AGENDA

Exploring blockchain applications

20 Blockchain overview

10 Smart Contracts

5 Etherscan tour

40 Live Coding

5 Next steps

10 Discussion
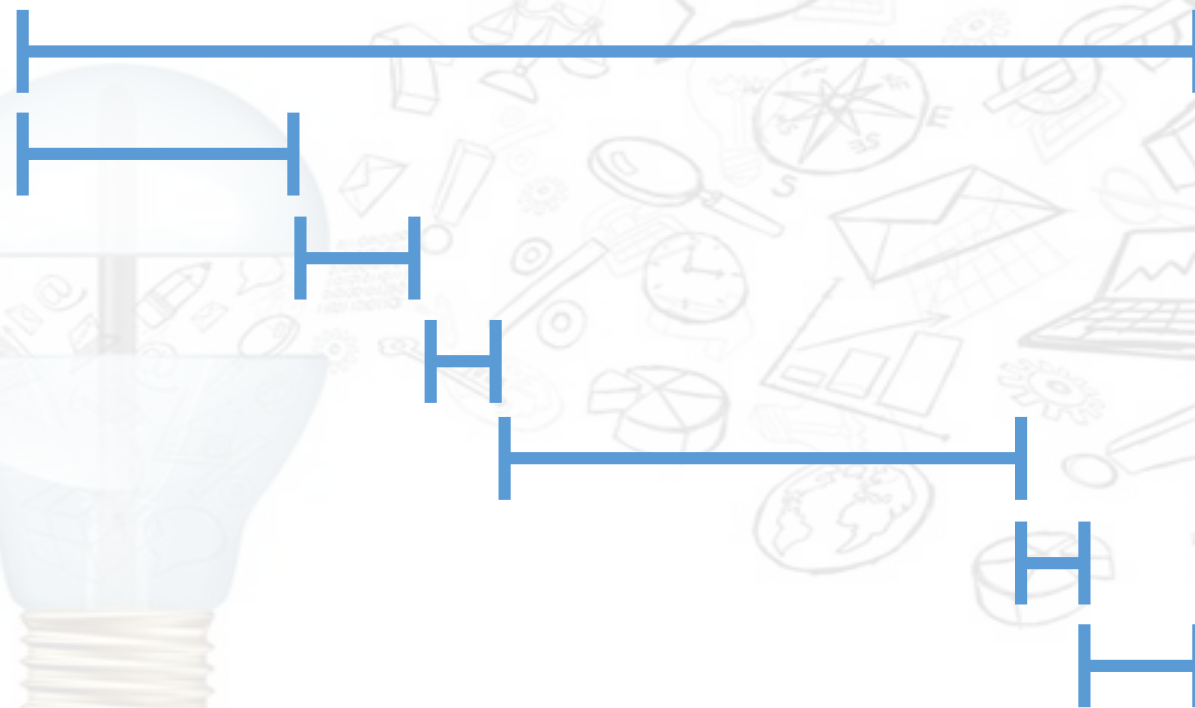
BLOCKCHAIN OVERVIEW

Gartner Hype Cycle for Emerging Technologies, 2017

Connected Home
Deep Learning
Virtual Assistants
IoT Platform
Machine Learning
Smart Robots
Autonomous Vehicles
Nanotube Electronics
Edge Computing
Cognitive Computing
Augmented Data Discovery
Blockchain
Smart Workspace
Commercial UAVs (Drones)
Conversational User Interfaces
Brain-Computer Interface
Cognitive Expert Advisors
Volumetric Displays
Quantum Computing
Digital Twin
Serverless PaaS
5G
Human Augmentation
Neuromorphic Hardware
Enterprise Taxonomy and Ontology Management
Deep Reinforcement Learning
Virtual Reality
Software-Defined Security
Artificial General Intelligence
4D Printing
Augmented Reality
Smart Dust

Plateau will be reached in:
- less than 2 years
- 2 to 5 years
- 5 to 10 years
- more than 10 years

Expectations

Innovation Trigger | Peak of Inflated Expectations | Trough of Disillusionment | Slope of Enlightenment | Plateau of Productivity

As of July 2017

Time

Trust the system

Remove intermediaries from the value exchange process

Disrupt the status quo

Economic   Social   Information   ?

Foundational

BLOCKCHAIN: THE HISTORY

Nick Szabo
Bit Gold

Vitalik Buterin
A Next-Generation Smart Contract and
Decentralized Application Platform

