATEAU
MIS EN BOUT
AU CHATE

Is this clothing 100% organic cotton?

Is this burger 100% beef?



Is this burger 100% beef?

DAILY Mirror

The shark whisperer!

GIANT THRILLER

HORSE MEAT IS FOUND IN TESCO BURGERS

Supermarkets clear shelves

Inquiry at supply plants

LE FIGARO·fr économie

European supermarkets flooded with horse meat

DAILY STAR

RiRi's naked romps with Mossy

FREE OSCARS MUSIC CD

Pistorius goes free

1D death threats

QUEEN EATS HORSE

Dodgy meat served at Royal Ascot

Yummy!

Sun

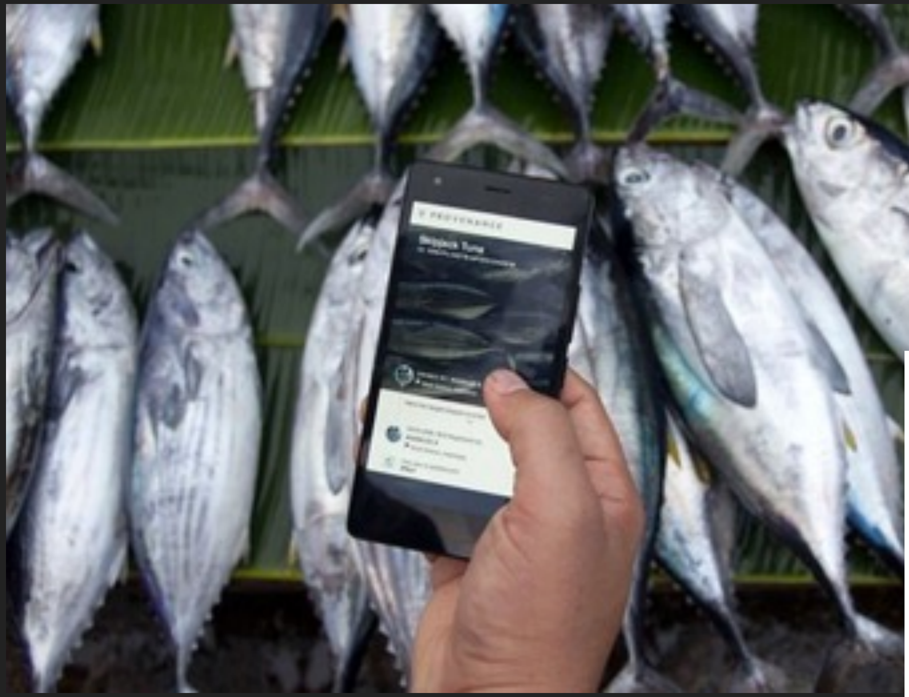
HORSE 'IN SCHOOL DINNERS'

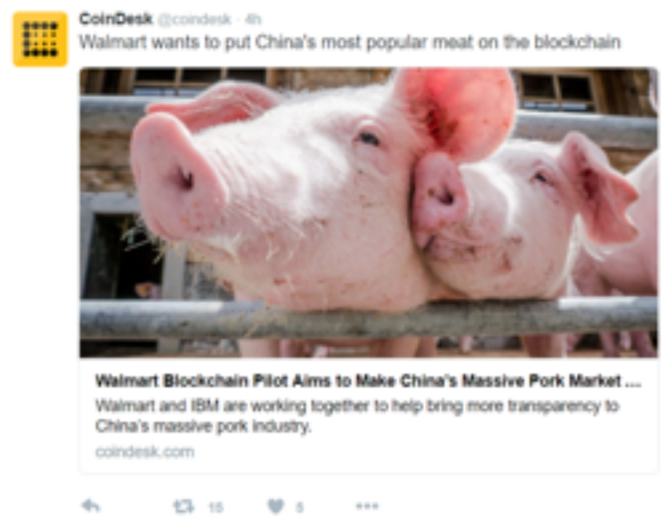
Govt order tests over meat fears

Mirror

FINDUS KNEW OF HORSE LASAGNE 12 DAYS AGO

BLOCKCHAIN FOR PROVENANCE OF PHYSICAL OBJECTS?





