

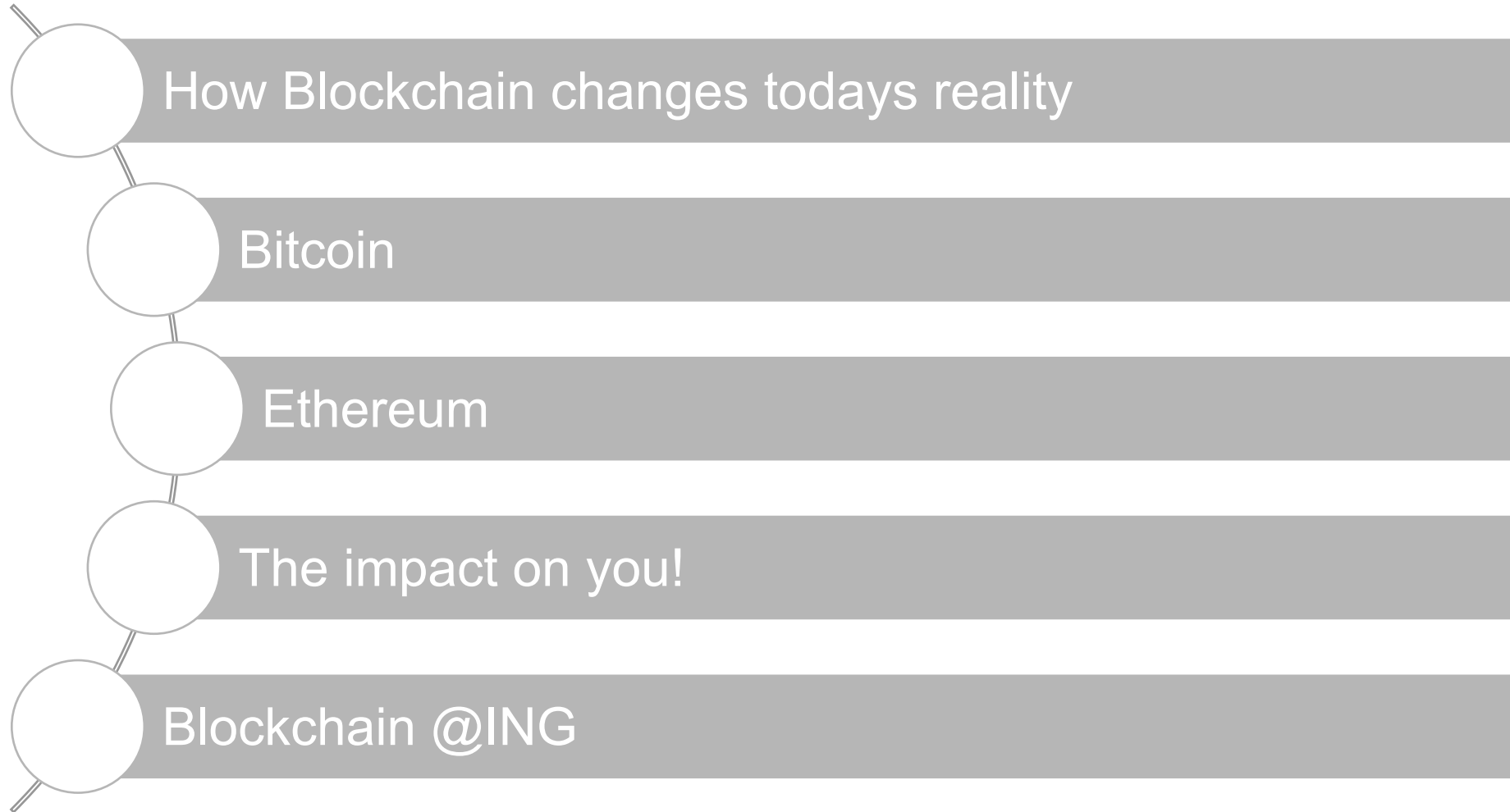
Blockchain for developers



Peter Penning and Cees van Wijk

Amsterdam, June 13th 2017

Program

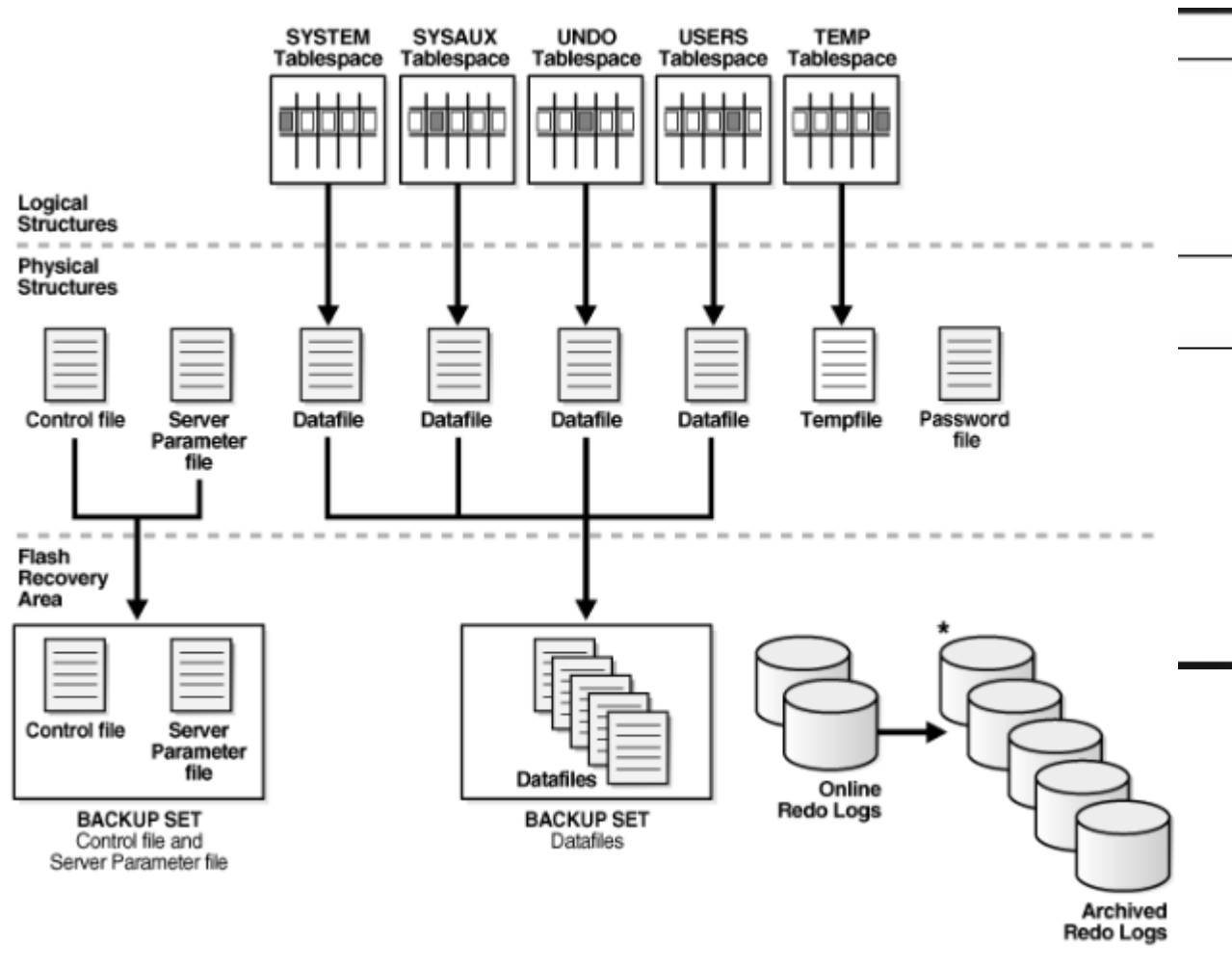


Today's reality

Classic Business Applications

- Models a part of the world from its own perspective
- Builds or buys a domain-specific solution
- Integrate in own application-architecture via interfaces (file, message or API-based)
- Deployment in own datacenter or cloud
- Every organisation models its own world and has its own set of applications and data

