UNIVERSITY OF CAMBRIDGE

An Architecture that Addresses Scalability and other Issues of Smart Contracts and Blockchains: Research at the Computer Lab.

Carlos Molina-Jimenez

Carlos.Molina@cl.cam.ac.uk

http://www.cl.cam.ac.uk/~cm770/

Department of Computer Science and Technology:

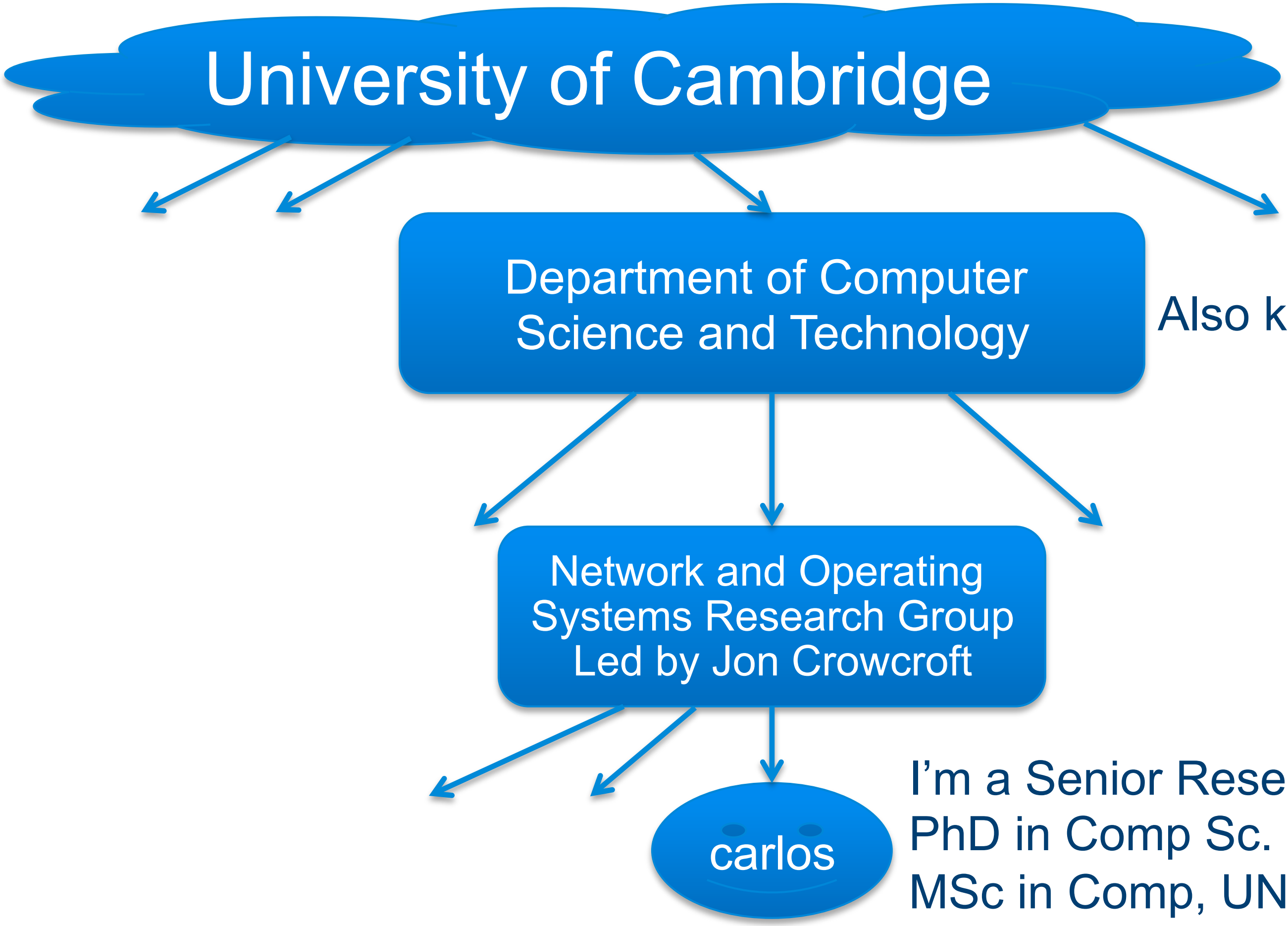
Computer Laboratory

Presented to Club de Innovacion Chileno, Cambridge 18 Jun 2018

Structure of this Presentation

- My research background.
- Introduction to Bitcoin to explain why it has a big generated.
- Relationship between smart contracts and blockchain.
- Potential applications of blockchain and smart contarts.
- Pending research questions about blockchain and smart contracts.
- My current research and progress on blockchain and smart contracts.
- Conclusions.

My Research Group



University of Cambridge

Department of Computer Science and Technology

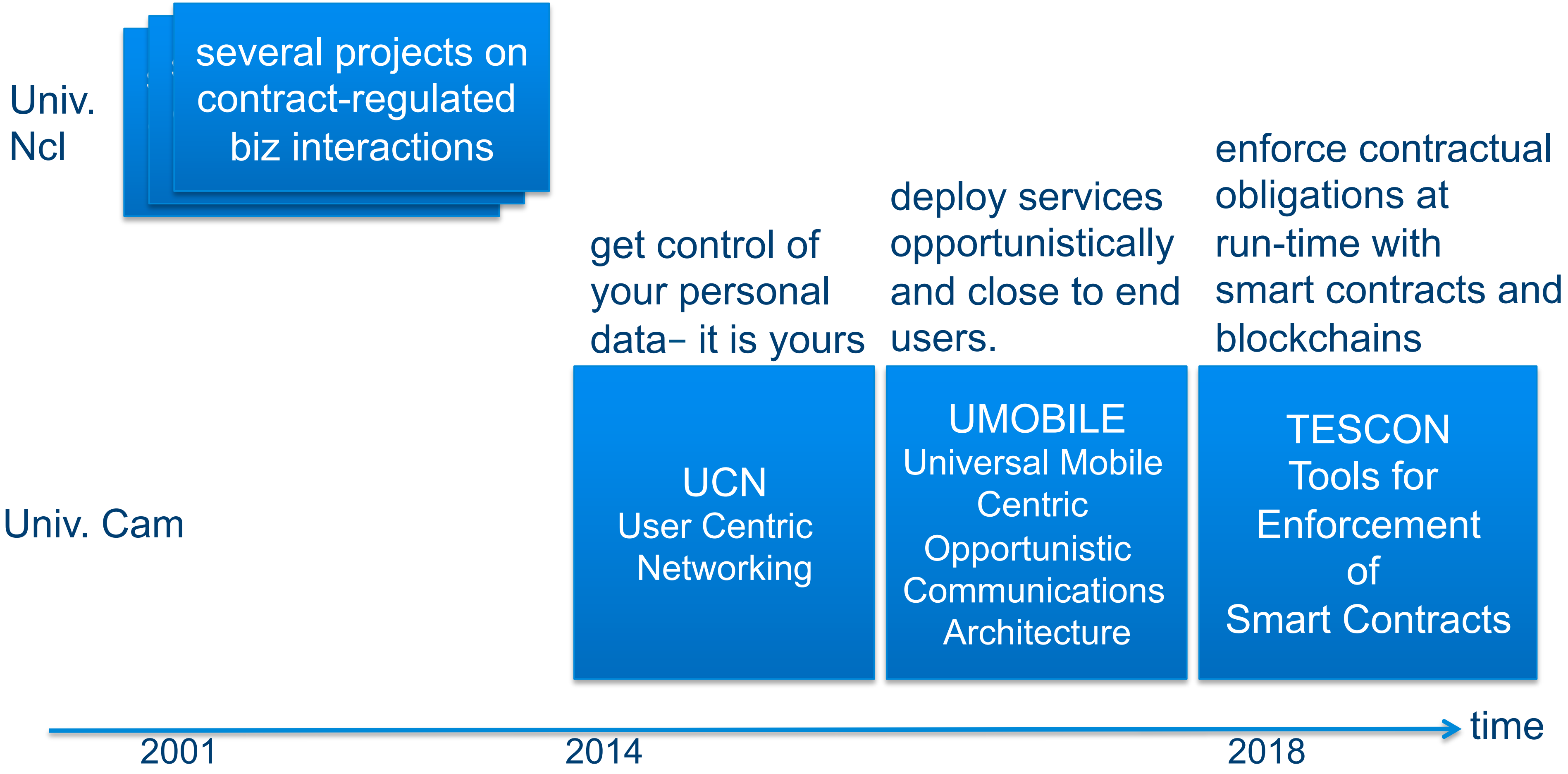
Network and Operating Systems Research Group
Led by Jon Crowcroft

carlos

Also known as the Computer Laboratory

I’m a Senior Research Associate.
PhD in Comp Sc. Univ of Newcastle, UK,
MSc in Comp, UNAM Mex,
Beng Polytechnic Institut Odessa.

My Research Experience



Univ. Ncl

several projects on contract-regulated biz interactions

Univ. Cam

get control of your personal data– it is yours

UCN
User Centric Networking

deploy services opportunistically and close to end users.

UMOBILE
Universal Mobile Centric Opportunistic Communications Architecture

enforce contractual obligations at run-time with smart contracts and blockchains

TESCON
Tools for Enforcement of Smart Contracts

2001

2014

2018

time

Bitcoin---what is it and who needs it?

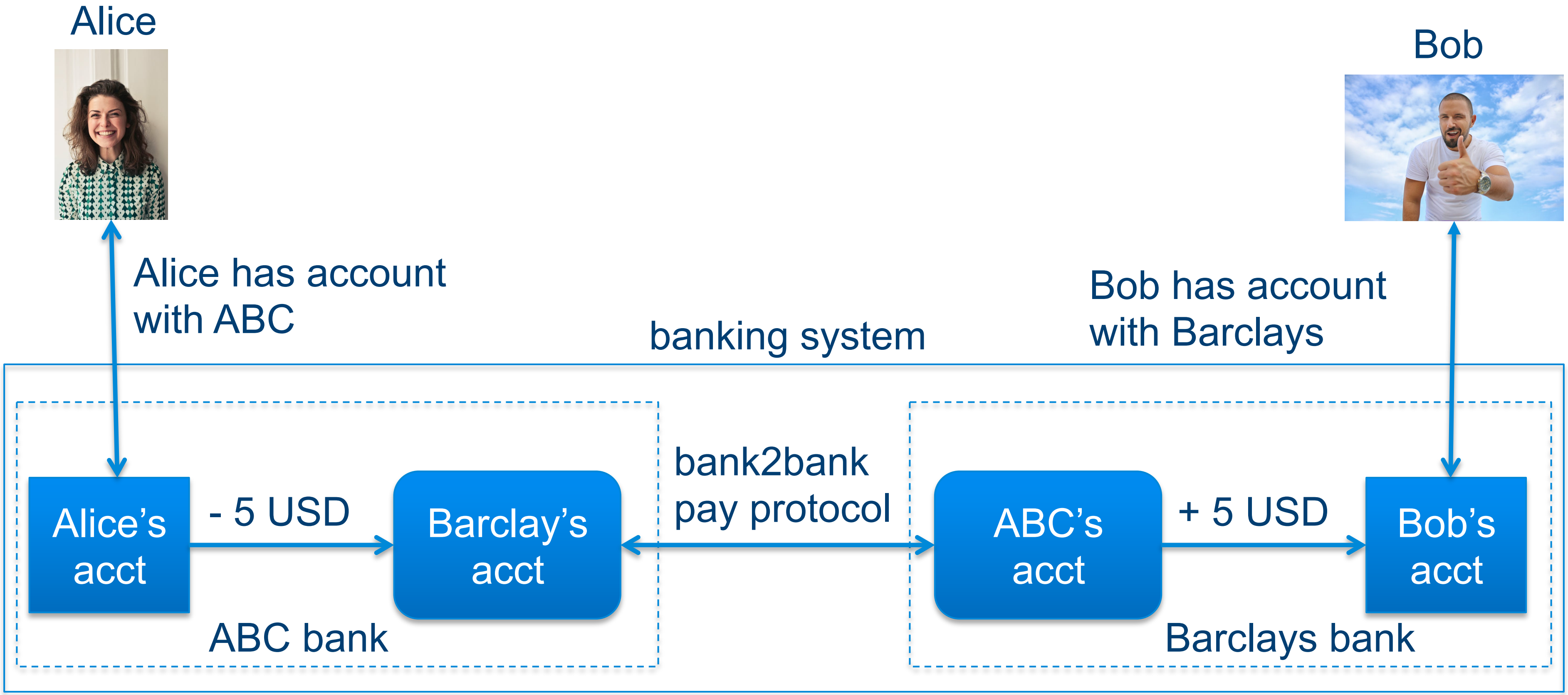
- Bitcoin is a sotfware platform that allows people to send electronic money (cryptocurrency) to each other.
- Who needs such a platform?
- **Me, I need it to send money to Mexico!!!**
  - I will use a money transfer example to introduce Bitcoin, cryptocurrency, blockchain and smart contracts.