1982   1997

1998   2008   2013

David Chaum
Blind signatures and e-cash

Adam Back
hashcash

Satoshi Nakamoto
Bitcoin: A Peer-to-Peer Electronic
Cash System

digital signatures
proof of work
decentralization
blockchain
scripting
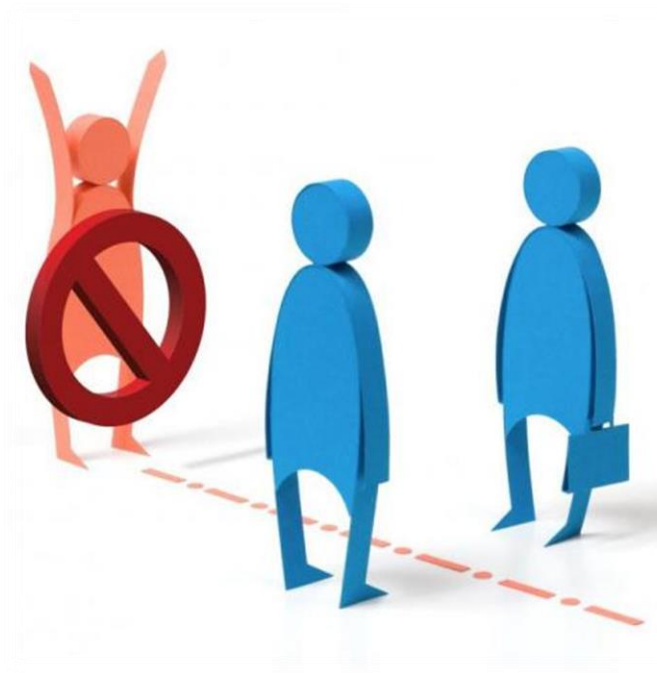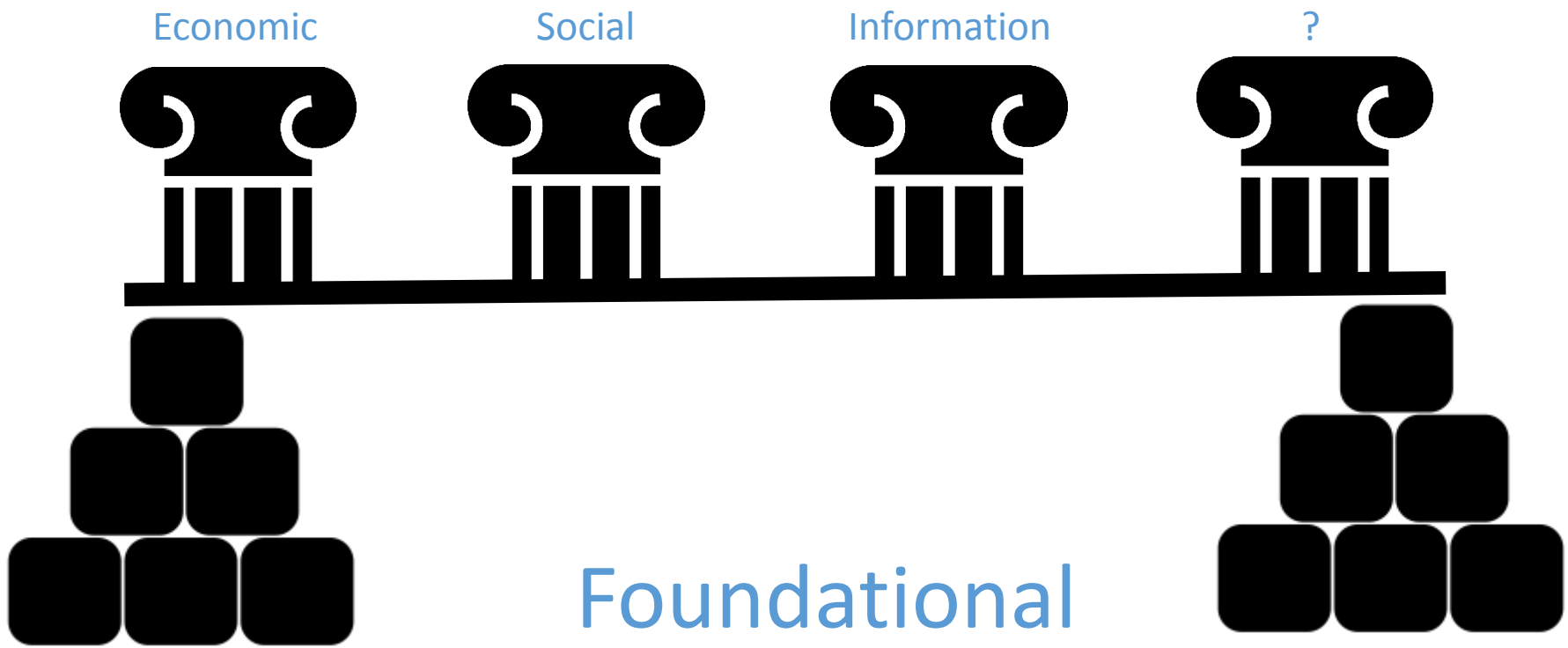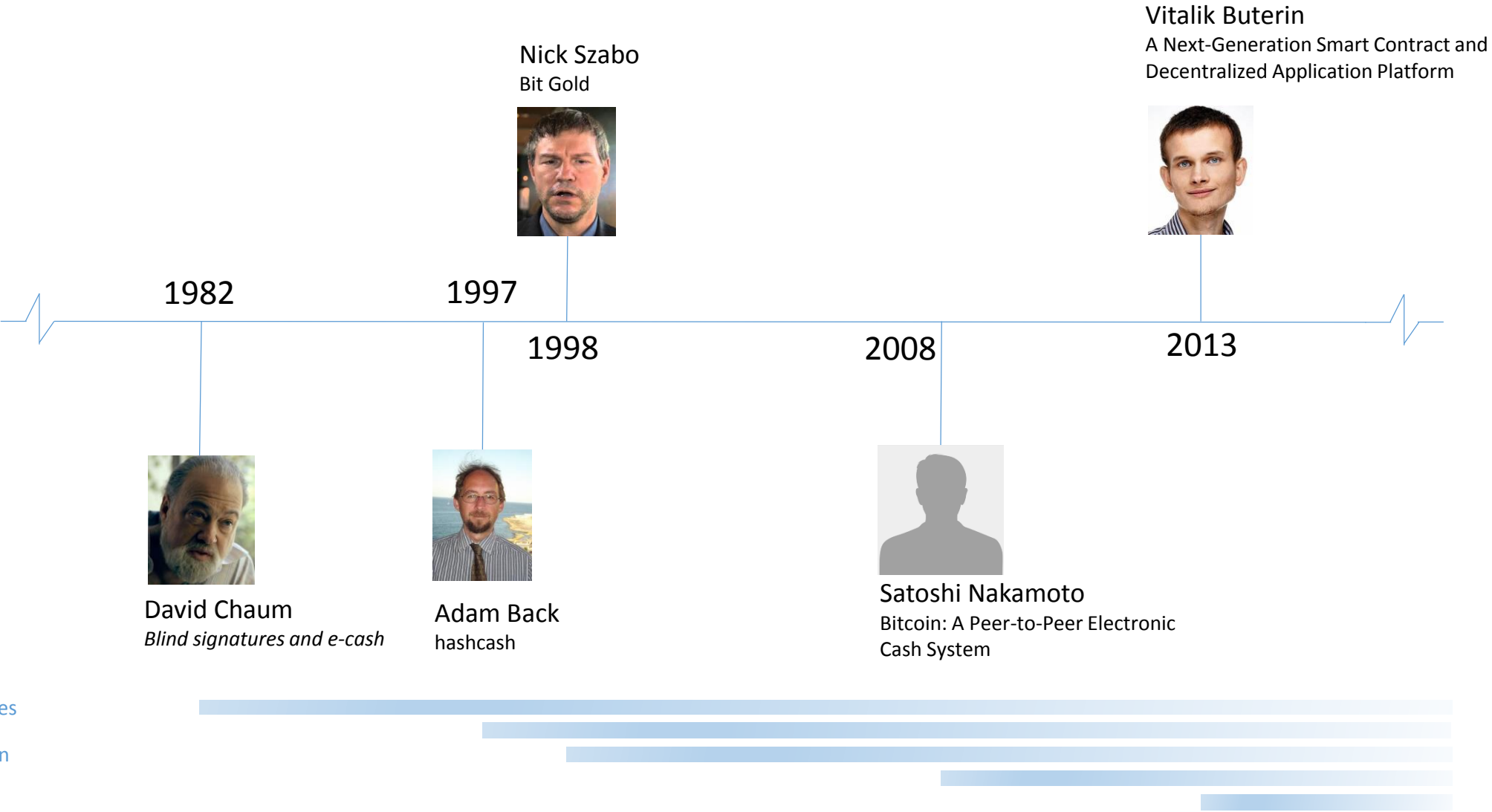
PUBLIC BLOCKCHAINS
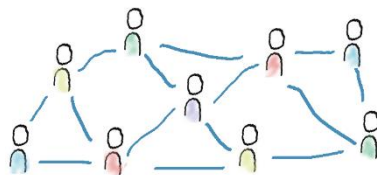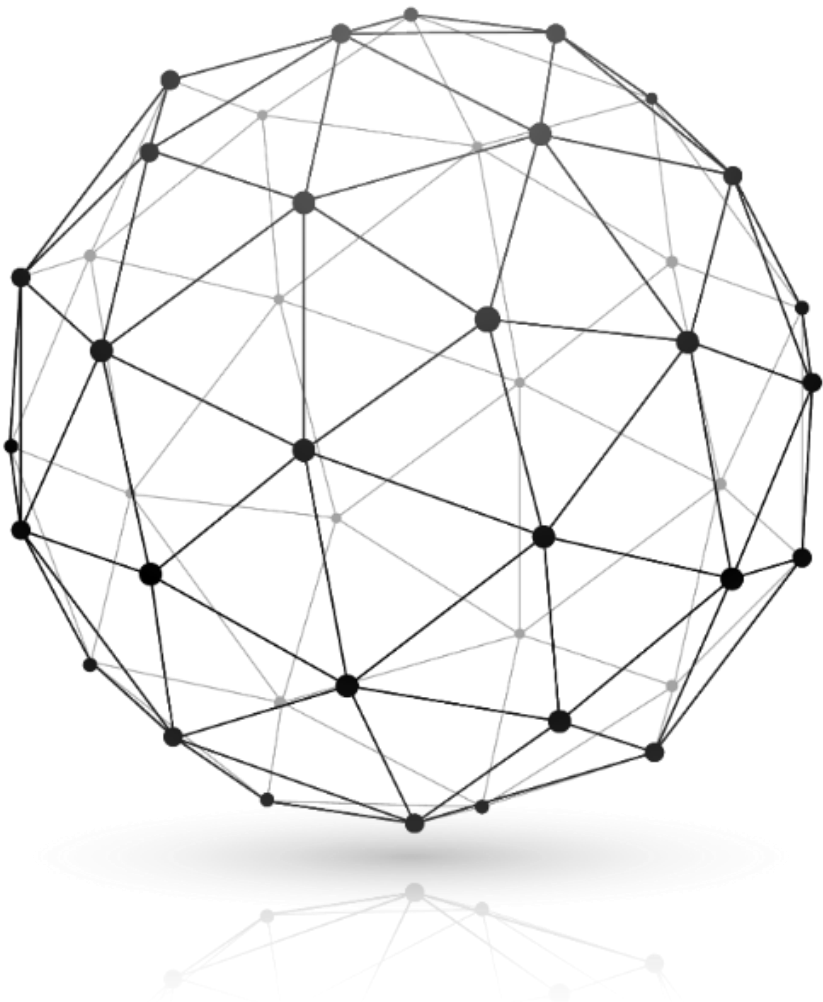
Decentralized