Classic Business Applications



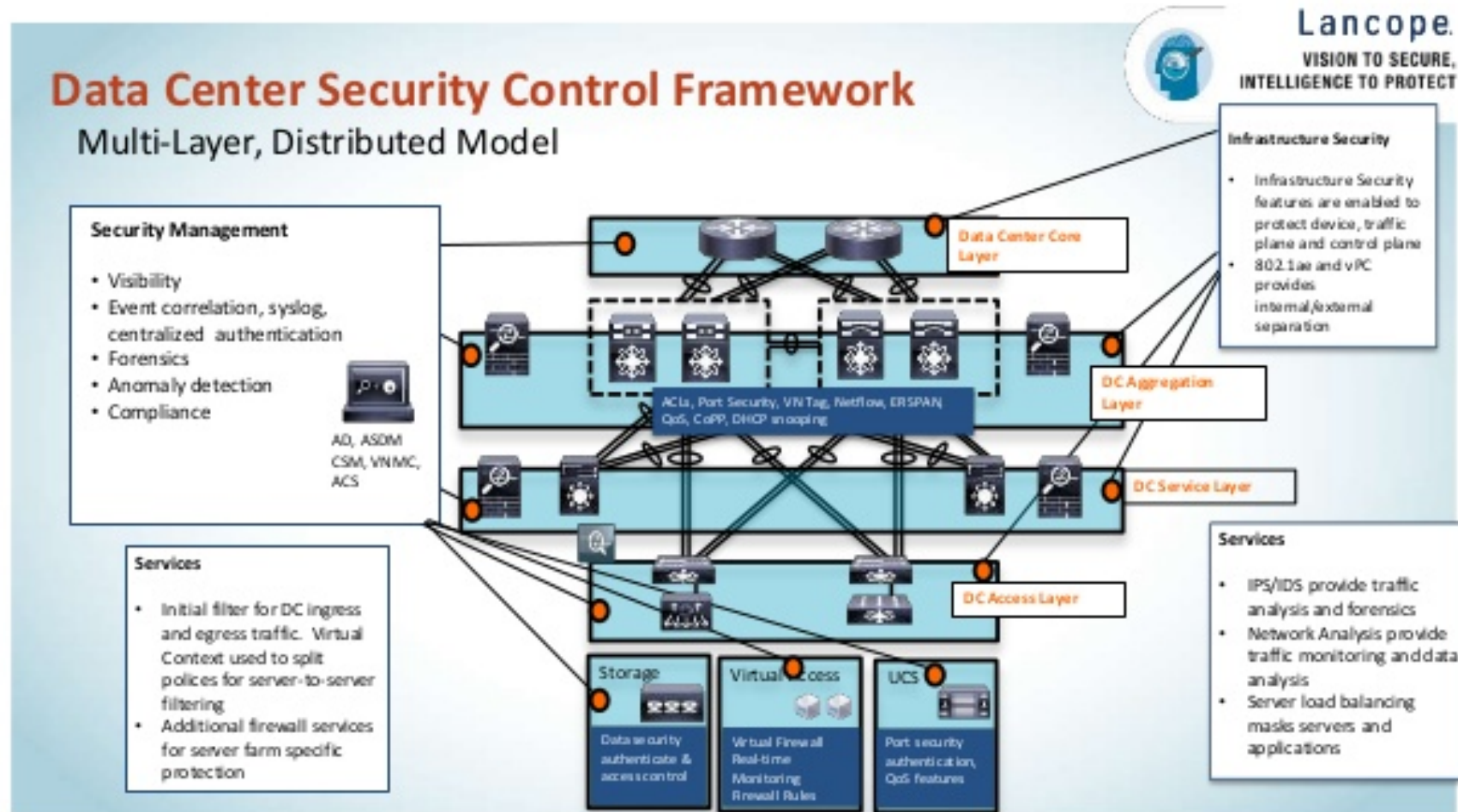
Every organization is keeping its own systems of record



Classic Business Applications - Security

- How do you make sure that data has no unauthorized changes
 - Assess requirements for Confidentiality, Integrity and Availability
 - Datamanagement measures (where is production?)
 - Physical access restrictions
 - User Access Management (Identification, Authorisation and Permissions)
 - Logical control access: network security
 - Fraude detection mechanisms
- How do you make sure your data is correct
 - Reconciliation with other datasources

Classic Business Applications



Today's reality



L A Y E R 8

Hacker breaches University of Greenwich, exposes 21,000 people's data

Patrick Howell O'Neill —2016-06-09 05:34 p.m. | Last updated 2016-06-09 07:20 p.m.

Reuters
Sep 26, 2016

☒ Heartland Payment Systems data breach coverage



'You guys decided to kick me out of University because you couldn't handle the beast.'















♡ Cybersecurity

♡ ICT

♡ Kadaster

BitCoin

First generation Blockchain – Beginnings and growth (1/4)

Market Cap ▾ Trade Volume ▾ Trending ▾ Tools ▾							Search Currencies	Q
All ▾	Currencies ▾	Assets ▾	USD ▾				Next 100 →	View All
▲#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)	
1	 Bitcoin	\$16,252,208,957	\$1005.51	16,163,150 BTC	\$124,961,000	1.26%		
2	 Ethereum	\$1,121,101,479	\$12.61	88,873,328 ETH	\$29,278,700	12.49%		
3	 Ripple	\$232,072,149	\$0.006265	37,044,533,660 XRP *	\$586,147	0.03%		
4	 Litecoin	\$186,819,438	\$3.75	49,782,806 LTC	\$3,726,780	0.62%		
5	 Monero	\$172,178,513	\$12.35	13,944,516 XMR	\$2,354,210	0.55%		
6	 Dash	\$122,058,038	\$17.19	7,099,948 DASH	\$1,430,550	2.15%		
7	 Ethereum Classic	\$110,208,461	\$1.24	88,831,226 ETC	\$1,528,940	4.11%		

