IoT with Blockchain

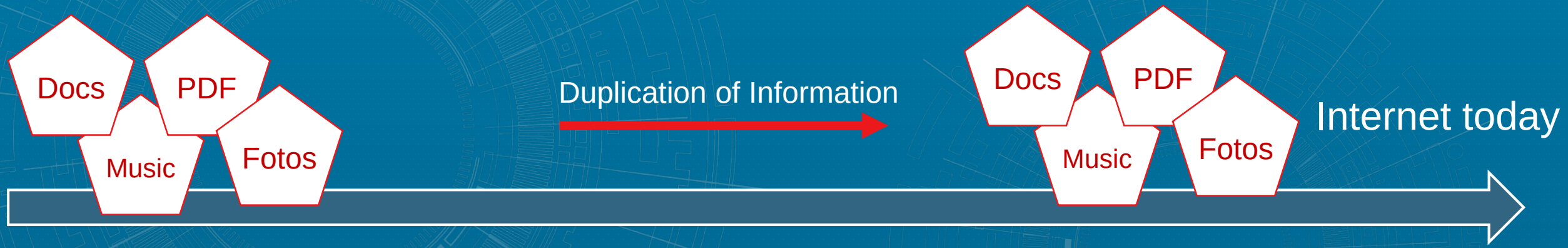
Smart Contracts implementation & interoperability

Aires Marques
Principal Blockchain Consultant, Oracle

IoT with Blockchain

More resources
Less barriers

Internet of information



Internet with Blockchain

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

financial crisis
eat Crash of 2008
Disbelief, and a punter
The plunging market yesterday dealt a
new blow to investors' confidence, as
the government decided to inject
million into counselling
losers in the financial
Retail
SATURDAY, OCTOBER
revised its economic
for this year down to
per cent. For next
to 2 per cent,
Last night
Chao
spokesman,

October 2008 – Bitcoin whitepaper

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

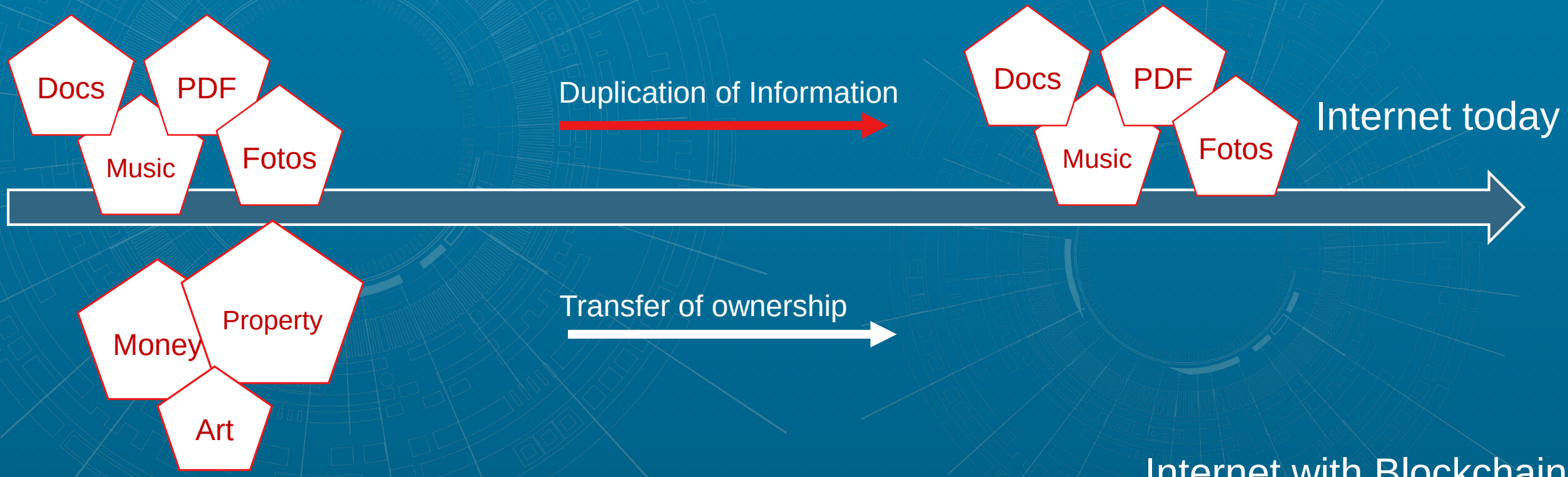
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