Censorship resistant

Robustness

Trustless

Immutable

BUT...

Blockchains by themselves are a far less efficient computer and database than technology that has existed for over 40 years...
- Vitalik Butterin

Actually, about a:
- 1,000,000x the overhead
- 1,000,000x the expense

BLOCK-*CHAIN*

Block

- BlockNumber: int
- Data: byte[]
- PreviousBlockHash: byte[]
- Hash: byte[]
- Nonce: int

Block #0	Block #1	Block #2	Block #...	Block #n	Block #n+1

Block #0	Block #1	Block #2	Block #...	Block #n	Block #n+1
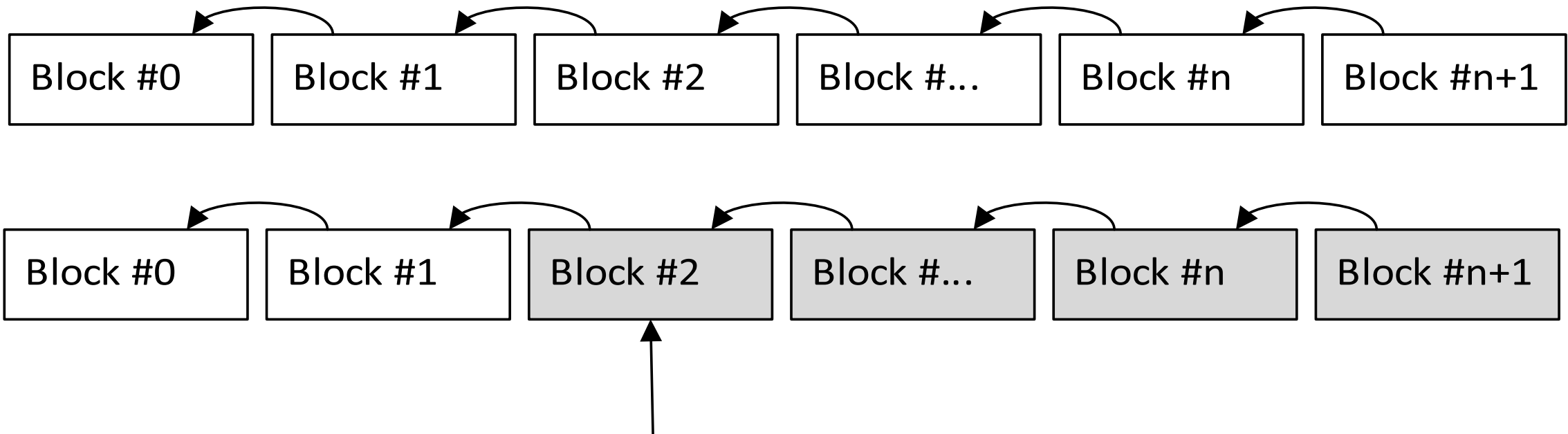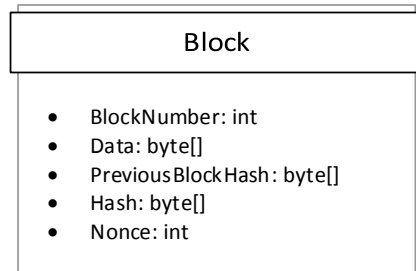
REACHING CONSENSUS

Proof **o**f **W**ork

requires processing time to complete,
but is **easy to check**
whether the work is done correctly

Proof **o**f **S**take

selects participants with the **highest stakes** as validators, assuming that the highest stakeholders are **incentivized** to ensure a transaction is processed.

Proof **o**f **A**uthority

uses **identity** as the sole verification of the **authority to validate**

Blocks are *mined*

Blocks are *minted*

Blocks are *sealed*

PERMISSIONED VS PUBLIC

	Permissioned (private)	Permission less (public)
Usage	Enterprise level systems, consortiums	Open access applications, permission less innovation
Who can join?	🔒 Access authorization	🔓 Open to anyone
Validators	**Preselected validators**	**Decentralized validation**
	Proof of Authority	Proof of Work
		Proof of Stake
Performance		
Implementations	Quorum HYPERLEDGER ethereum	NEO ethereum Bitcoin

OXFORD BLOCKCHAIN STRATEGY FRAMEWORK

YES   NO

☐ ☐ Is there a predictable, repeatable process that lends itself well to automation?

☐ ☐ Is there an ongoing or long-running transaction or process, rather than a process that occurs only once?

☐ ☐ Are there multiple stakeholders in this process or value chain?

☐ ☐ Is the role of reconciling disparate data usually played by one party or a limited number of parties?

☐ ☐ Remembering that value is not only monetary, is there an element of value transfer?