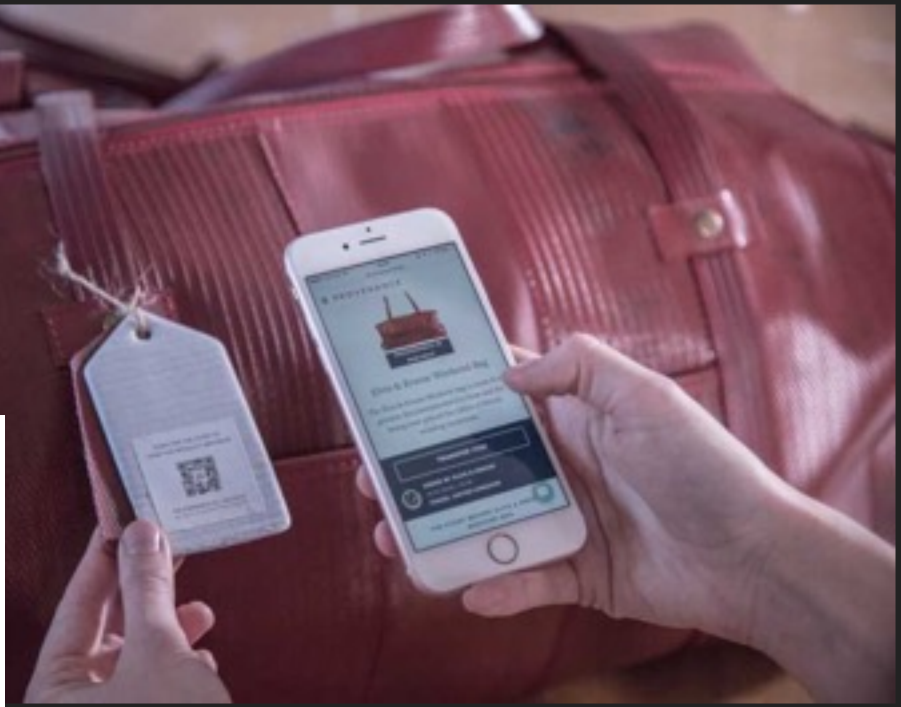
CoinDesk @coindesk · 4h

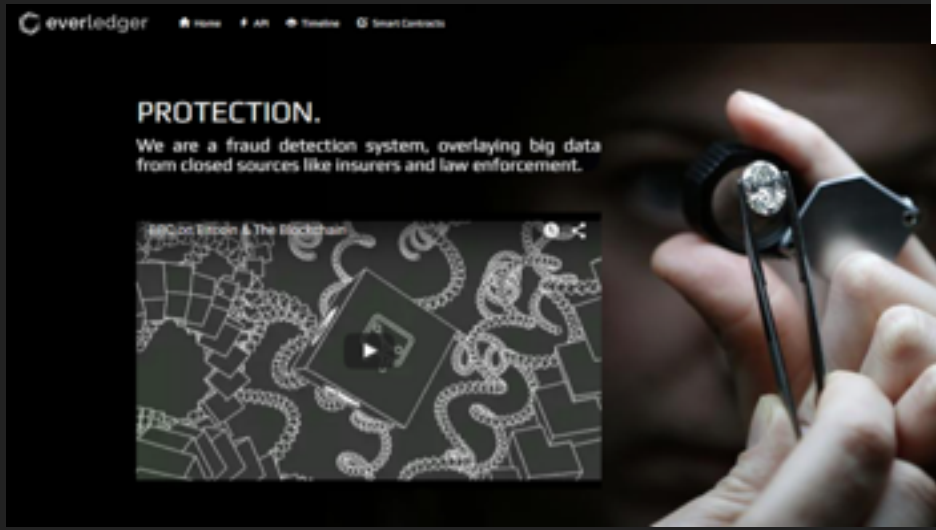
Walmart wants to put China's most popular meat on the blockchain

Walmart Blockchain Pilot Aims to Make China's Massive Pork Market ...

Walmart and IBM are working together to help bring more transparency to China's massive pork industry.