Motivation: I’d been invited to a XV b/day party!

Contributions in **cash** are very welcome!

World map
Arctic OCEAN
Arctic OCEAN
Arctic OCEAN
N
ALASKA (USA)
GREENLAND (DENMARK)
C A N A D A
R U S S I A
North Pacific OCEAN
North Pacific OCEAN
UNITED STATES OF AMERICA
North Atlantic OCEAN
MEXICO
K A Z A K H S T A N
M O N G O L I A
C H I N A
I N D I A
B R A Z I L
INDIAN OCEAN
A U S T R A L I A
South Pacific OCEAN
South Atlantic OCEAN
Antarctica
@Copyright MapsNWorld.com 2011
Map Not To Scale

Money transfer: Traditional Bank-mediated Approach



Alice

Bob

Alice has account with ABC

banking system

Bob has account with Barclays

Alice's acct

- 5 USD

Barclay's acct

bank2bank pay protocol

ABC's acct

+ 5 USD

Bob's acct

ABC bank

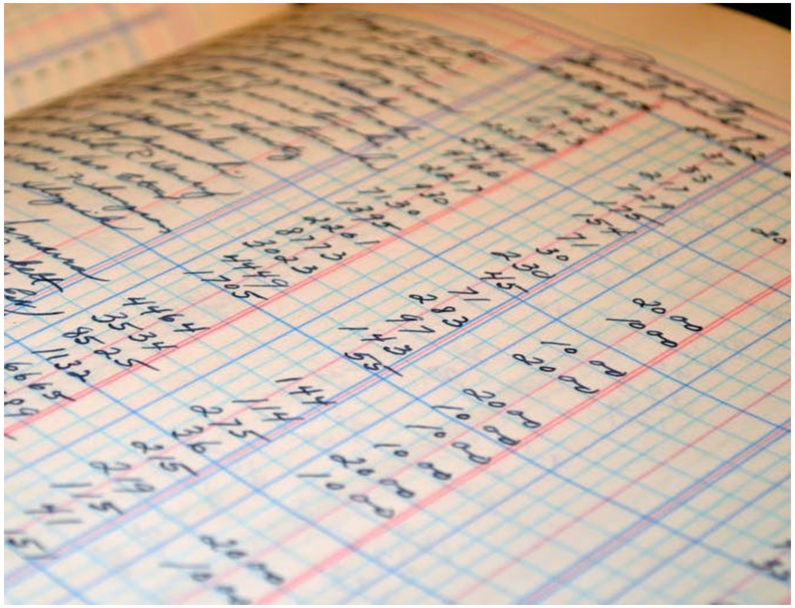
Barclays bank

What Role does the Bank Play?

- The bank is a centralised Trusted Third Party (TTP).
- This TTP solves several potential transaction problems:
  - Alice has enough money in her account to cover the transaction.
  - Alice does not spend the same coin two o more time (double spending).
  - The money is deposited in Bob’s account.

How does the Bank Look After Transactions?

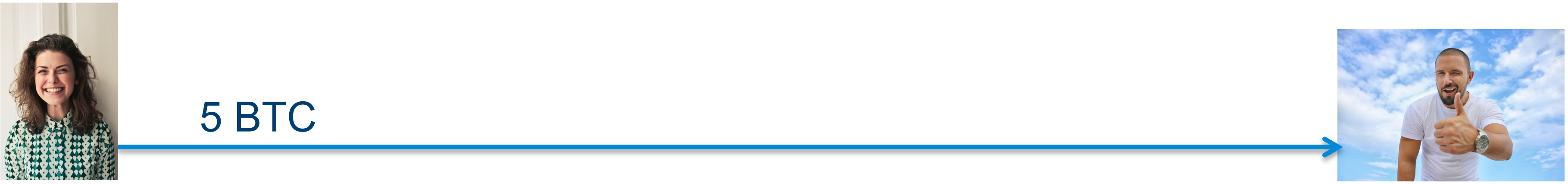
- It has a centralised ledger with records of all the transactions: it knows Alice’s and Bob’s balances and personal information (address, age,…)



Problems with Bank-mediated Transfers

- It takes ages (several days).
- There is a exchange rate that the bank abuses.
- The bank transaction fees (typically 15 to 30 pounds).
- It excludes people without bank accounts.

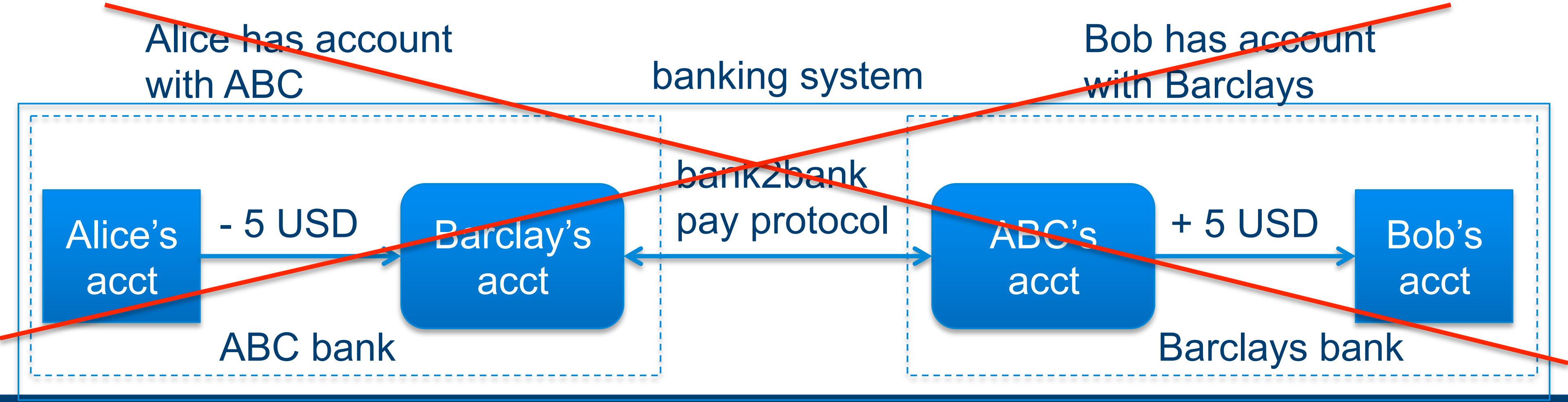
Bitcoin to the Rescue– Let us Get Rid of the Bank Said Satoshi in 2008.



Alice

5 BTC

Bob



Alice has account with ABC

banking system

Bob has account with Barclays

Alice's acct

- 5 USD

Barclay's acct

bank2bank pay protocol

ABC's acct

+ 5 USD

Bob's acct

ABC bank

Barclays bank

No Bank in The Middle

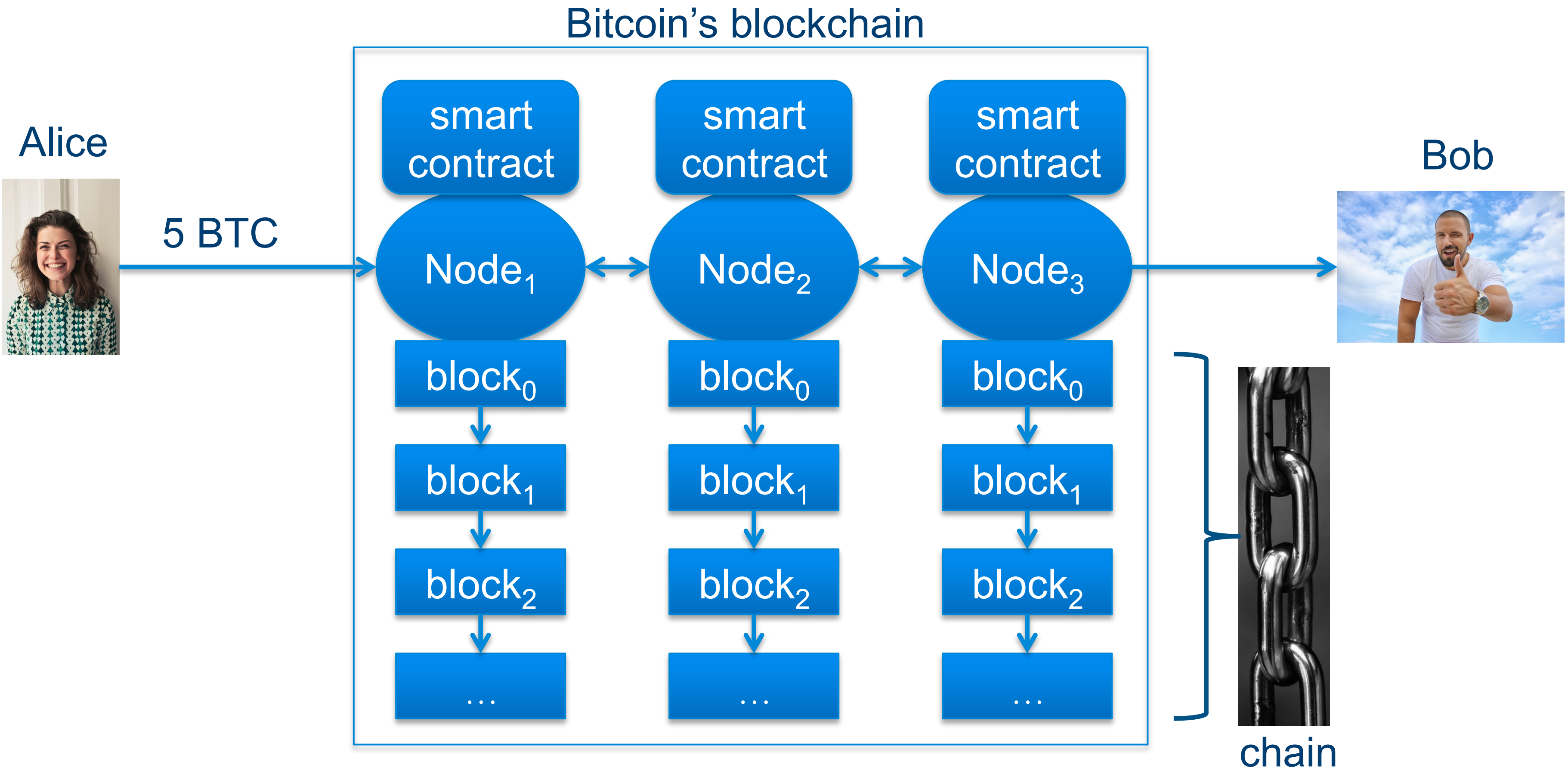
- No banks in the middle means goods things
  - person-to-person money transfer, that is, without the bank mediating between the two parties. Some people call it pee-to-peer.
  - Business: No transaction fees, no money transfer time, no abusive exchange rate, no need to have a bank account, no need to disclose my transaction habits to the bank, etc.
  - Technical: no dependency on the functionality of the bank that might suffer breakdowns.
- No bank in the middle means potential problems as well.
  - No guarding to control illegal Txs (see Silk Road case) , no body to resort to if I loose my money,….