☐ ☐ Is there value in an immutable record? Or is an immutable record a requirement?
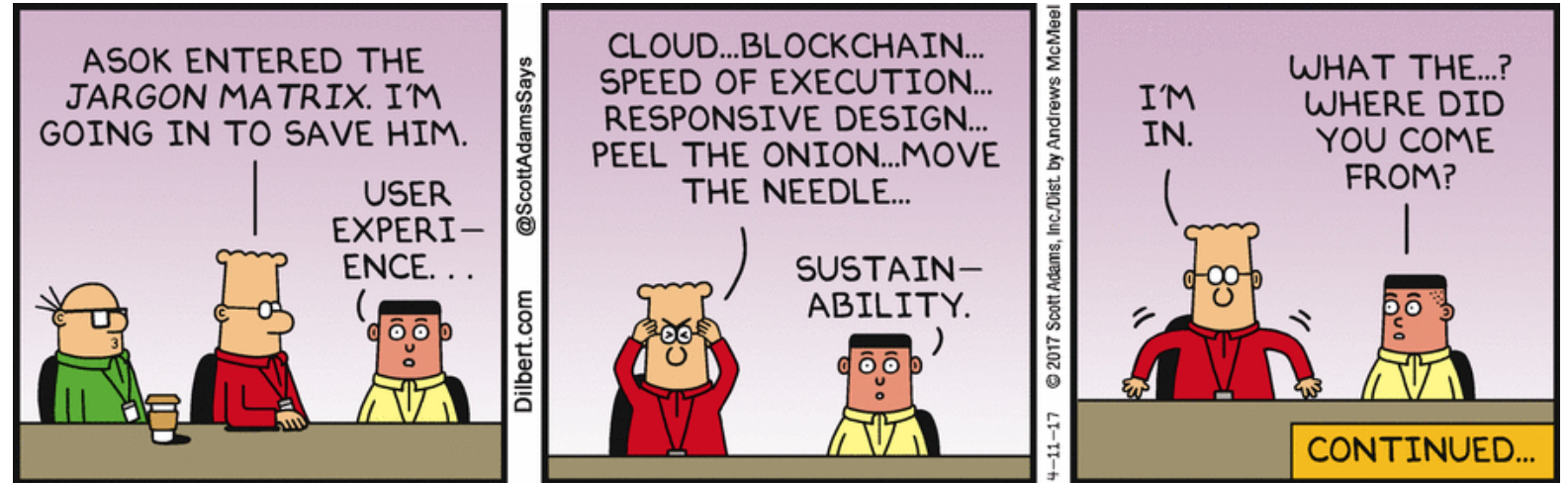
SMART CONTRACTS
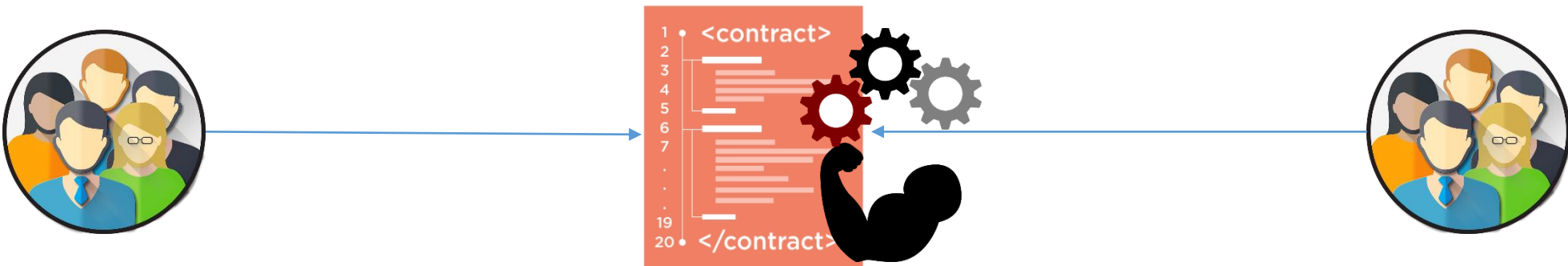
```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

    /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```
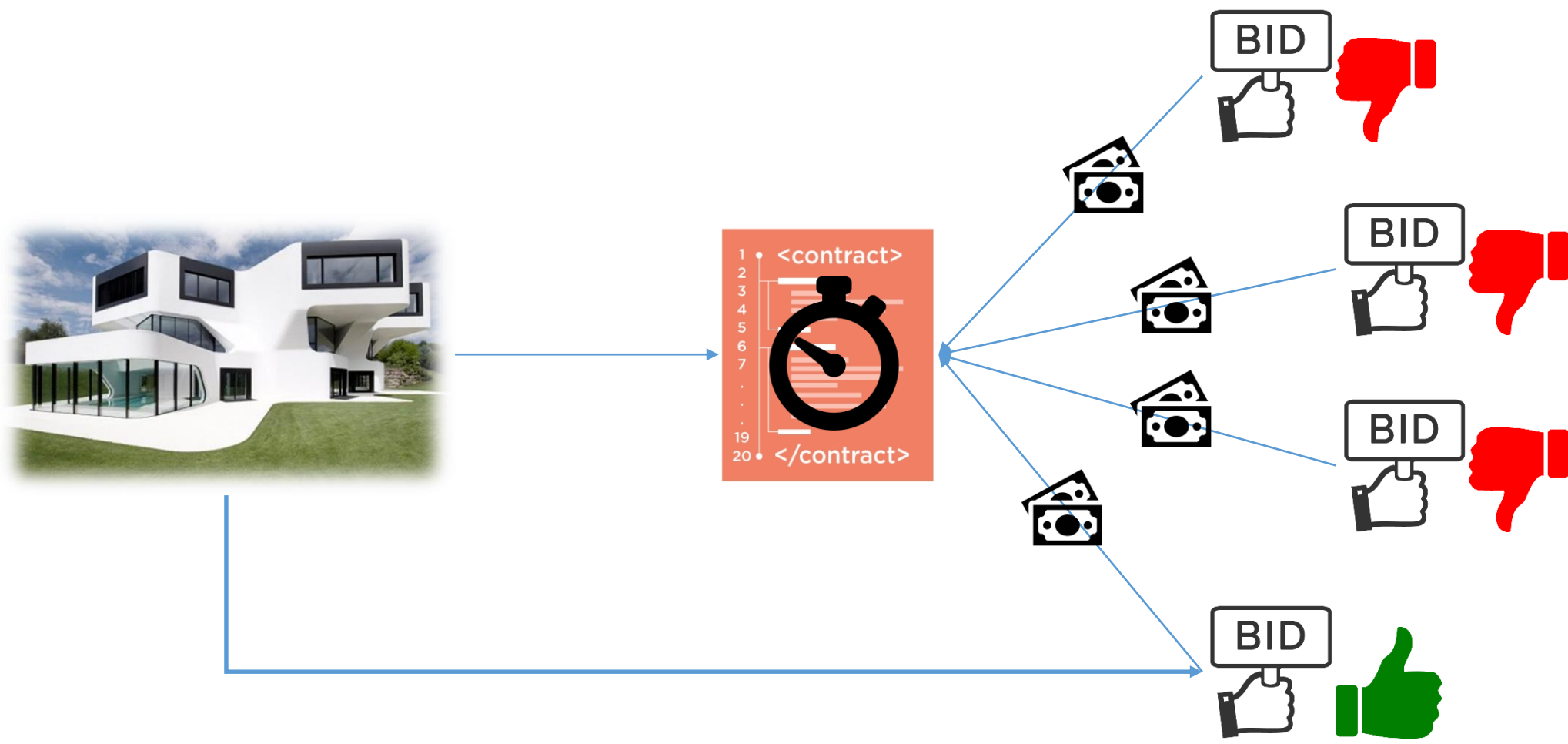
Industry examples

Shipping and logistics

(Container) contents

Documents

Transit tracking

Transfer/handoff

Exceptional events

Asset lifecycle and history

Parts history

Maintenance/repair history

Events

Transfer of ownership

Supply chain

Ingredients

Manufacturers

Trackability

Traceability

Temperature controlled supply chains
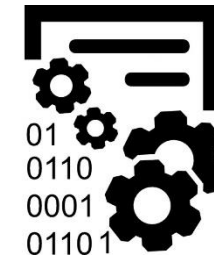
Data

Provenance / Quality

Ownership

Monetization

Ethereum Virtual Machine (EVM)

Sandboxed

Turing complete

Executed by all