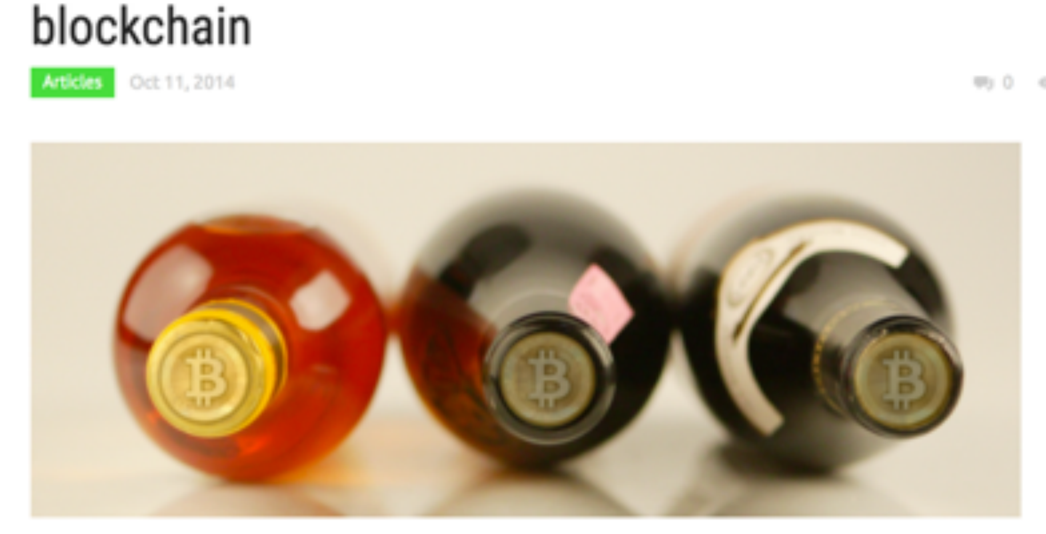
coindesk.com





PROTECTION.

We are a fraud detection system, overlaying big data from closed sources like insurers and law enforcement.



Future of Wine Provenance in the Bitcoin blockchain

“Every physical product [will] come with a digital ‘passport’ that proves authenticity (Is this product what it claims to be?) and origin (Where does this product come from?), creating an auditable record of the journey behind all physical products”

provenance.org

LIFE IS TOO SHORT TO DRINK FAKE WINE

Ponsot

Bottle #1 is represented by coin *burgundy1*

SIGNED: PONSOT

Rudy pays Ponsot

Ponsot transfers burgundy1 to Rudy.