January 3rd 2009 – The Genesis Block

```
GetHash()      = 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
hashMerkleRoot = 0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
txNew.vin[0].scriptSig     = 486604799 4 0x736B6E616220726F662074756F6C69616220646E6F63657320666F206B6E697262206E6F20726F6C6C65636E6168432039303032 2F6E614A2F33302073656D695420656854
txNew.vout[0].nValue       = 5000000000
txNew.vout[0].scriptPubKey = 0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4C3FBCF649B6DE611FEAE06279A60939E028A8D65C10B73071A6F16719274855FEB0FD8A6704 OP_CHECKSIG
block.nVersion = 1
block.nTime    = 1231006505
block.nBits    = 0x1d00ffff
block.nNonce   = 2083236893

CBlock(hash=000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505, nBits=1d00ffff, nNonce=2083236893, vtx=1)
  CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
    CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030332f4a616e2f323030392043686616e63656c6c6f72206f6e206272696e6b206f66207365636f6e642061696c6f757420666f722062616e6b73)
    CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
  vMerkleTree: 4a5e1e
```

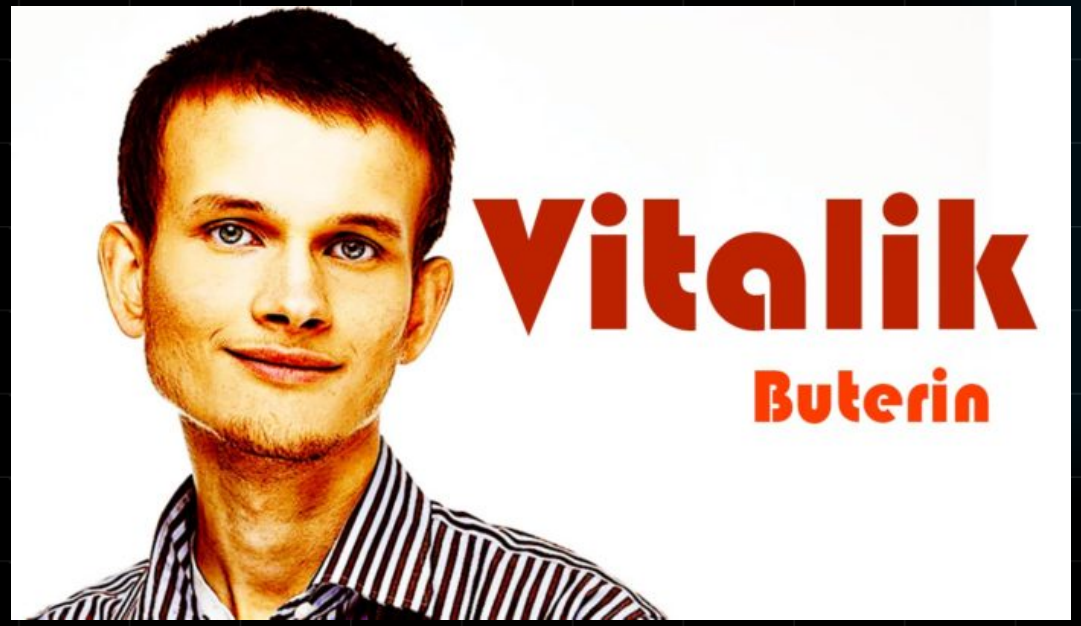
Blockchain – The internet of value



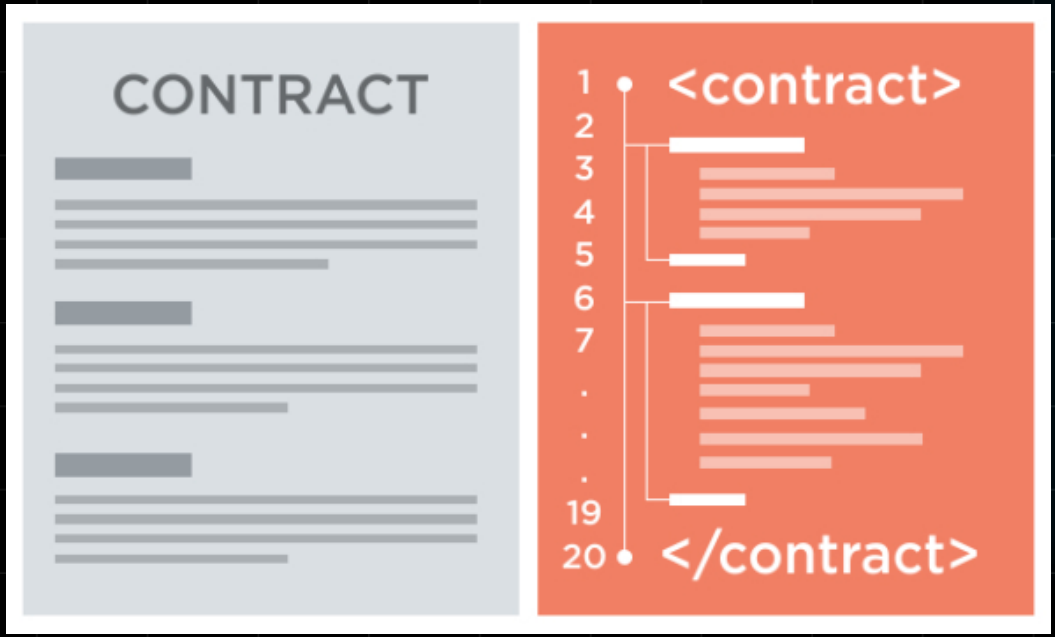
Blockchain creates TRUST

- Immutable
- Unforgeable
- Replicated

July 2015 – Ethereum / smart contracts



Smart contracts



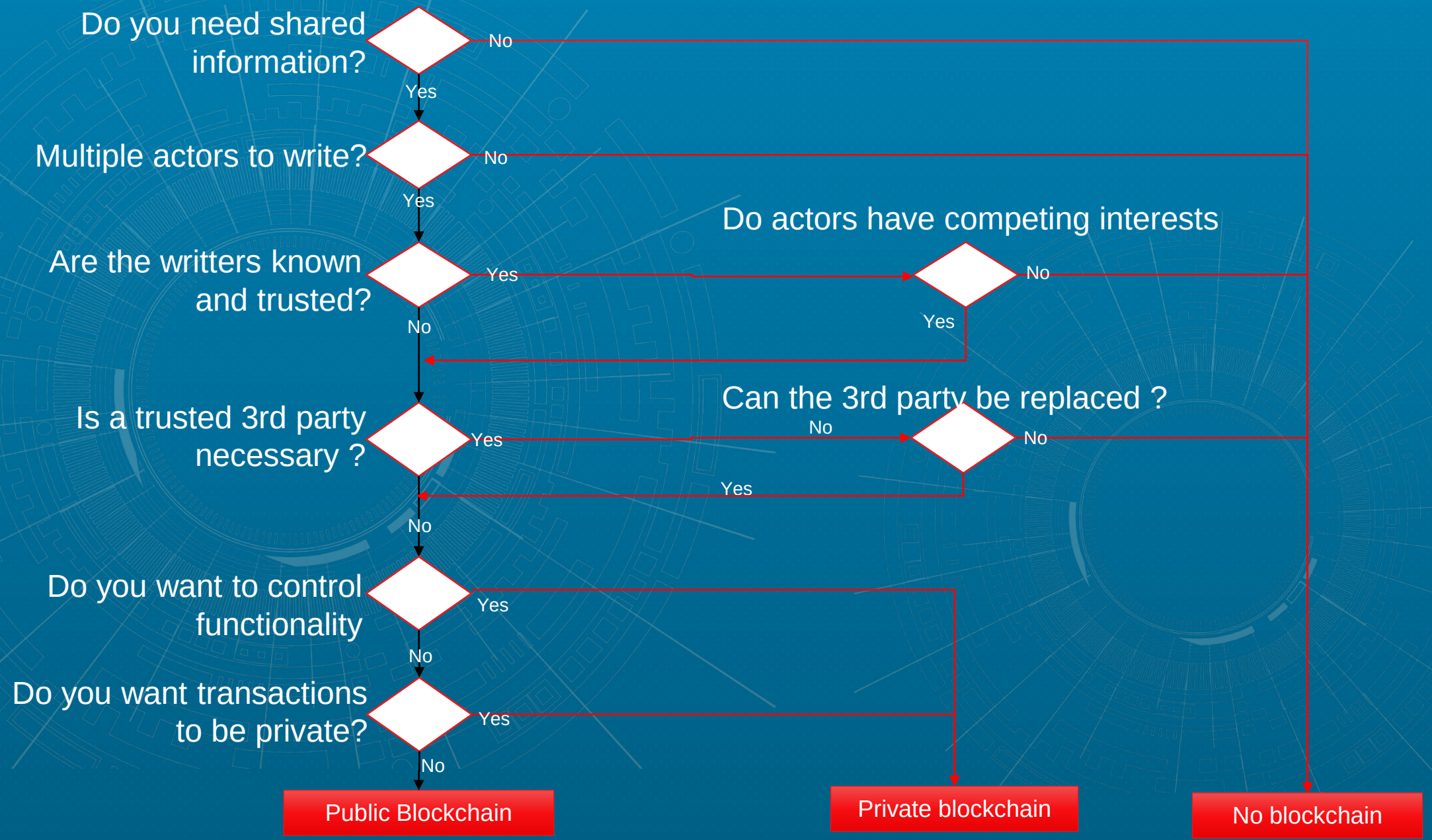
- It’s code !
- Simple logic
- Blockchain specific
- Reactive
- Can be legally binding
- Autonomous
- Contract account

Example:
0x4B8ef9f403b6bA4ab19A6390146f52ad6cb6486c

Blockchain for everything ?

How to decide ?

Do we need blockchain ?