How does Bitcoin Keeps Track of Transactions?---textual explanation

- It relies on a decentralised (distributed) data structure called the Decentrealised Ledger (DL) or the blockchain.
  - Indelible (append only).
  - Decentralised (replicated at several nodes).
- It runs consensus algorithms to sychronised the replicas with each other: ensures that eventually, all of them have identical information about all transactions.
- It uses cryptographic techniques (eg. public key technology) to identify senders and receivers of money.
- It runs a **smart contract**: a piece of code that ensure (enforce) that only valid transactions take place: right amount of money and to the right receiver.

How does Bitcoin Keeps Track of Transactions?---graphical explanation

- Bitcoin uses blockchain and smart contracts



Beyond Bitcoin’s Cryptocurrency

- Bitcoin’s cryptocurrencies was only the first application of blockchain and smart contracts.
- It was enough to generate commercial and research interest based on blockchain and smart contracts.
- Key Idea: if we managed to get rid of the bank, let us get rid of other parties that needlessly mediate interactions.
- Let us build the Internet of decentralised applications.

New business models (banking, health, …) and new computation paradigms, new…

Competition Joins the Race

- Bitcoin shook the banking and financial system.
- Competition appeared quickly
  - Blockchain platforms: Ethereum, Hyperledger, etc.
  - Blockchain-based applications: legalese, credits, sweetbridge, etc.

What Problems do Smart Contracts and Blockchain Solve—brief explanation?

- They can help build applications where
  - two or more remote parties interact with each other under certain rules
    - for ex. *operation cancellation is valid only if payment has been executed before.*
  - the parties do not trust each other.
  - storage of historical records are essential for examination.

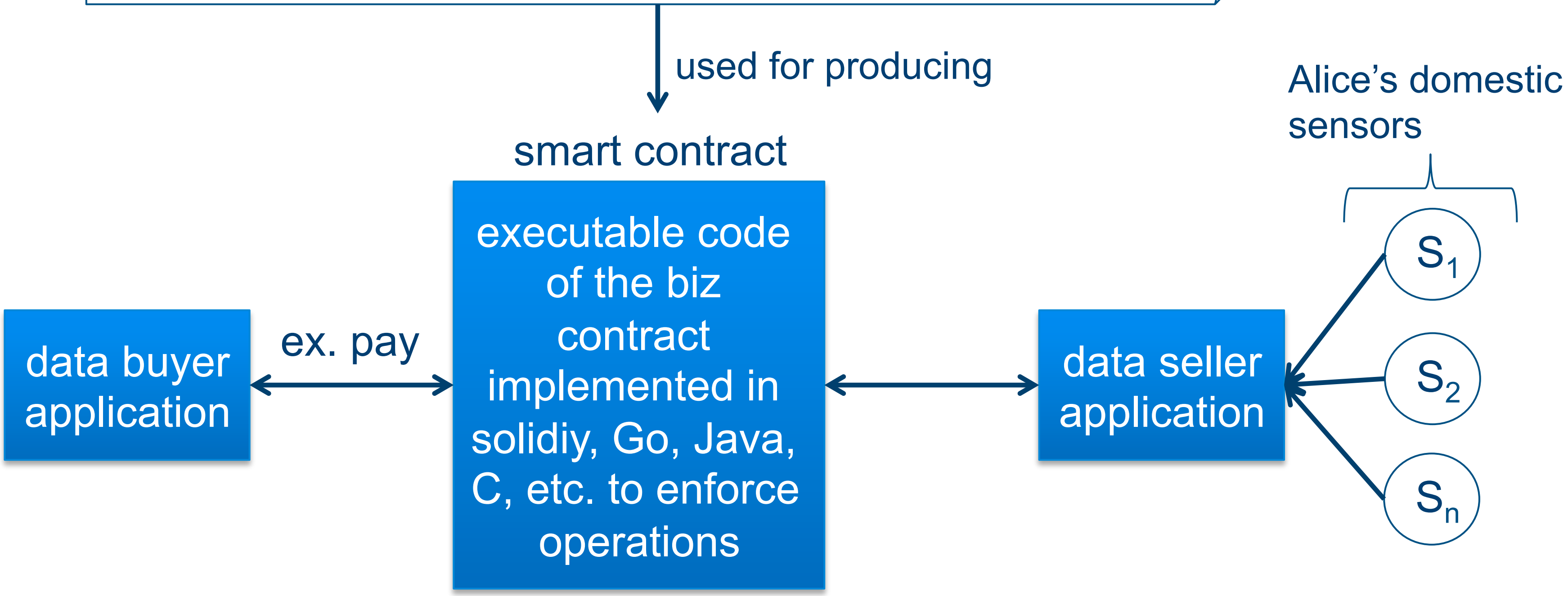
What Problems do Smart Contracts and Blockchain Solve—elaborated explanation?

- Blockchain can help when you need to build an application where
  - there are two or more independent parties (ex. companies) that collaborate in the execution of the application but they do not necessarily trust each other.
    - the parties are reluctant to trust and rely on a single party to mediate in the execution.
  - the application has a state (data) shared between the parties. For ex. buyer’s payment is pending, Alice has passed her final exam, Bob has been released from hospital, etc.
  - operations to alter the state are strictly allowed or disallowed depending on the history of previous operations.
  - transparency is essential: parties (possibly the general public) need means of accessing and verifying historical records.
- I will discuss some example of innovative applications that can be built on the basis of blockchain and smart contracts.

What is a Smart Contract?

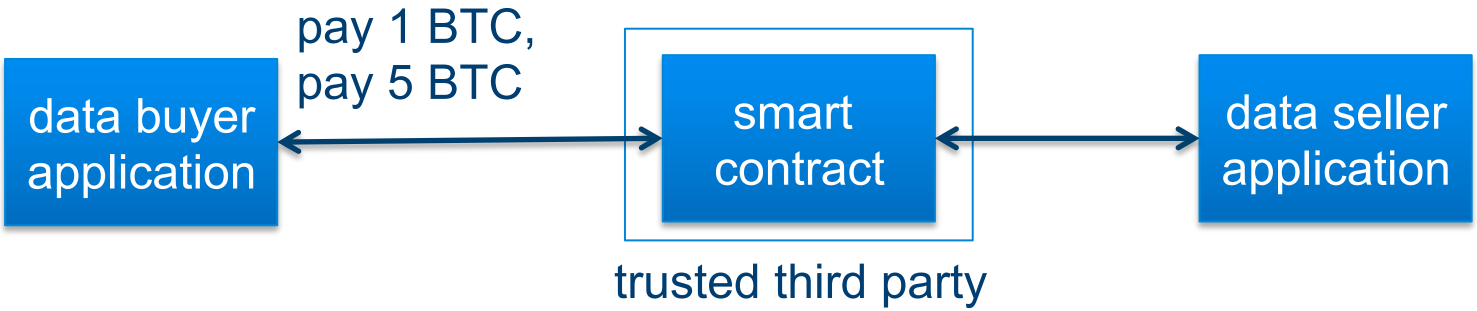
business contract in natural language (ex. English)

1) The data buyer is entitled **to send purchase orders** to buy data …
2) The data seller is free to use her discretion to **either reject the offer** or
3) The data buyer **is obliged to pay** within three days after receiving …
4) The data buyer has the **right to cancel** the purchase order …



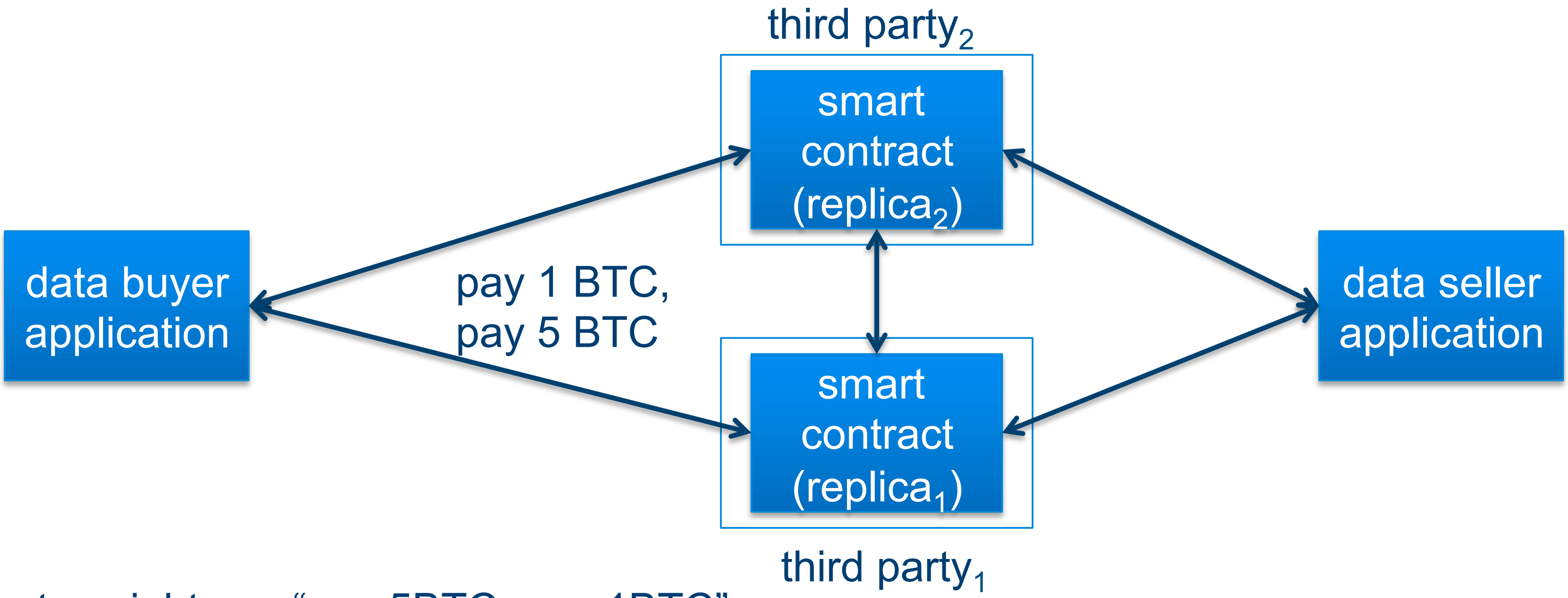
What is a Smart Contract: where to deploy it?