SIGNED: PONSOT

Rudy

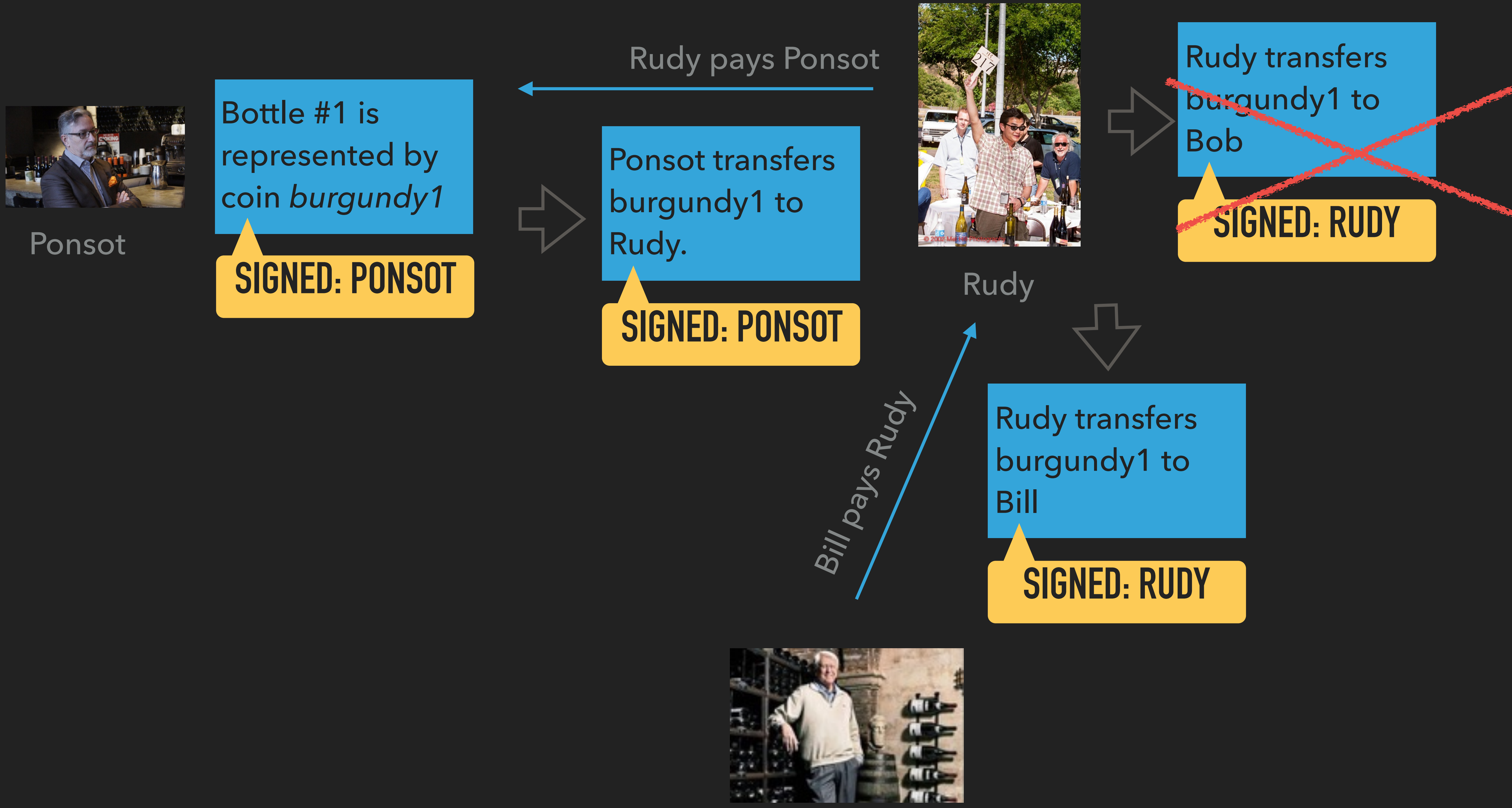
Rudy transfers burgundy1 to Bill

SIGNED: RUDY

Bill pays Rudy

Bill

LIFE IS TOO SHORT TO DRINK FAKE WINE



Ponsot

Bottle #1 is represented by coin *burgundy1*

SIGNED: PONSOT

Rudy pays Ponsot

Ponsot transfers burgundy1 to Rudy.

SIGNED: PONSOT

Rudy

~~Rudy transfers burgundy1 to Bob~~

~~SIGNED: RUDY~~

Bill pays Rudy

Rudy transfers burgundy1 to Bill

SIGNED: RUDY

Bill

PROBLEM 1: CAN YOU TRUST THE PRODUCER?

- Bill has to trust that Ponsot is not malicious or incompetent
- Even if Bill trusts Ponsot, what if Rudy has created a fake Ponsot key, and burgundy1 was not created by the real Ponsot? How does Bill find out what Ponsot’s real public key is?
- One solution is to check some external trustworthy look-up service which lists public keys and their owners (e.g. a key server or certificate authority)

LIFE IS TOO SHORT TO DRINK FAKE WINE

Ponsot

Bottle #1 is represented by coin *burgundy1*

SIGNED: PONSOT

Ponsot transfers burgundy1 to Rudy.

SIGNED: PONSOT

Rudy

~~Rudy transfers burgundy1 to Bob~~

~~SIGNED: RUDY~~

Rudy transfers burgundy1 to Bill

SIGNED: RUDY

Bill pays Rudy

Bill checks the chain all the way back to Ponsot's original sig, verifies against public keys from a trusted third party

Bill

PONSOT@BURGUNDY.COM: AI70X0HX
RUDY@RUDY.COM: SHAXAE2A
BILL@KOCH.COM: AHK8KIEZ

Trusted Third Party

PROBLEM 2: DOUBLE SELLING

- How does Bill know that *burgundy1* really represents the bottle Rudy is trying to sell?
- Rudy could have drunk the contents of the real bottle, or sold it
- Problem is particularly bad if many customers would still be willing to buy the good without a blockchain passport
    - Meat, raw materials, precious stones and metals, gold?

TAMPER-PROOF SEALS

- RFID / EMV chips inside the seal (e.g. blockverify.io)
- Breaking the seal destroys the chip
- Java Card: a microcontroller that contains the object's private key, and responds to cryptographic challenges: "I am burgundy1"

TAMPER-PROOF SEALS

- Problems:
- Private key kept on the chip, so vulnerable to cloning
- NFC chips can't do ECDSA
- Do you trust the chip manufacturer?
- Can only be opened once: not useful for things that need to be unboxed along the way: meat, cotton, rare metals or stones

HOW DECENTRALISED IS THIS?