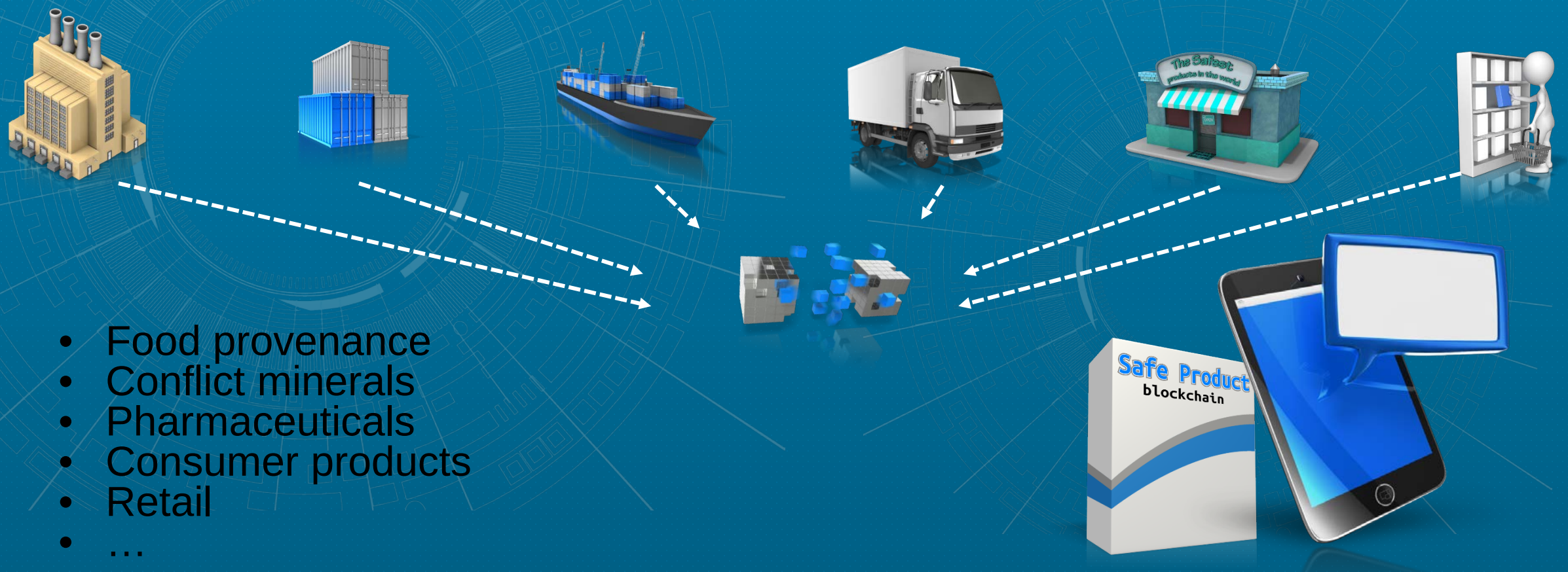


Based on Bart Suichies Blockchain model 2015

Use cases

Supply Chain with Blockchain / IoT

Every actor can verify the goods on the Blockchain
Some actors can write transactions on the Blockchain
IoT, GPS location, temperature, vibration, humidity enrich the data



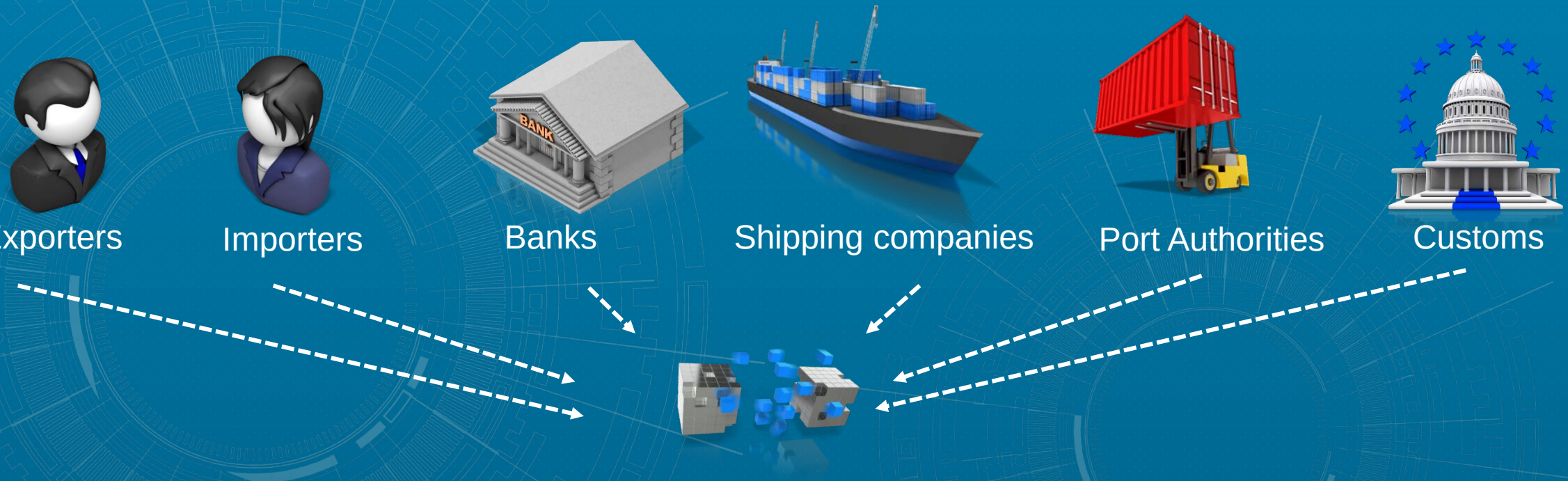
- Food provenance
- Conflict minerals
- Pharmaceuticals
- Consumer products
- Retail
- …