1) In a single trusted third party



What is a Smart Contract: where to deploy it (2)?

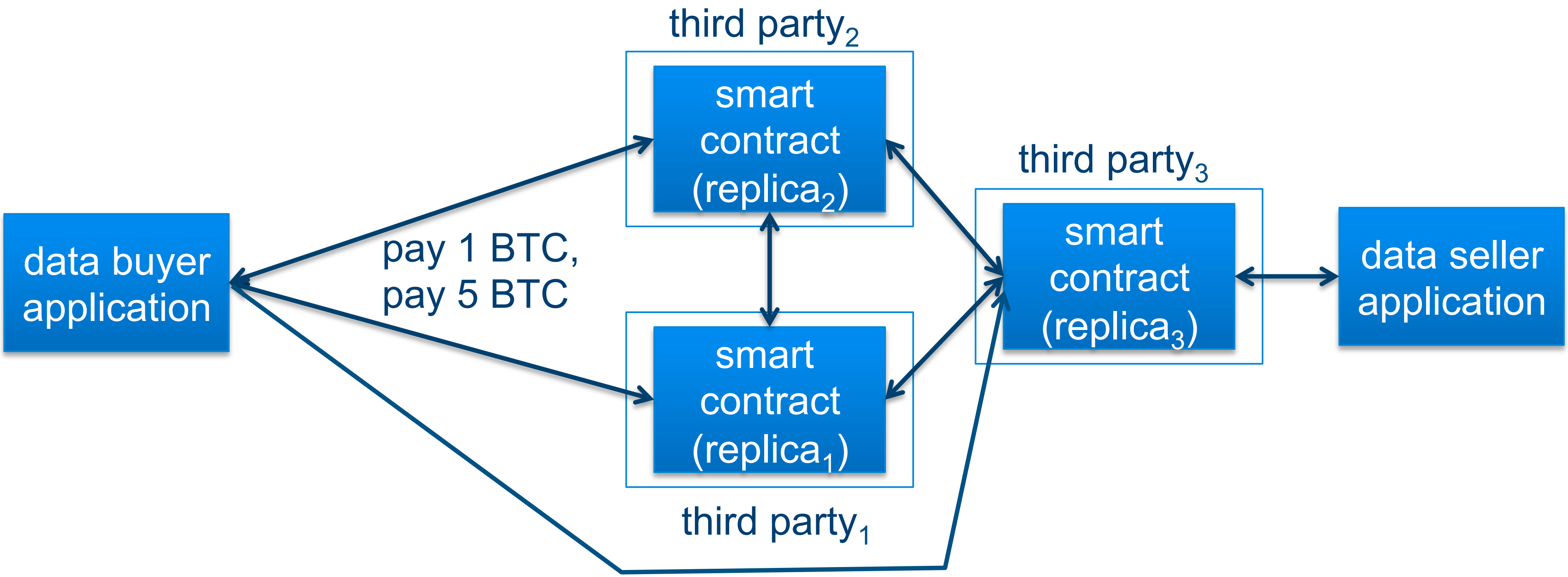
2) If data buyer and data seller cannot find a trusted third party they can use two untrusted third parties.



party$_1$ might see “pay 5BTC>pay 1BTC”
whereas party$_2$ sees “pay 1BTC>pay 5BTC”

What is a Smart Contract: where to deploy it (3)?

2) Replicate the smart contract in many untrusted parties



The problem: it is hard to synchronise the states of the smart contract replicas. What was first: pay 1 BTC or pay 5 BTC? −replicas might receive them in different order.

At the Heart of Blochain is Consensus

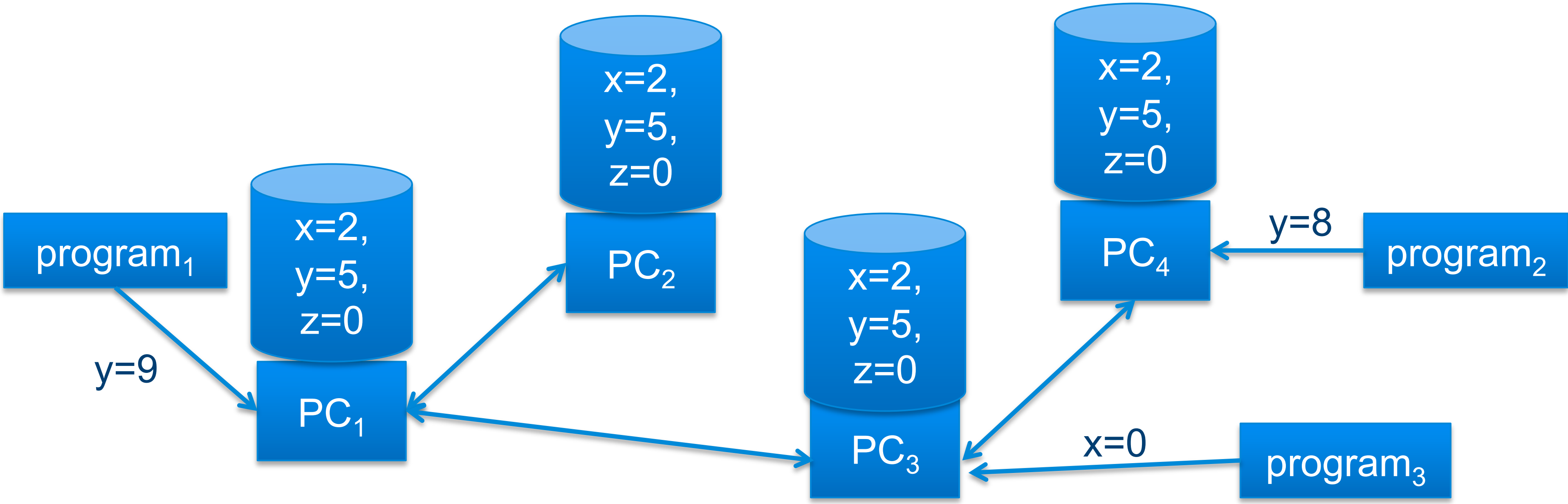
- Bitcoin offers a pragmatic solution to a very old distributed systems problem: consensus--- all about reaching agreements between N remote parties.

Ex1: 3x2+1= ?

Ex2: Let's meet to play football.

At the Heart of Blochain is Consensus

- Consensus--- all about running algorithms between n>=2 networked computers that store a copy of a piece of data on their local disks to ensure that the content of the copies are identical (agree with each other).

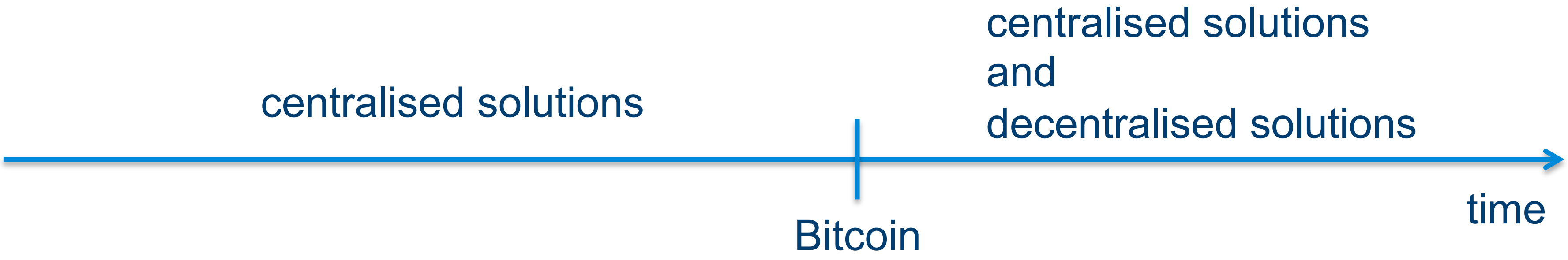


Advantages and Disadvantages of N-party Deployment

- The problem: it is hard to synchronise the states of the smart contract replicas.
  - This is the main issue that Bitcoin solved. It is called consensus.
- Main advantages:
  - Decentralised solution.
  - No need to trust or depend on a single trusted third party like a bank, and government.
  - Replicas can be deployed anywhere.
  - Anybody can verify the indelible historical logs.

Life Before and After Bitcoin

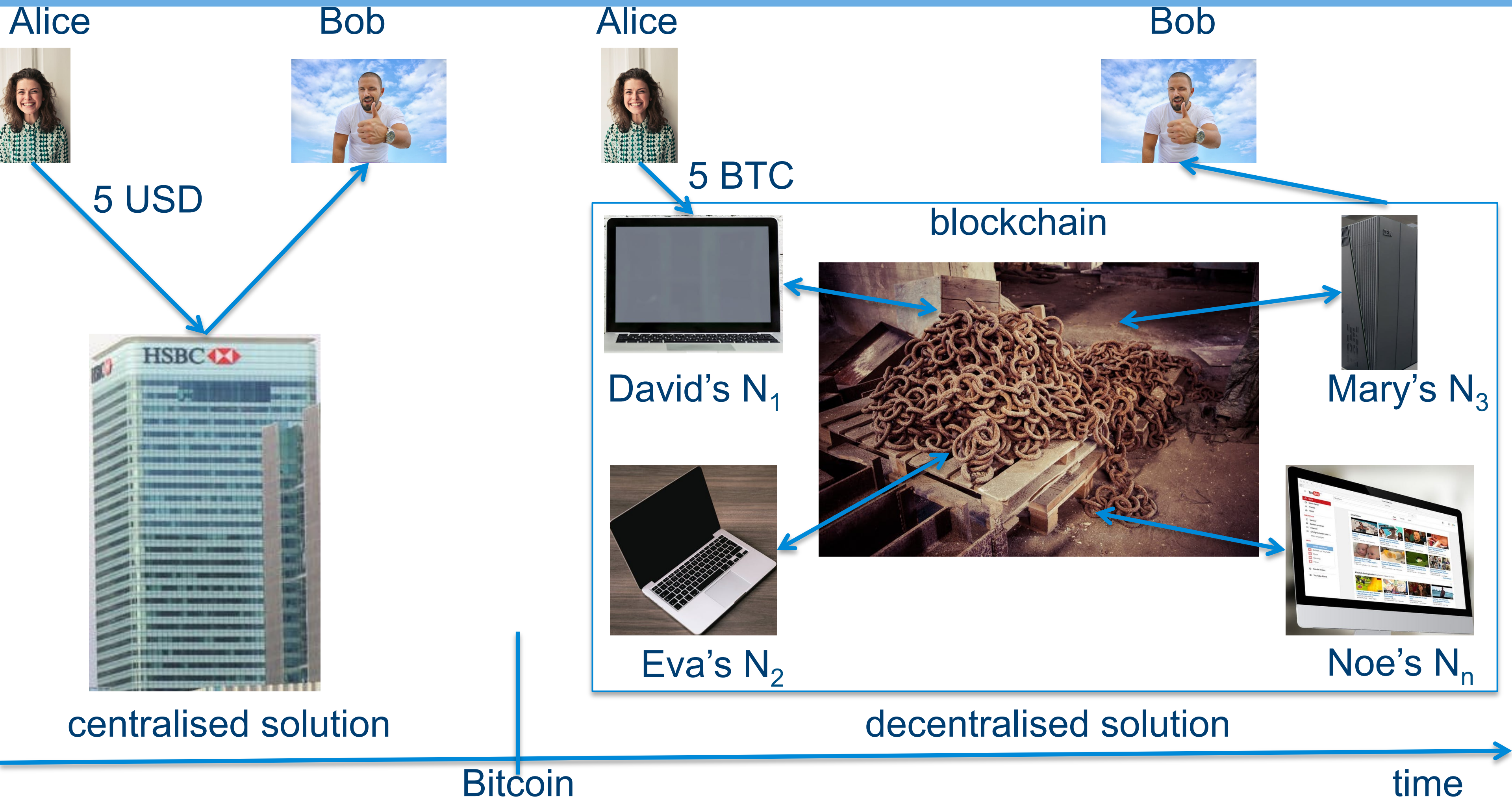
- The solution to this problem took the research community by storm.
- We are devising Bitcoin-based solution to old and new problems.