What is it

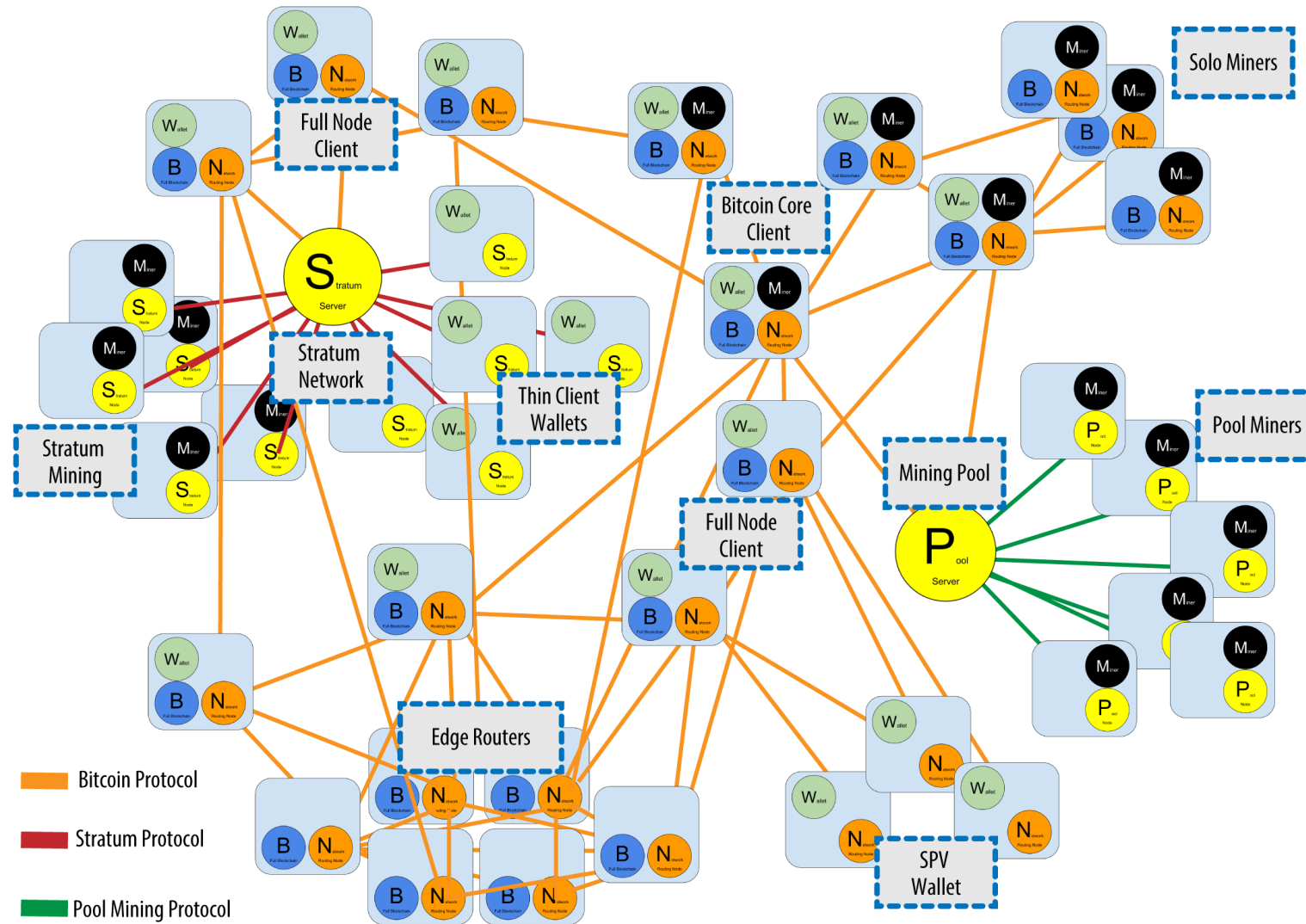
- Peer-to-peer network
- Cryptographically protected data
- Decentralized trust via reward and consensus mechanism