```
0x00    STOP        Halts execution
0x01    ADD         Addition operation
0x02    MUL         Multiplication operation
0x03    SUB         Subtraction operation
0x04    DIV         Integer division operation
0x05    SDIV        Signed integer
0x06    MOD         Modulo
0x07    SMOD        Signed modulo
0x08    ADDMOD      Modulo
0x09    MULMOD      Modulo
0x0a    EXP         Exponential operation
0x0b    SIGNEXTEND  Extend length of two's complement signed integer
```

Solidity

```solidity
pragma solidity ^0.4.18;

contract Multiplication {

    int multiplicationFactor;

    function Multiplication(int factor) public {
        multiplicationFactor = factor;
    }

    function Multiply(int number) public constant returns (int)
    {
        return number * multiplicationFactor;
    }

    function setFactor(int factor) public
    {
        multiplicationFactor = factor;
    }
}
```

Opcodes

PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE ISZERO PUSH2 0xF JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x40 MLOAD PUSH1 0x20 DUP1 PUSH2 0x126 DUP4 CODECOPY DUP2 ADD PUSH1 0x40 MSTORE DUP1 DUP1 MLOAD SWAP1 PUSH1 0x20 ADD SWAP1 SWAP2 SWAP1 POP POP DUP1 PUSH1 0x0 DUP2 SWAP1 SSTORE POP POP PUSH1 0xE5 DUP1 PUSH2 0x41 PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN STOP PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT PUSH1 0x49 JUMPI PUSH1 0x0 CALLDATALOAD PUSH29 0x100000000000000000000000000000000000000000000000000000000 SWAP1 DIV PUSH4 (…)

Bytecode

6060604052341561000f57600080fd5b60405160208061012683398101604052808051906020019091905050806000819055505060e58061004160003960
00f300606060405260043610604957600035
7c010000000000000000000000000000000000000000000000000000000000900463ffffffff168063c7fbc2f81460
4e578063d76ab67f146082575b600080fd5b341560585857600080fd5b606c6004808035906020019091905050506060a2565b6040518082815260200191505060604
05180910390f35b3415608c57600080fd5b60a060048080359060200190919050505060af565b005b6000805482029050091905056b8060000819055050560