Who Needs Decentralised Solutions?

- There are many old and new applications that can benefit from decentralised solutions.
  - Mind you that centralised and decentralised solutions can coexist.
- Let us have a look at some examples.

Life before and after Bitcoin: banking



Alice

Bob

5 USD

centralised solution

Alice

Bob

5 BTC

blockchain

David’s N_1

Mary’s N_3

Eva’s N_2

Noe’s N_n

decentralised solution

Bitcoin

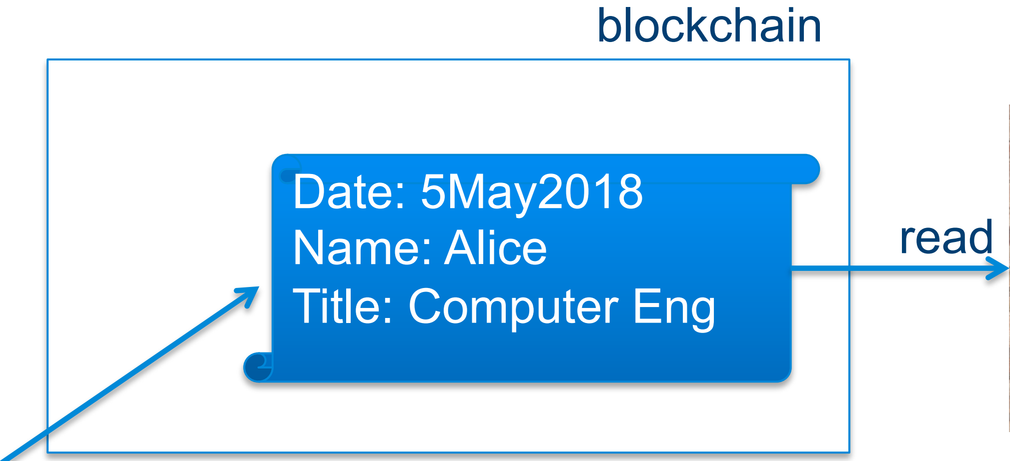
time

Indelible Records on Blockchain

- We produce records that
  - follow the “write once– read many times” model.
  - are immune (not affected) to accidental or malicious alterations.
  - are kept for good and always available (for reading) from anywhere, not necessarily to the general public.
    - consultation and verification.
- Examples: birth/death certificates, medical records, property (land) registries, university certificates.
- The indelibility property that blockchain offers seems ideal for storing such records.
- Pioneering studies have been conducted in Honduras (developing country afflicted by violence, corruption and untrusted governments).

Indelible Records: Ex. University Certificates on Blockchain

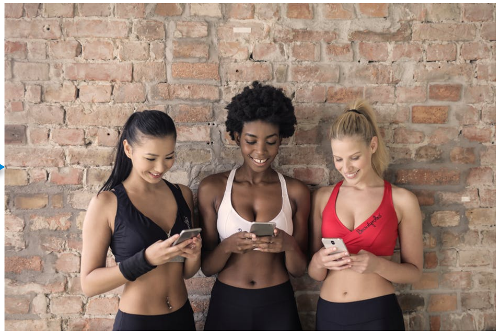
1. Alice passed her final exam.



blockchain

Date: 5May2018
Name: Alice
Title: Computer Eng

read

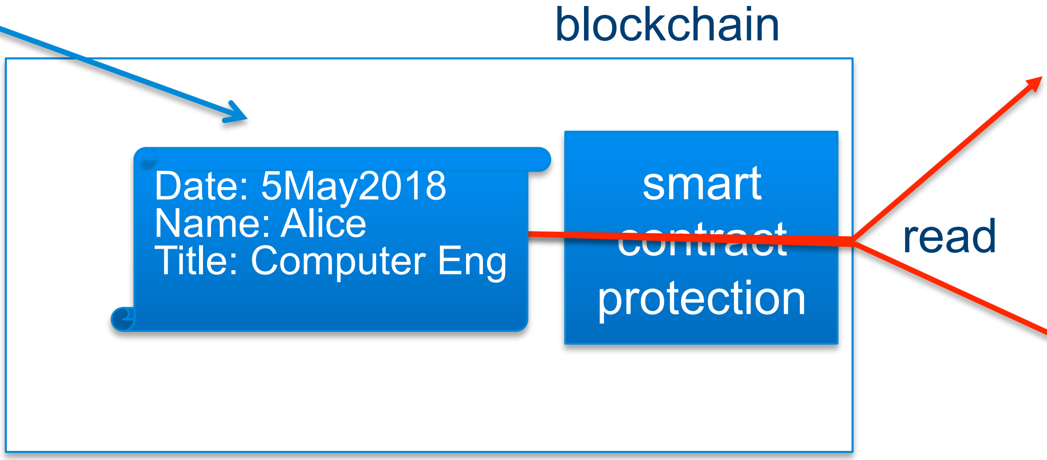


3. Anybody can see it.
Is this OK?

2. Her examiners place certificate in a blockchain

Univ Certificate on Blockchain with a Smart Contract

2 Examiners place record on blockchain but protected by a smart contract.



blockchain

Date: 5May2018
Name: Alice
Title: Computer Eng

smart contract protection

read

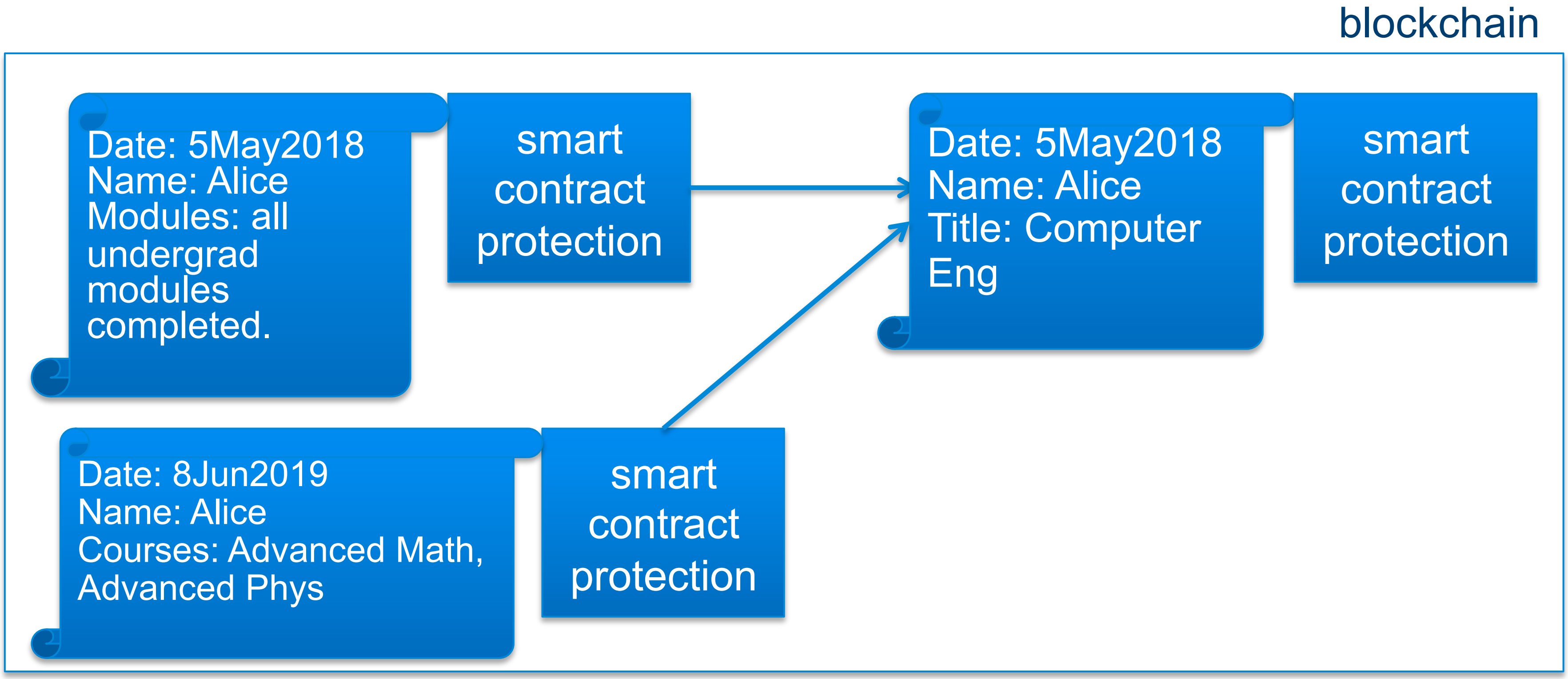
Ex of contract clauses

c1: Prof has the right to access the records at any time.

c2: Researcher has the right to access the record only after biz hrs

3. Only some people can it it.

Smart Contracts can Help Create Records from Records automatically and systematically: ex 1



blockchain

Date: 5May2018
Name: Alice
Modules: all undergrad modules completed.

smart contract protection

Date: 5May2018
Name: Alice
Title: Computer Eng

smart contract protection

Date: 8Jun2019
Name: Alice
Courses: Advanced Math, Advanced Phys

smart contract protection

Ex of a contractual clauses

C1: students that have completed all their undergrad modules of Comp Sc. and Advanced Math and Advanced Phys courses are entitled to Computer Eng. degrees without writing Dissertations.

Why do I need blockchain to record univ documents?