First Generation - A look under the hood

ING video

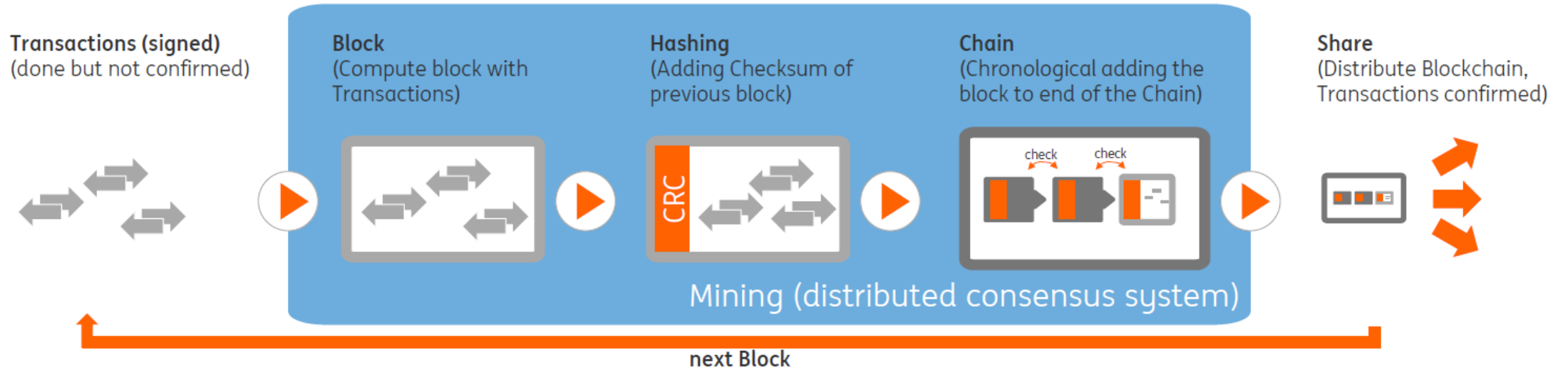
<http://www.videobox.intranet/videos/1479/ing-blockchain-animation-v1.1>