- Is this system really decentralised? Buyers have to trust:
  - Original producer and their coin minting process
  - Identity provider (probably centralised)
  - Tamper-proof chip manufacturers
- Is the distributed consensus protocol still worth it? Can we get the same level of assurance without it?

DO WE NEED THE BLOCKCHAIN?

- Original producers and buyers already have incentives to block attempts by intermediaries to double-sell
- So they just need a record of who said what about each token, when, to whom

DO WE NEED THE BLOCKCHAIN?

Ponsot

Bottle #1 is represented by coin *burgundy1*

SIGNED: PONSOT

Ponsot transfers burgundy1 to Rudy.

SIGNED: PONSOT

Rudy

~~Rudy transfers burgundy1 to Bob~~

~~SIGNED: RUDY~~

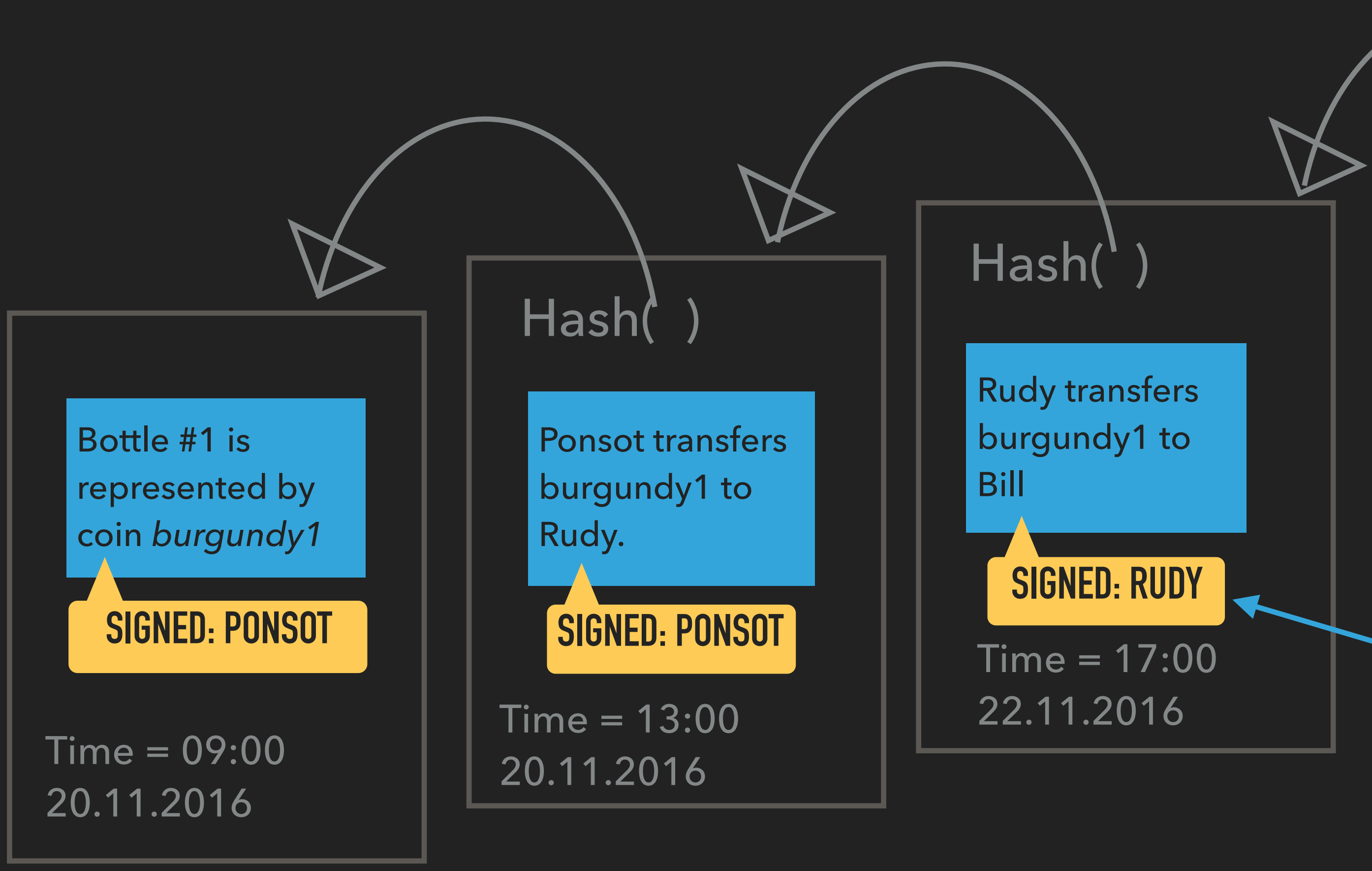
Rudy transfers burgundy1 to Bill

SIGNED: RUDY

Bill

Bill also checks for double-spending

SECURE TIME STAMPING WITH CHAINED HASH POINTERS



Bottle #1 is represented by coin *burgundy1*

SIGNED: PONSOT

Time = 09:00
20.11.2016

Hash( )

Ponsot transfers burgundy1 to Rudy.