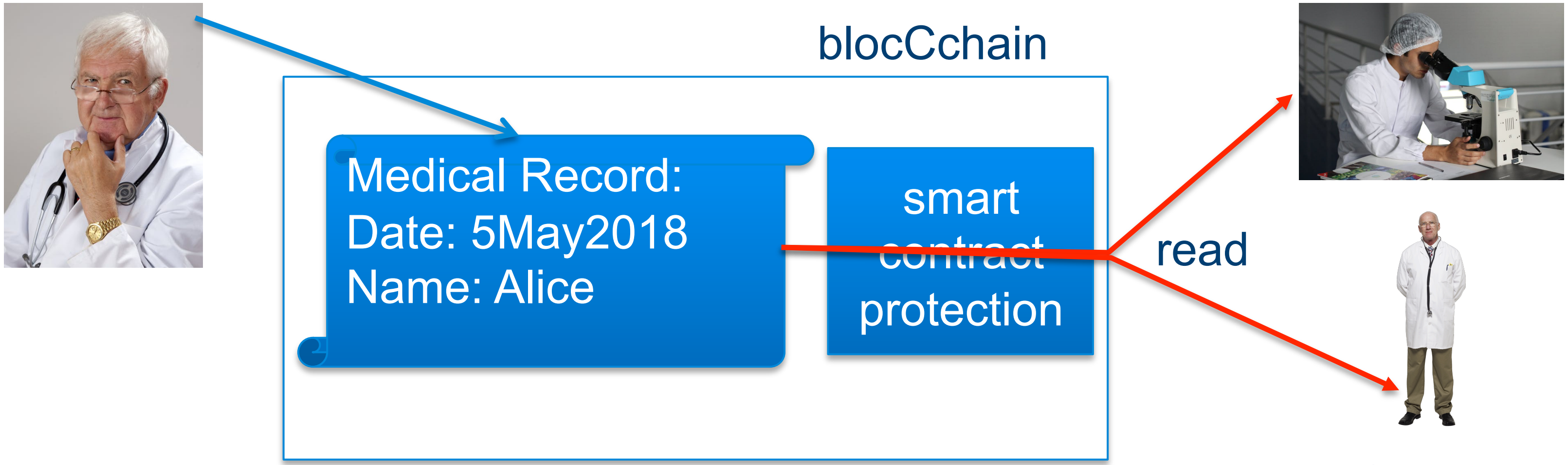
- Universities might disappear, records need to persist.
  - The Polytechnic Institute of Odessa has disappeared! ---changed its name to Odessa National Polytechnic University.
  - Where are the schools documents issued in Crimea?--- are they now in Kiev or Moscow archives?
- Some Mexican politicians have failed to produce their university degree certificates—immediate access to university records would help clarify their situations.

Jose Cordova Montoya   Miguel Angel Osorio Chon

CANACINTRA ESTADO DE MÉXICO
CONVENCIÓN
NACION 2017
DELEGACIONES, SECTORE INDUSTRIALES
BUSCANDO NU ZONTES
Miguel Angel Osorio Chong
SECRETARIO DE GOBERNACIÓN
M

Medical Record on Blockchain with a Smart Contract

1 Alice's Dr places medical record on blockchain but protected by a smart contract.



blocCchain

Medical Record:
Date: 5May2018
Name: Alice

smart contract protection

read

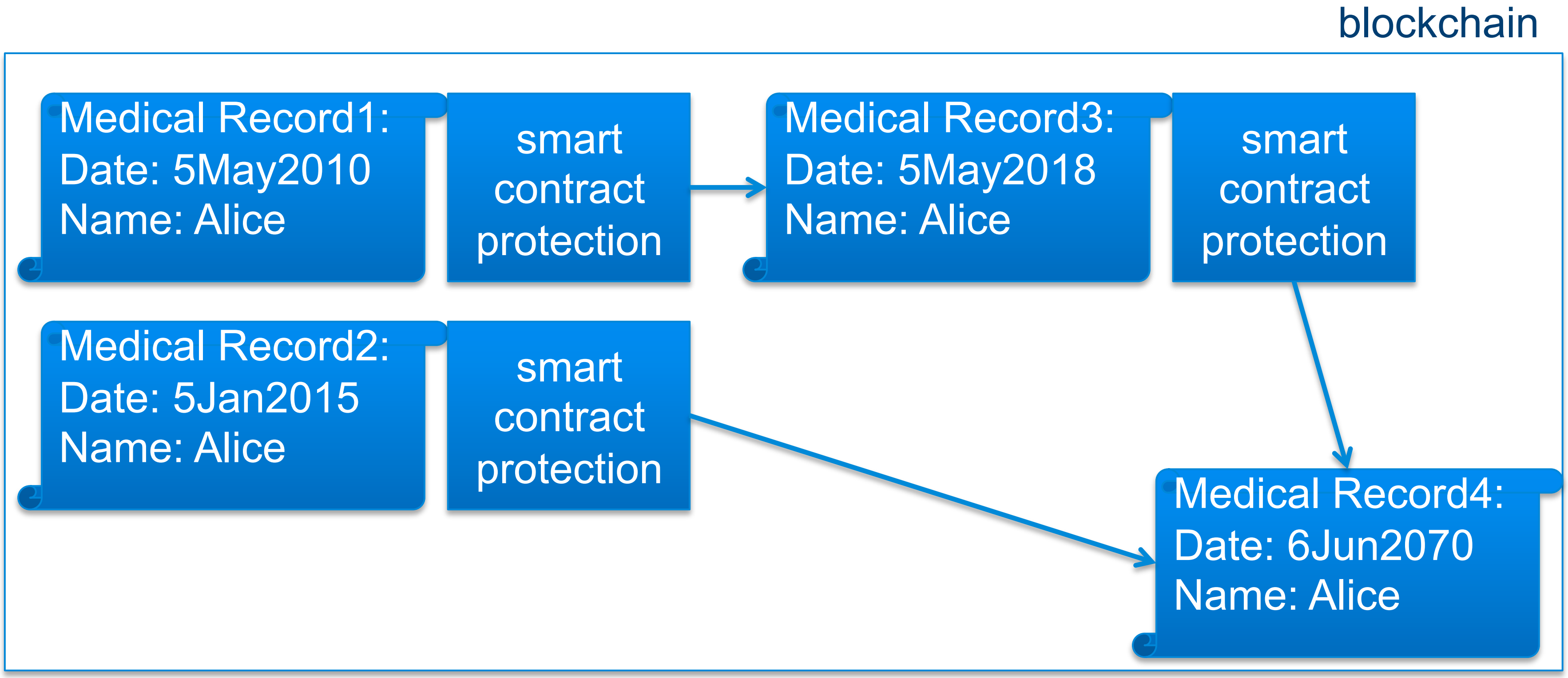
2. Only some people can it it.

Ex of contract clauses

c1: Dr has the right to access the records at any time.

c2: Researcher has the right to access the record only after biz hrs

Smart Contracts can Help Create Records from Records automatically and systematically

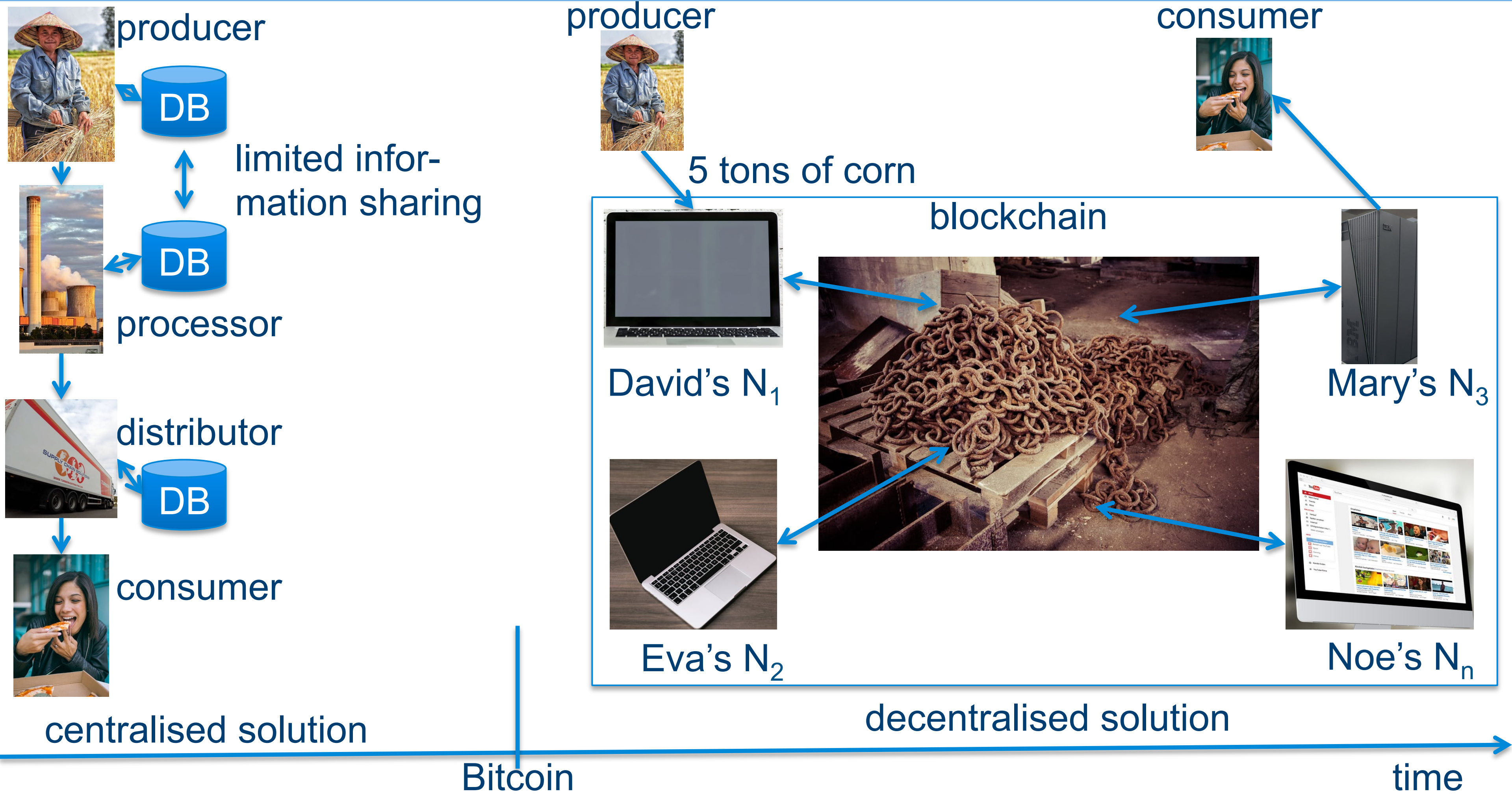

blockchain
Medical Record1: Date: 5May2010 Name: Alice
smart contract protection
Medical Record3: Date: 5May2018 Name: Alice
smart contract protection
Medical Record2: Date: 5Jan2015 Name: Alice
smart contract protection
Medical Record4: Date: 6Jun2070 Name: Alice

Ex of a contractual clauses

C1: On Alice's 18th b/day create Med Record3.