Peer2peer network



First generation Blockchain - Conceptual view

Generation of one Block and adding to the Chain



Block: collection of transactions

Transaction: message with sender, receiver, and information

Consensus: rules on accepting a transaction

First generation Blockchain - Core concepts to remember

distributed

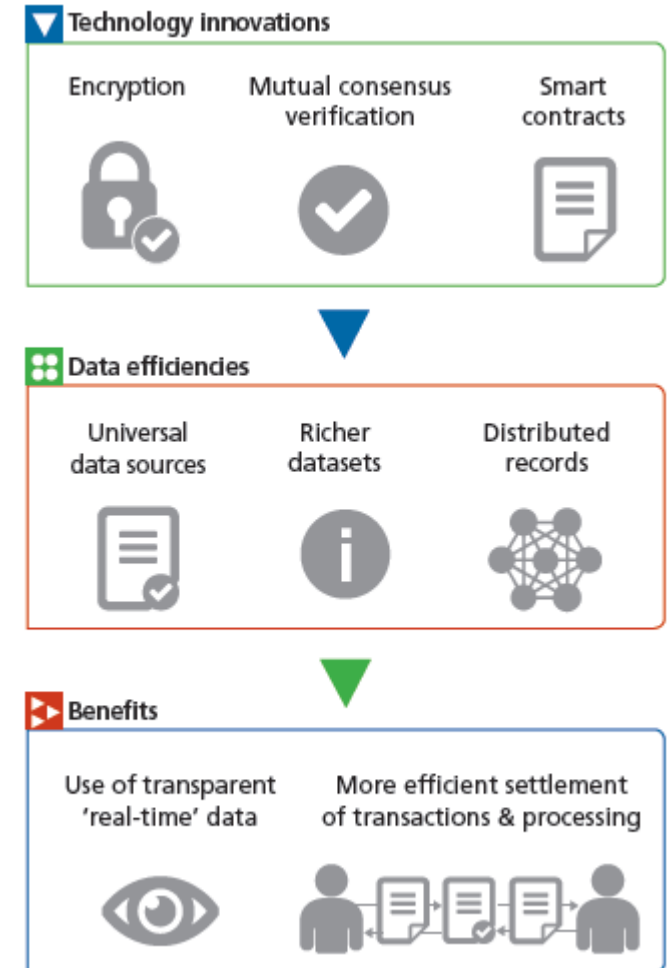
immutable

ledger

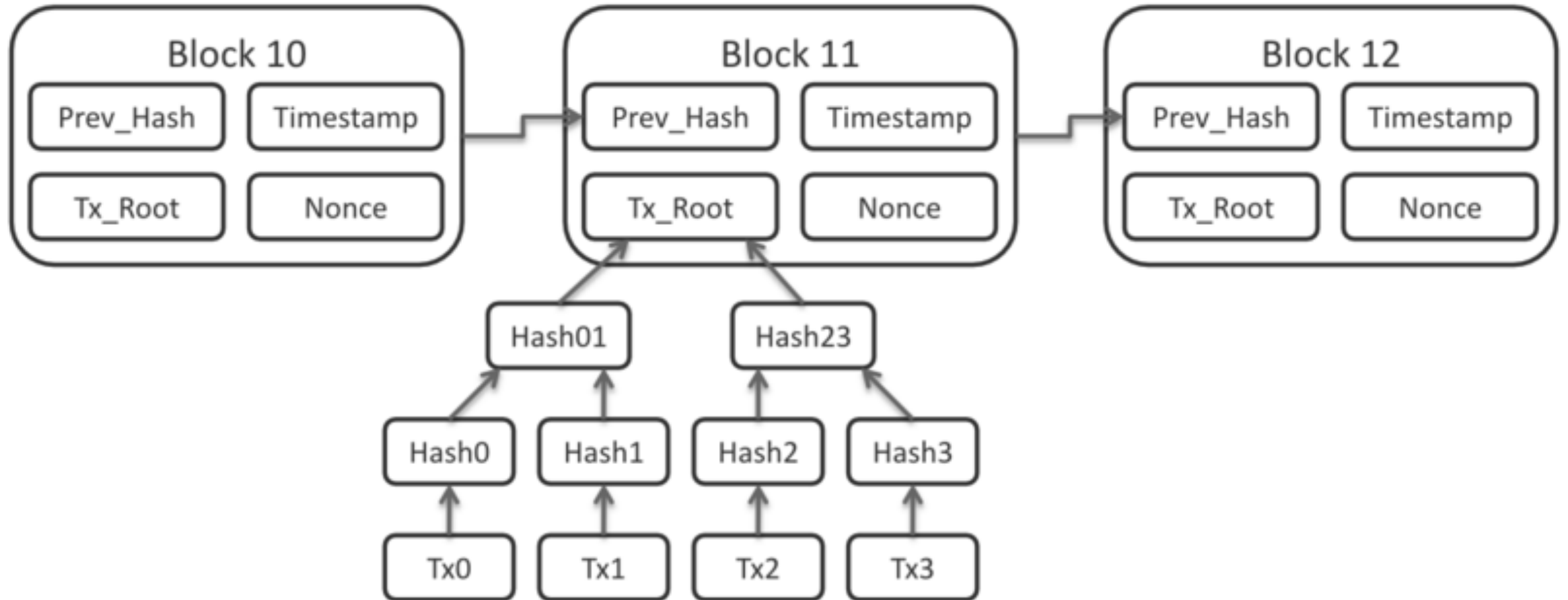
Replicated datastores, no central storage

Trust is created by design, not given by or to individual participants

Data is cryptographically guaranteed consistent and correct



Immutability



Ethereum

Next generation Blockchain - Ethereum

- The best known 2nd generation Blockchain is Ethereum
- Instead of a small script, Ethereum runs code specified in a Turing-complete language
- It means there are no logical limitations to the code
- The user-defined code on Ethereum are called Smart Contracts
- Executing a contract consumes Ether, a digital currency
- Value: let's have a look <https://coinmarketcap.com/>
- In a way, it's a slow but very reliable World Computer

Ethereum's Vitalik Buterin Wins World Technology Network Award

Nermin Hajdarbegovic | Published on November 19, 2014 at 16:52 BST



Vitalik Buterin has beaten Facebook's Mark Zuckerberg to win the World Technology Network (WTN) award for IT software.

Buterin, the developer of crypto 2.0 platform Ethereum and co-founder of *Bitcoin Magazine*, received the honour at the WTN's [2014 summit](#) held at the Time & Life building in New York City. The event was organised in association with *Fortune* and *Time*.



What is smart contract?

“A smart contract is software that can automatically execute the terms of a contract.”

In 1994 [Nick Szabo](#) (cryptographer) first coined the term "smart contract."

The key difference with smart contracts is that it is a decentralized system accessible to anyone, that doesn't require any intermediary party or costs.

Smart contracts

- Smart contracts are executed by all nodes in the network
- Smart contracts include business logic and can automatically
 - Verify conditions
 - Check external information sources
 - Automate processes
- Because of this logic we can now not only register (historic) and simple transactions but also manage future rights & obligations (for example the right to future cash flows or access to information)