0a165627a7a72305820a1f70a08c99fc26697344bfdec6fe2501cb58bef1472adb413f2040a89ef69410029

Gas

- Decoupled concept of transaction fees
  - Each transaction or EVM operation costs a fixed amount of gas
- Compensates the network
  - Makes Denial of Service prohibitively expensive
- Halting problem
  - Gas limit
- Gas is priced
  - Market determined
- Gas price is included in transaction
  - Miners seek out the most profitable transactions to include
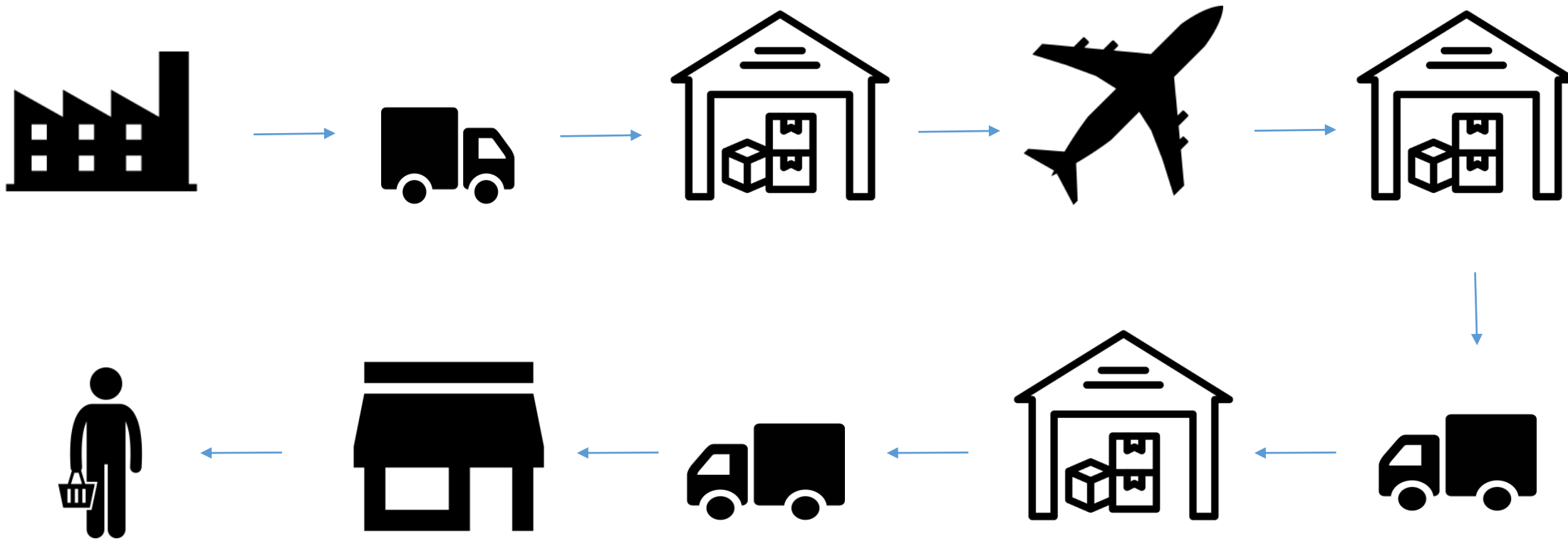- Gas fees are collected by the miners

COLD CHAIN

Cold chain

Product »

| Ethereum Dapp | | | | |

- Manufacturer
- Edge Historian — Sensor
- Edge Historian — Sensor
- Edge Historian — Sensor
- Customer

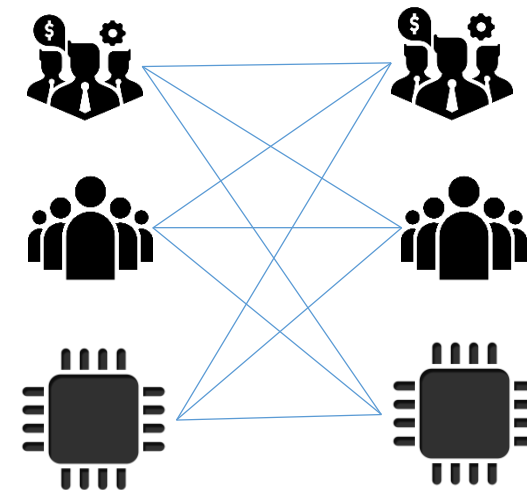Trip segment　　Trip segment　　Trip segment　　Trip segment　　Trip segment
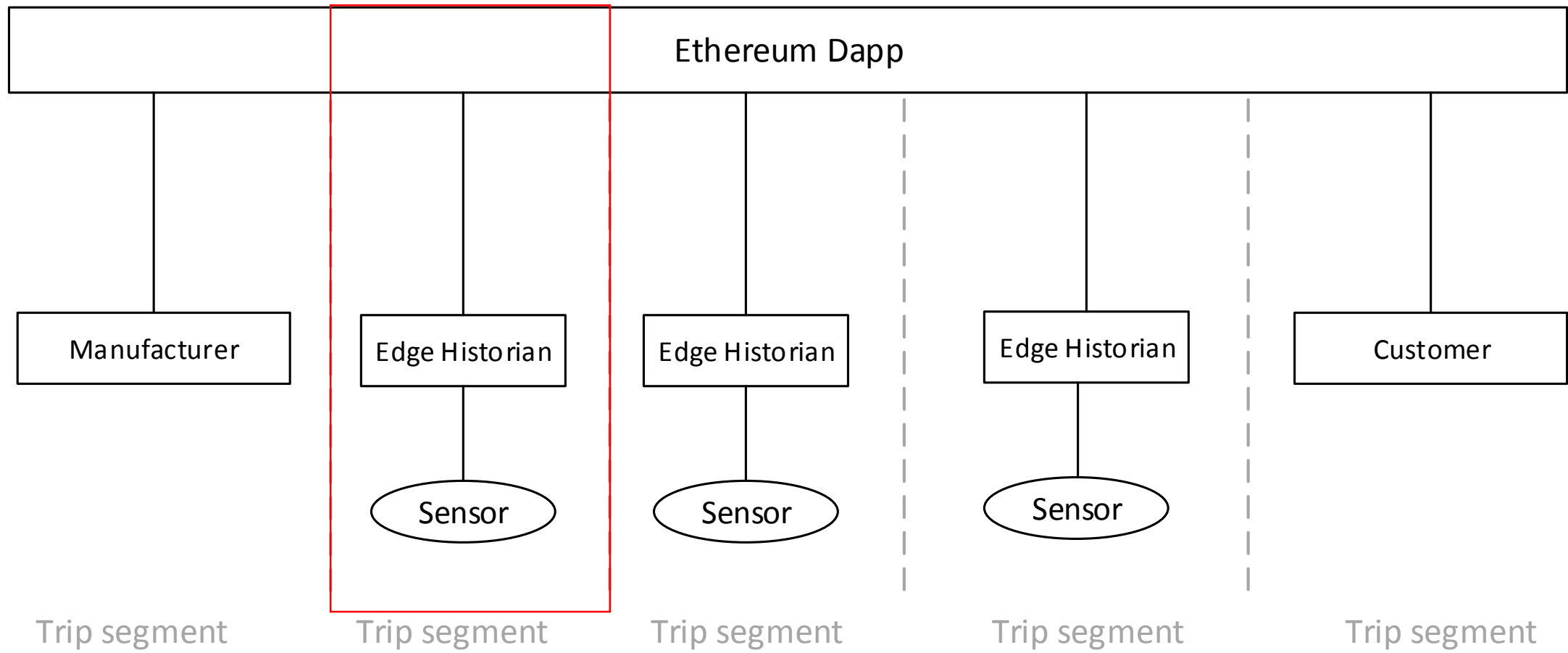
LET'S CODE!

NEXT STEPS

Blockchain …

✓ … Will not replace the PI System, *the cloud* or databases in general
   ✓ Not a panacea

✓ … Will have a huge impact on how we create and maintain relationships

✓ … Slightly uncomfortable
   ✓ Huge attention to decentralization
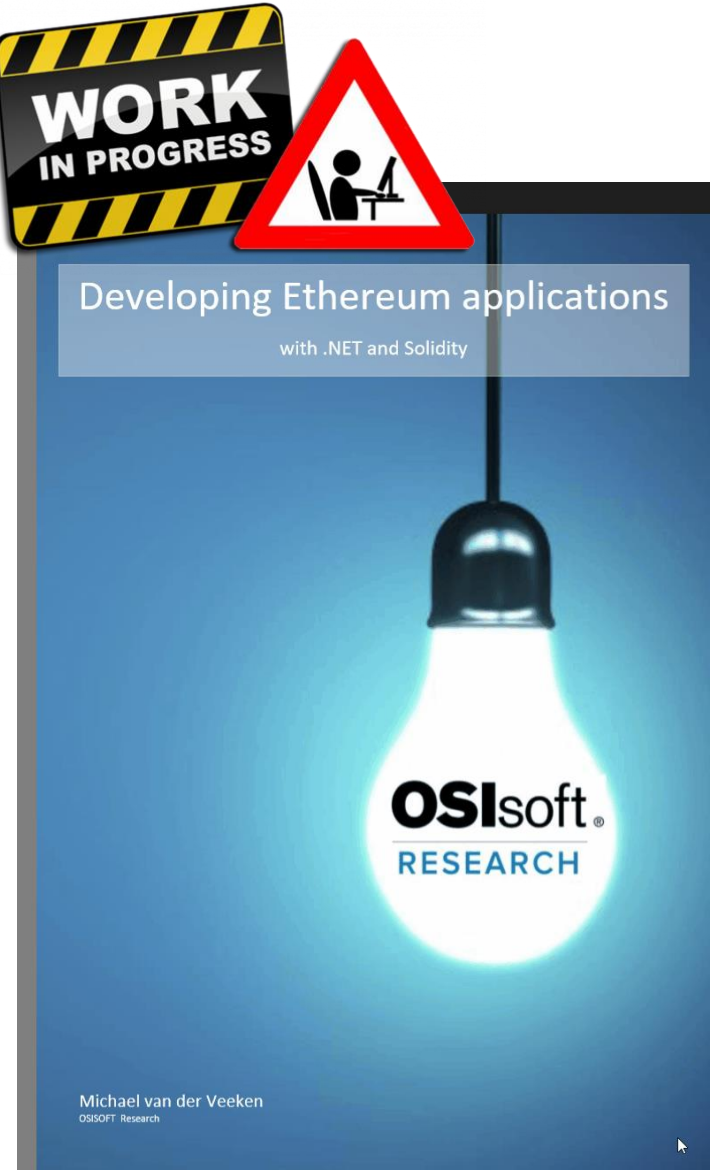
✓ … Is happening between now and 5 years

Blockchain can play a vital role in realizing
the Community Vision

- Take your time
- Understand the technology
- Be wary of the hype
- Do research

This is an **exciting** time

Developing Ethereum applications

with .NET and Solidity

OSIsoft®
RESEARCH

Michael van der Veeken
OSISOFT Research

https://goo.gl/FxrSM9

*Or you can give me your business card
and I'll send you the link*

LET'S DISCUSS TOGETHER

? How could blockchain apply to your industry?

? What blockchain projects or proof of concepts have already started in your organization?

? What would OSIsoft's role be to make these projects successful?

? How could blockchain be applied in the PI System?

? What would the best way be for us to engage?

THANK YOU