C2: If Med Record2 and Med Record3 exist then create Med Record4

Life before and after Bitcoin: supply chain



producer

DB

limited information sharing

DB

processor

distributor

DB

consumer

centralised solution

Bitcoin

producer

consumer

5 tons of corn

blockchain

David’s N_1

Mary’s N_3

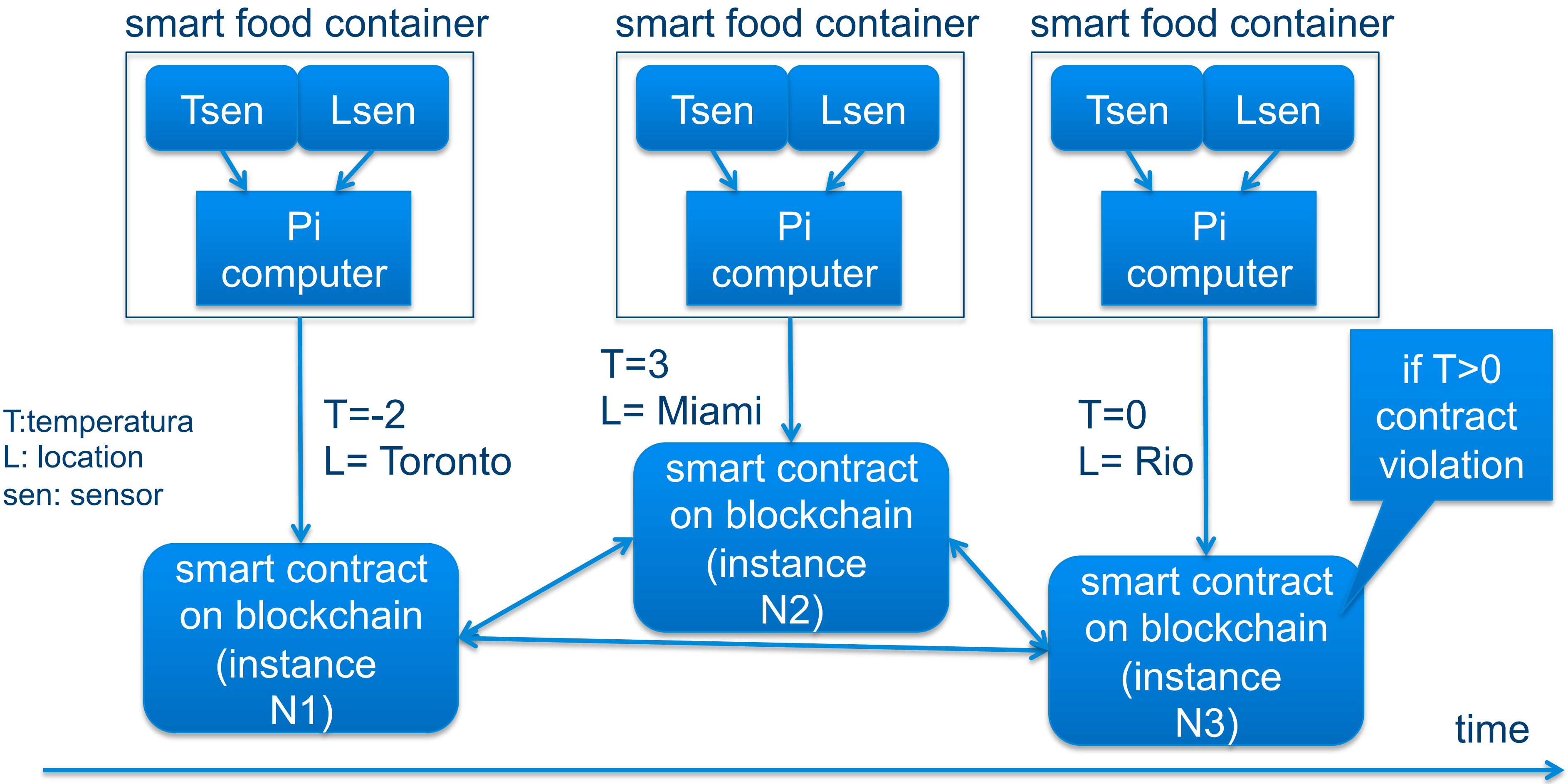
Eva’s N_2

Noe’s N_n

decentralised solution

time

Food Policies Enforcement with Smart Contracts



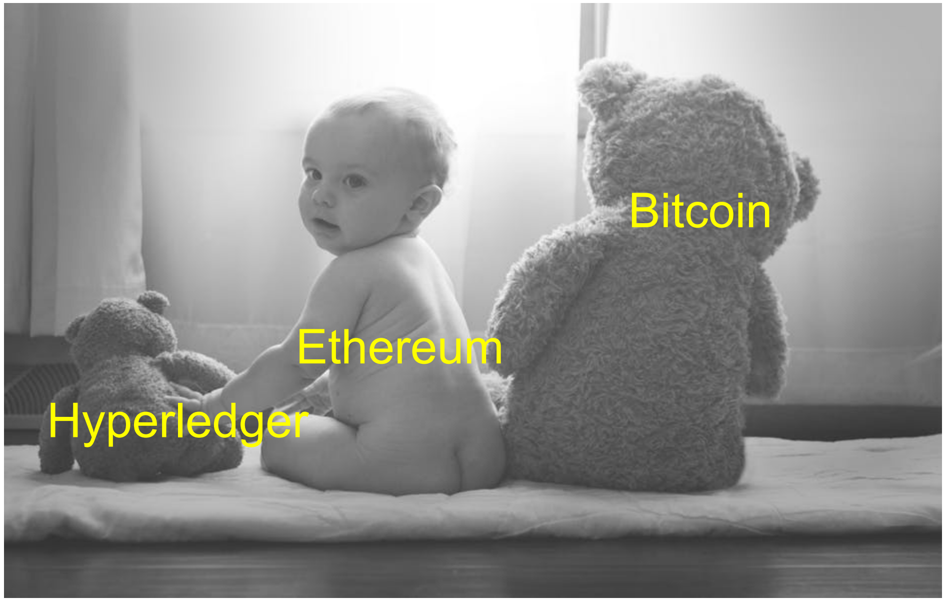
T:temperatura
L: location
sen: sensor

Cheap Liquidity Cryptocurrency Cash in Supply Chain (see sweetbridge.com)

1. Alice (a member of a supply chain) can cook and sell pizzas.
2. Alice does not have cash to buy ingredients. Bank credits are unaffordable (interests too high).
3. Alice has assets (her car, house, etc.).
4. Alice deposits an asset (ex. car) in an asset vault and gets 100 sweetcoins (cryptocurrency).
5. Alice buys ingredients (cheese, tomato, …) makes pizzas and sells them for 150 sweetcoins.
6. Alice pays her debt and recovers her car.

The State of the Art

- Bitcoin, Ethereum, Hyperledger and other blockchains have been operating for years and has proved that the idea works.
- Yet, they is still at experimental stage, very immature and looking for the killing application.



Are Blockchains and Smart Contracts Here to Stay?

- Yes, but there are hurdles to clear

Bitcoin Mining is Burning the Planet

- Bitcoin mining (computation required to validate a transaction) consumes a ridiculous amount of energy [Feeding the Blockchain Beast, Peter Fairley]
- The energy consumed by a second of Bitcoin mining is equivalent to the energy consumed by 325 000 houses.
- A Bitcoin transaction consumes 5 000 times more energy than a Visa transaction.

Bitcoin is too slow

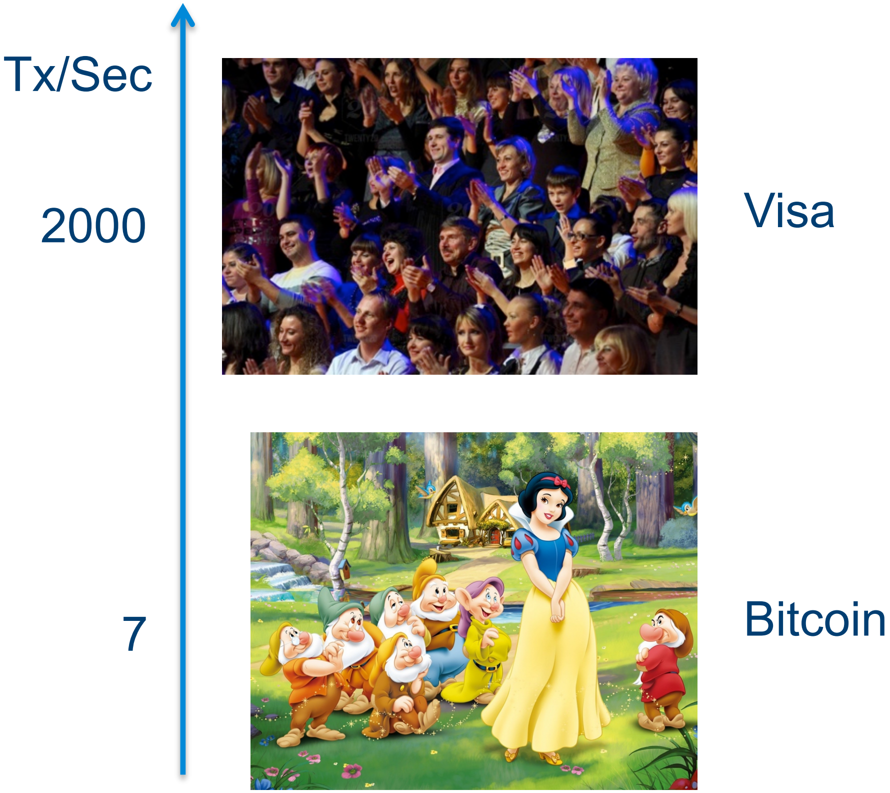
- The response time of Bitcoin (and other blockchains) is too slow for applications that demand quick response (sec, milliseconds).

Quick response: real time applications: ex. car sensors

UNIVERSITY OF CAMBRIDGE

Bitcoin does not Scale Up

- Bitcoin can process only about 7 transactions per second.
- Visa can process 2 000 per second.



Cambridge Potential Solution to Blockchain Limitations: hybrid approach

- Use a hybrid solution combines centralised smart contract enforcement and decentralised smart contract enforcement.
- There are two approaches to implement applications that involve enforcement of contractual commitments like in banking, supply chain, and business to business processes.
  - Centralised: implemented using a trusted party (ex. traditional banking).
  - Decentralised: implemented using blockchains (ex. Bitcoin).
- Different applications demand different quality of services (ex. number of transactions per sec, response time, transparency and privacy).
  - some applications can be implemented more naturally with either of the two approaches.
  - there are applications that none of the approaches can handled individually and thus require a hybrid approach.
- In the near future we will be running applications that will demand support from several centralised and decentralised smart contracts enforcers that will collaborate with each other.

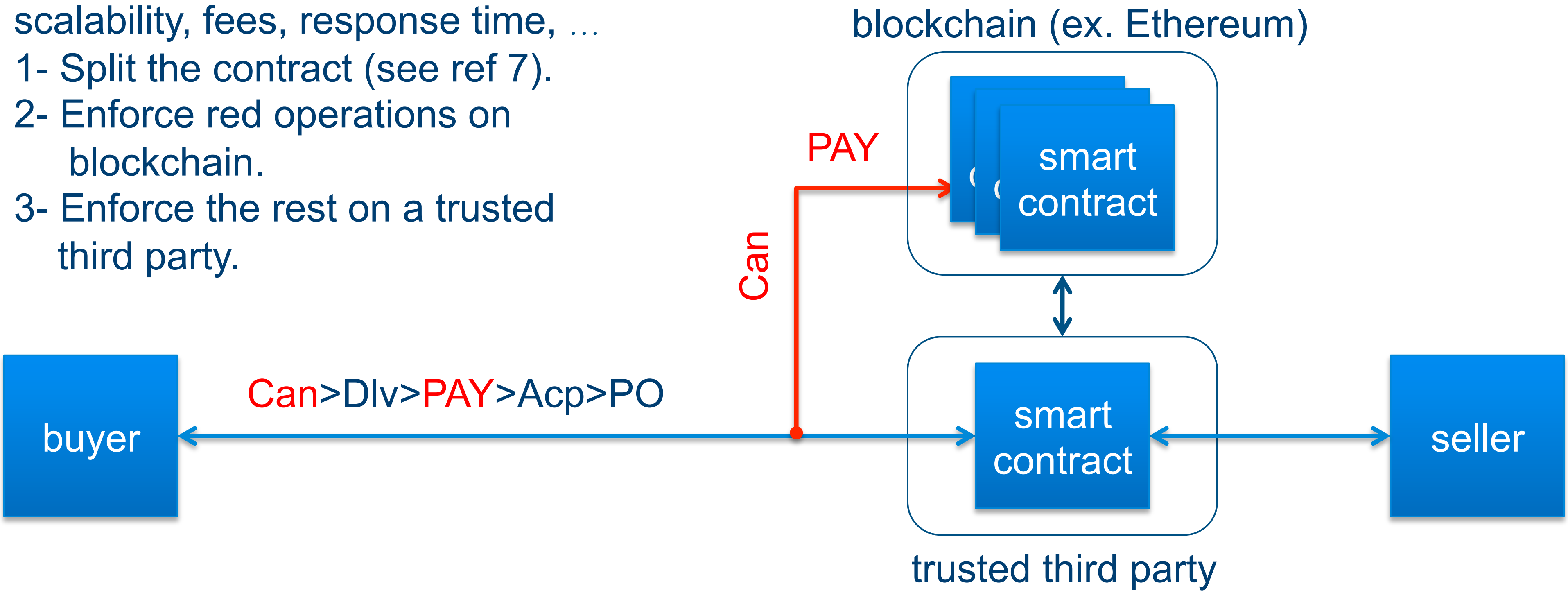
Cambridge Potential Solution to Blockchain Limitations: hybrid approach

To address blockchain issues: scalability, fees, response time, …

1- Split the contract (see ref 7).