Ethereum

- Multi purpose platform
- PoW consensus

Ethereum Virtual Machine

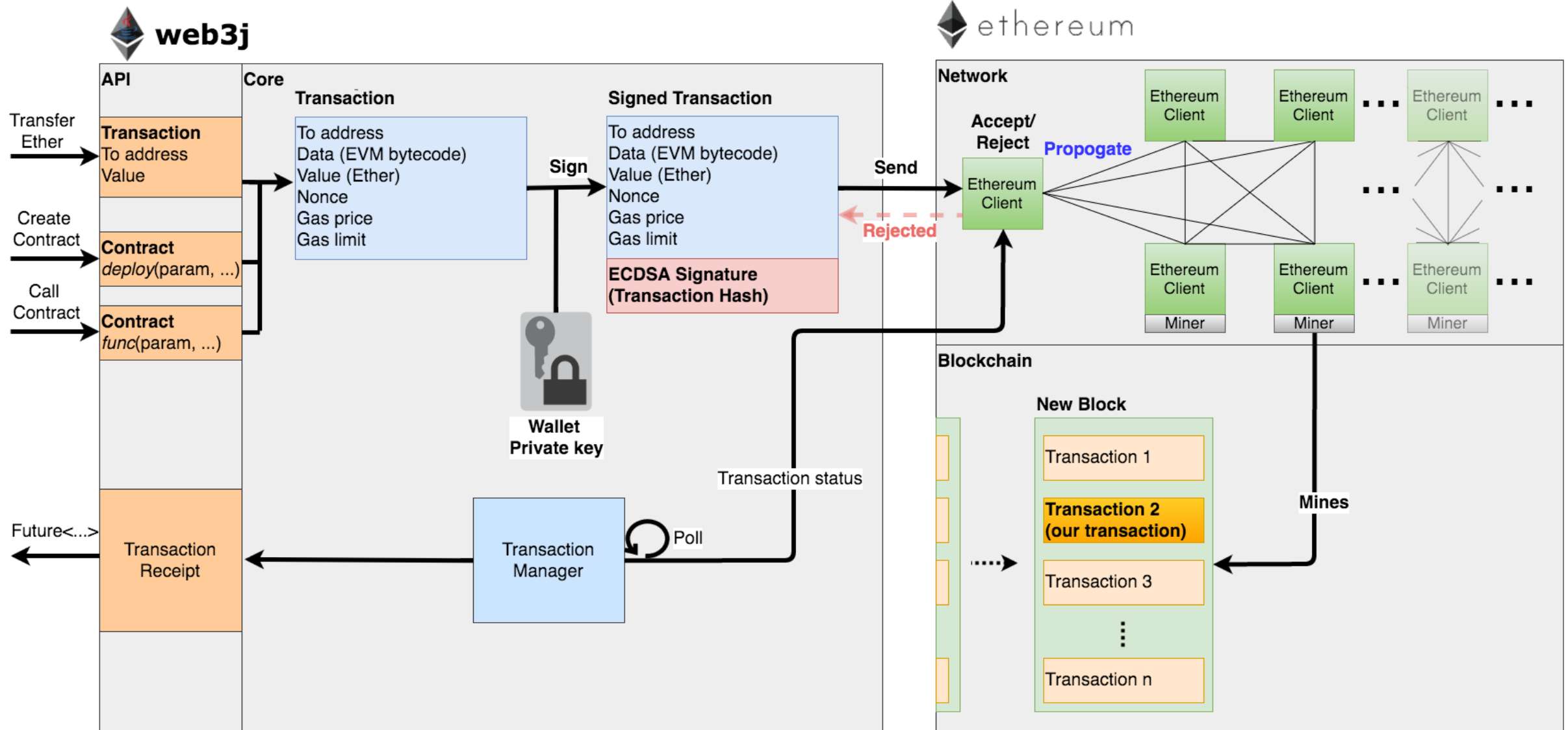
- Stack, Heap, environment variables, event, logs, sub-calling

Solidity

- Turing complete
- Gas limit (Halting problem)

JSON-RPC API

- JavaScript & Java libraries



Platform comparison

Platform	Consensus	Confidentiality	Smart contracts
BitCoin	PoW (SHA256)	None	BitCoin Scripts
Ethereum	PoW	None	Solidity / EVM
Corda	Pluggable	Selective broadcasting	Java/Kotlin (fully deterministic JVM)
HyperLedger Fabric	Pluggable	Transactions shared only with validator ('s)	Java/Go (standard JVM)
Sawtooth Lake	PoET	None	Yes
Quorum	Pluggable	Private transactions	Solidity / EVM

The impact of Blockchain on you!

```

1  contract Bank {
2
3      // Record of all balances (in wei).
4      mapping (address => uint256) public userBalances;
5
6      function getBalance(address user) constant returns(uint) {
7          return userBalances[user];
8      }
9
10     function deposit() payable {
11         userBalances[msg.sender] += msg.value;
12     }
13
14     function executePayment(uint256 amount, address to) payable {
15
16         // Only allow transfers from the message sender.
17         address from = msg.sender;
18
19         if (amount > userBalances[from]) {
20             throw;
21         }
22         if (!to.call.value(amount)()) {
23             throw;
24         }
25         userBalances[from] -= amount;
26     }
27 }

```

```

109
110     function () payable {
111
112         if (attackCount < attackCountMax) {
113
114             attackCount++;
115             vulnerableBank.executePayment(amount, this);
116         }
117     }

```

```
1  var filesystem = require("fs"),
2      Web3 = require('web3');
3
4  var web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8080"));
5
6  var abiString = filesystem.readFileSync("compiledContract/abi/VulnerableBank.abi", "utf8");
7  var Bank = web3.eth.contract(JSON.parse(abiString));
8  var bank = Bank.at("0xf1b89c99c0e3a6d2c138a850d8cbf4b51b938a6f");
9
10 bank.deposit({
11   from: web3.eth.accounts[0],
12   gas: 300000,
13   value: 20000000
14 }, (error, txhash) => {
15
16   if(error) {
17     console.warn("ERROR confirming deposit: " + error);
18   } else {
19     console.log("Deposit-TX successfully sent.");
20   }
21 });
```