Supply Chain with Blockchain / IoT

Benefits:

- Visibility across the whole Supply Chain
- Prevention of counterfeit goods
- Track & Trace products
- Instant payments
- Recall identification & Management
- Quality management
- Reduced paperwork and administrative costs
- Supply chain acceleration
- VAT tax collection
- Customs, Certification & Compliance

Trade finance : Letter of Credit



Today’s challenges :
Manual processes
Documentary fraud
Expensive and ineffective process

Benefits with IoT/Blockchain:
Increased speed
Reduced cost
Reduced risk
Value added

Public records

- Real estate records
- Vehicle registration
- Citizen identity
- Land ownership
- School certificates
- E-Voting

Interoperability

Interoperability IoT with Blockchain

Software vendors are aware of the value of combining Blockchain with IoT.

- Cloud services offering integrate IoT with Blockchain.

Most leading Blockchain technologies support IoT

Distributed ledger protocols such as IOTA were created specifically for IoT

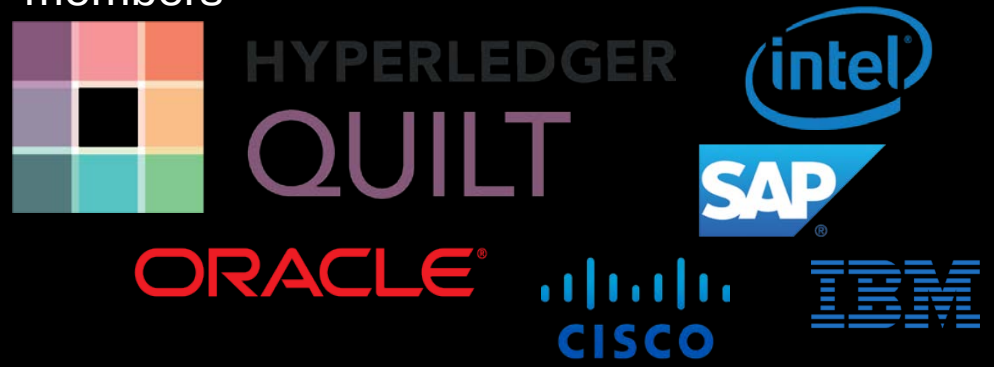
W3C, IEEE are defining Industry standards

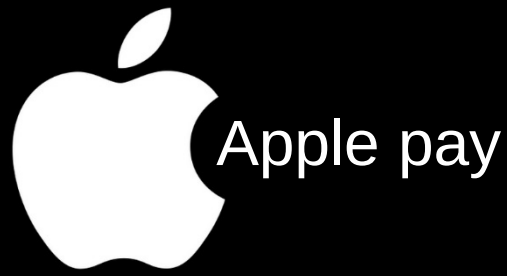
Interoperability between blockchains

Ripple has over 100 member banks

Currently only for payments

- Hyperledger is one of the leading permissioned enterprise Blockchains
- More than above 100 large corporations as members





Apple pay

Implementation

The most important decision is the choice of technology

- Use the decision model to know if blockchain is a fit.
- Use cases should drive the decision of which blockchain to be used.
- Look into the future, consider the roadmap of different technologies.
- Choose technology that today already has high interoperability.

IoT with Blockchain

Empowering people and business

More resources - Less barriers

Aires Marques
Principal Blockchain Consultant, Oracle