2- Enforce red operations on blockchain.

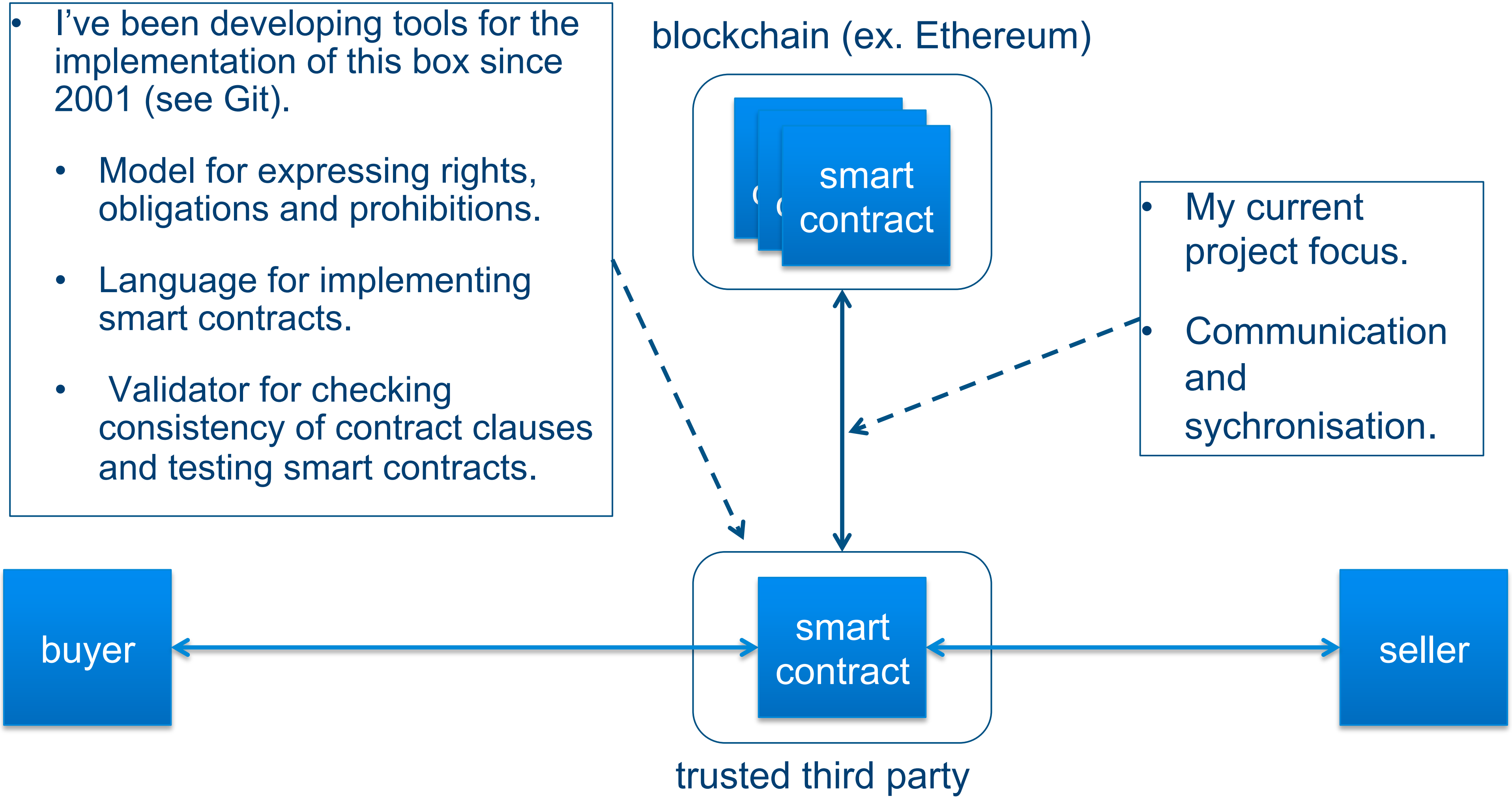
3- Enforce the rest on a trusted third party.



PO=Purchase Order, Acp=Accept, Dlv= Delivery, Can=Cancel, buyer= buyer’s application, seller= seller’s application

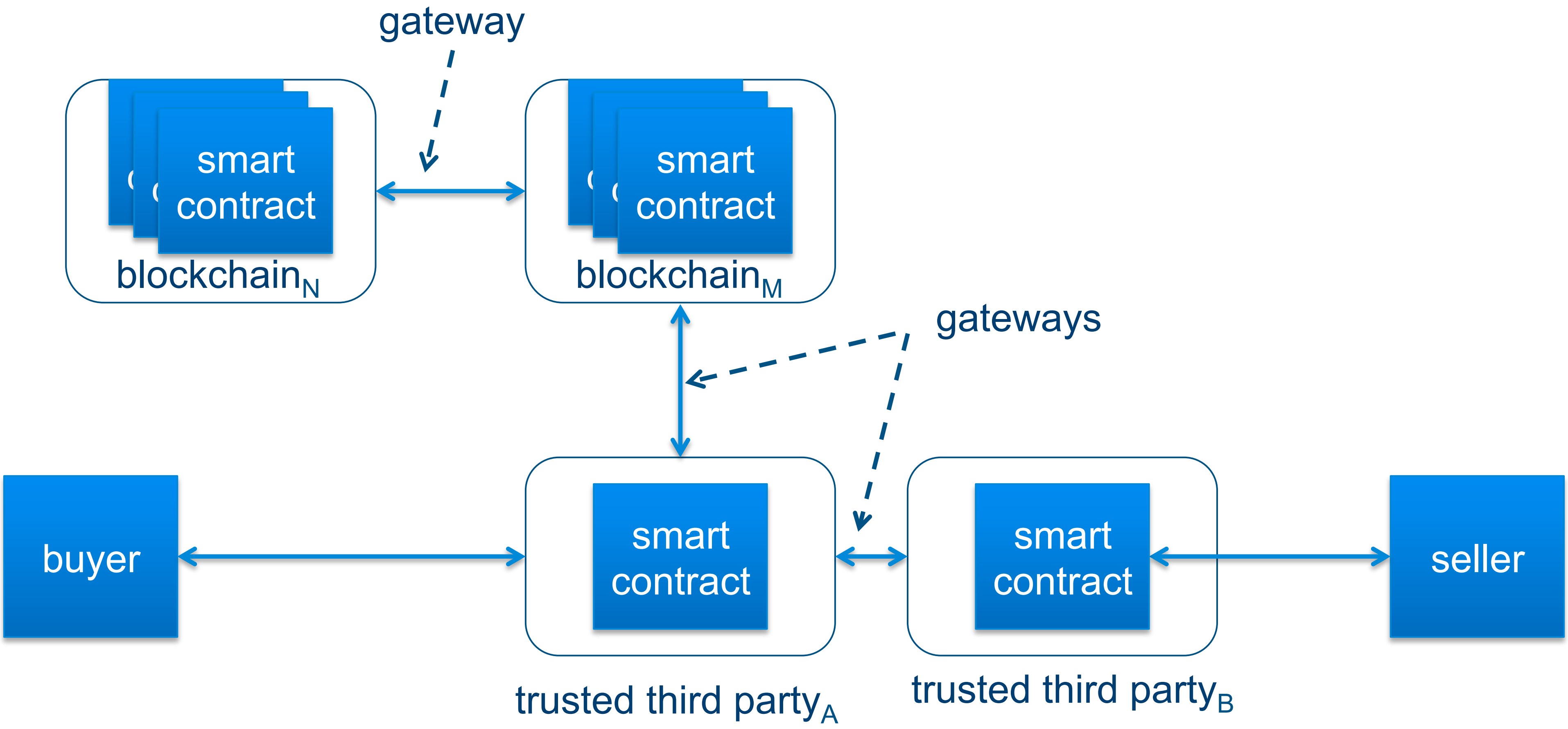
Technology under Development at Computer Lab

- I’ve been developing tools for the implementation of this box since 2001 (see Git).
  - Model for expressing rights, obligations and prohibitions.
  - Language for implementing smart contracts.
  - Validator for checking consistency of contract clauses and testing smart contracts.



- My current project focus.
- Communication and sychronisation.

Future: On and off—blockchain Computation Paradigm



Conclusions

- Blockchain and smart contracts have a large potential to:
  - enhance (re-implementation?) existing applications.
  - implement new applications.
- Buzz words: lots of noisy, misunderstandings and expectations.
- The fact is, they are new technologies and currently at laboratory experimentation stage:
  - legal + business + technical issues to clarify.
  - libraries + standards + developers + blockchain minded biz people are missing.
- This is the right time to invest in these innovative technologies and risks--- if you can afford it, you might lost money and time or take the lead.

References

1. “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satosh Nakamoto, 2008.
2. “Mastering Bitcoin”, Andreas M. Antonopoulos, O’Relilly, 2nd Edition 2017.
3. “Feeding the Blockchain Beast”, P. Fairley, Spectrum. IEEE Oct 2017
4. “On and Off Blockchain Enforcement of Smart Contracts”, Carlos Molina, … Jon Crowcroft, arXiv, May 2018.
5. “A Model for Checking Contractual Compliance of Business Interactions”, Carlos Molina-Jimenez, et. al. IEEE Tran on Services Computing, V.5 N.2 Apr-Jun 2012.
6. Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser, 2015.
7. “Trusting records: in Blockchain technology the answers?”, Victoria Louise Lemieux, Records Management Journal, V26, Issue 2016.

References 2

8. “Using Blockchain to Secure Honduran Land Titles”, *Jorge* Constantino Collindre*, et. al.* https://s3.amazonaws.com/ipri2016/casestudy_collindres.pdf

9. The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project, Feb 2017, https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#13f494704dcd

10. Academic Certificates on the Blockchain, https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/