SIGNED: PONSOT

Time = 13:00
20.11.2016

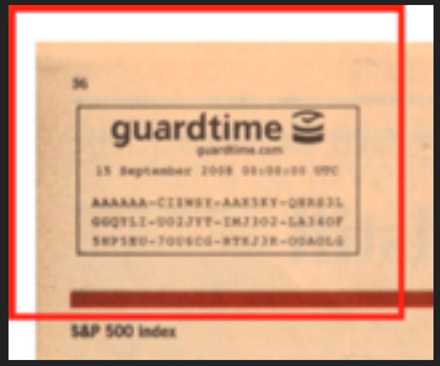
Hash( )

Rudy transfers burgundy1 to Bill

SIGNED: RUDY

Time = 17:00
22.11.2016

Hash ( )



36

guardtime
guardtime.com

15 September 2008 00:00:00 UTC

AAAAAA-CIIWSY-AAKSKY-QBR8JL
GGQYLI-UO2JYT-IMJ3O2-LA34OF
5HPSBU-7OU6CG-RTKJ3K-OOAOLG

S&P 500 index

Bill checks the hash to see the chain hasn't been tampered with

Bill

PONSOT@BURGUNDY.COM: AI70X0HX
RUDY@RUDY.COM: SHAXAE2A
BILL@KOCH.COM: AHK8KIEZ

Trusted Third Party

Bill checks the provenance of the bottle by verifying the signatures against public keys listed in a trusted third party

CHAINED HASH POINTERS FOR PROVENANCE

- Self-regulating: buyer can check where the object came from and check for double spending
- Any attempts to change history will break the hash pointer chain
- Bill can verify the signed messages against a trusted list of public identities:
    - Specifically, Ponsot’s original message ‘minting’ the coin, and intermediate transactions

ADVANTAGES OF HASH CHAINS FOR PROVENANCE

- No need for mining pools, proof-of-work, or even a cryptocurrency
- No transaction costs or miner’s rewards
- Lower computational costs
- Less environmental damage
- No ‘polluting’ of Bitcoin’s carefully balanced miner’s incentives
- Potentially resistant to quantum computing attacks (http://eprint.iacr.org/2014/321.pdf)

ADVANTAGES OF HASH CHAINS FOR PROVENANCE

- All transactions on bitcoin-style blockchains are public by default
- This is a potential privacy nightmare
- Chained hash pointers don’t contain any transaction data…

WHEN DO YOU ACTUALLY NEED THE BLOCKCHAIN?

- The blockchain is essential to Bitcoin
- It enables us to prevent double spending of cryptocurrency using *distributed consensus*
- It's very expensive, but that's the cost of preventing double-spending in a trestles environment
- The blockchain is also essential to smart contracts: it ensures that we can make binding agreements on what code will run

SMART PROPERTY: YOU NEED MORE THAN A BLOCKCHAIN

- Smart property uses the blockchain
- But you still need to trust the original product manufacturer and be able to check their certificates
- You need to trust the object’s computer
- Only works if the object is completely controlled by its computer
- All your smart property could become deposit / collateral
- Weird combination of trusted computing and decentralisation

PROVENANCE OF PHYSICAL GOODS: YOU DON'T NEED THE BLOCKCHAIN

- You don’t need a full proof-of-work blockchain to track provenance of physical objects in a decentralised way
- This can be done more cheaply, with greater privacy, using simpler blockchain technology (invented in 1990!)
- Neither system works well for goods which require unpacking / repacking along the supply chain
- Either way, you also need an identity layer.

CONCLUSION

- Blockchains are useful for decentralised cryptocurrency, smart contracts and digital property
- They might help us create smart property, but smart property is weird
- For provenance, it’s better to use chained hash pointers

THANK YOU / GRACIAS!

- r@reubenbinns.com
- @RDBinns