Software quality: Formal Verification

- Formal Verification

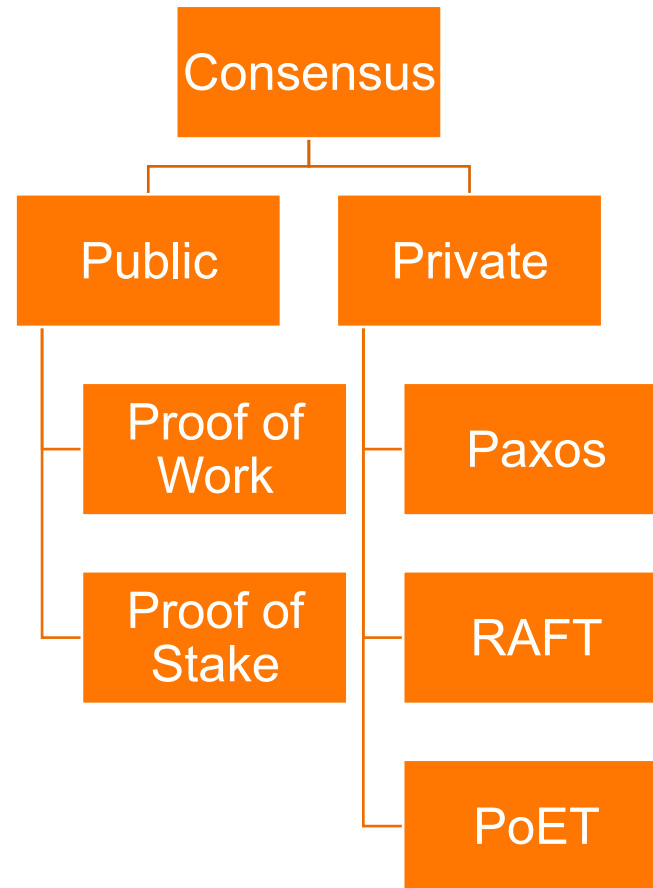
- *Formal proof of correctness for all possible inputs.*
- *2 ways:*
 - *Add formal specification to a regular language*
 - *Use a purpose built language: OCaml or Ada.*
- *Aviation standards allow to replace tests by formal verification: DO-178 (B & C)*

- Limitations

- *Huge overhead*
- *Halting problem*
- *External calls.*

```
byte[] a; /* The array a is sorted */  
/*@ invariant  
    (\forall int i; 0 <= i && i < a.length-1;  
        a[i] < a[i+1]);  
@*/
```

Consensus algorithms



Blockchain @ING!



Maternal
Tutorials
Box
4 of 12

in
Box
Box
1 of 12

Minicraft
Box
1 of 12

Stop
Motion
Box
9 of 12

Cats in
Boxes
Box
4 of 12

How to
Open
Things

Lady
Gaga
Parodies

Low Fat
Chocolate
Milk



Blockchain examples


uport

DEVELOPERGITHUBGITTERSUPPORTWHITE PAPERSIGN UP FOR ALPHA

DECLARE DIGITAL INDEPENDENCE

uPort is an open source software project to establish a global, unified, sovereign identity system for people, businesses, organizations, devices, and bots.

SIGN UP FOR ALPHA





GUTS

say farewell to ticket fraud and disgraceful secondary ticket prices

GUTS is a ticketing system which uses blockchain technology to register ownership of SMART-tickets. GUTS makes ticket fraud impossible. The ticket can only be (re)sold at a fixed price, so no more disgraceful prices for secondary tickets.

LEARN MORE





Ujo

We're building a home for artists that allows them to own and control their creative content and be paid directly for sharing their musical talents with the world.

We will be at SUMMIT AT SEA

Bahamas

9 NOV

Home

The Problem

Tiny Human

The Future

Blog/Contact

Team



followmyvote.com

Get Involved ▾Our Technology ▾FAQ ▾News ▾Knowledge Center ▾Log In ▾


Introducing a secure and transparent online voting solution for the modern age:

FOLLOW MY VOTE

Join Our List Of Supporters!

Enter Your Email

Select Country



everledger

Home API Timeline Smart Contracts

sign in via twitter

PROTECTION.

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

BBC on Bitcoin & The Bloc...

Blockchain @ING

- Understand the technology:
 - Platform evaluations
 - Fundamental technology (crypto, consensus etc.)
- Develop Blockchain applications
 - Trade Finance

Questions?