UNIVERSITY OF CAMBRIDGE

On Potential Research Directions on Blockchain and Smart Contracts

Carlos Molina-Jimenez

Carlos.Molina@cl.cam.ac.uk

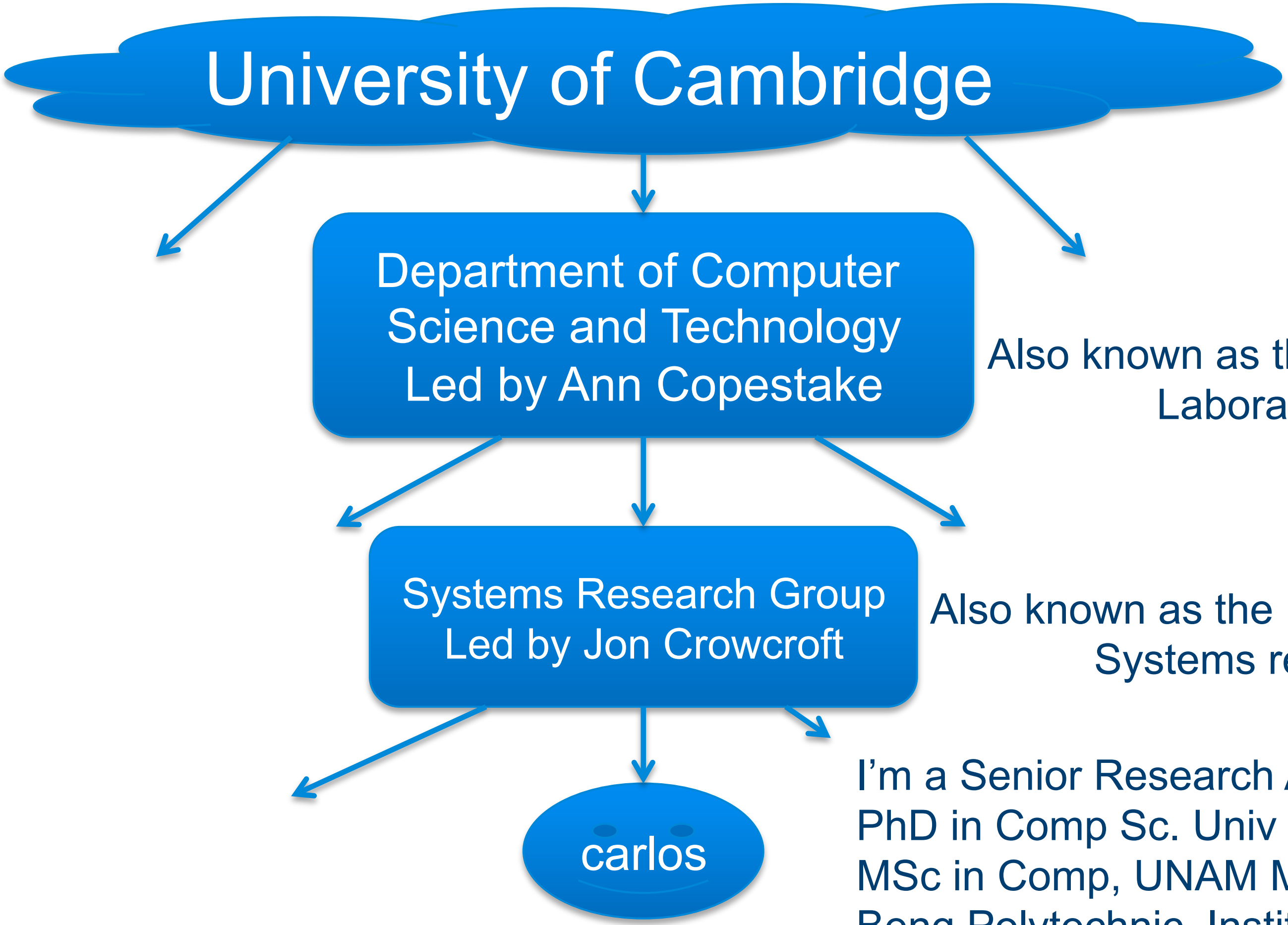
http://www.cl.cam.ac.uk/~cm770/

Department of Computer Science and Technology:

Computer Laboratory

University of Central Asia 16 May 2018

My Research Group



University of Cambridge

Department of Computer Science and Technology
Led by Ann Copestake

Systems Research Group
Led by Jon Crowcroft

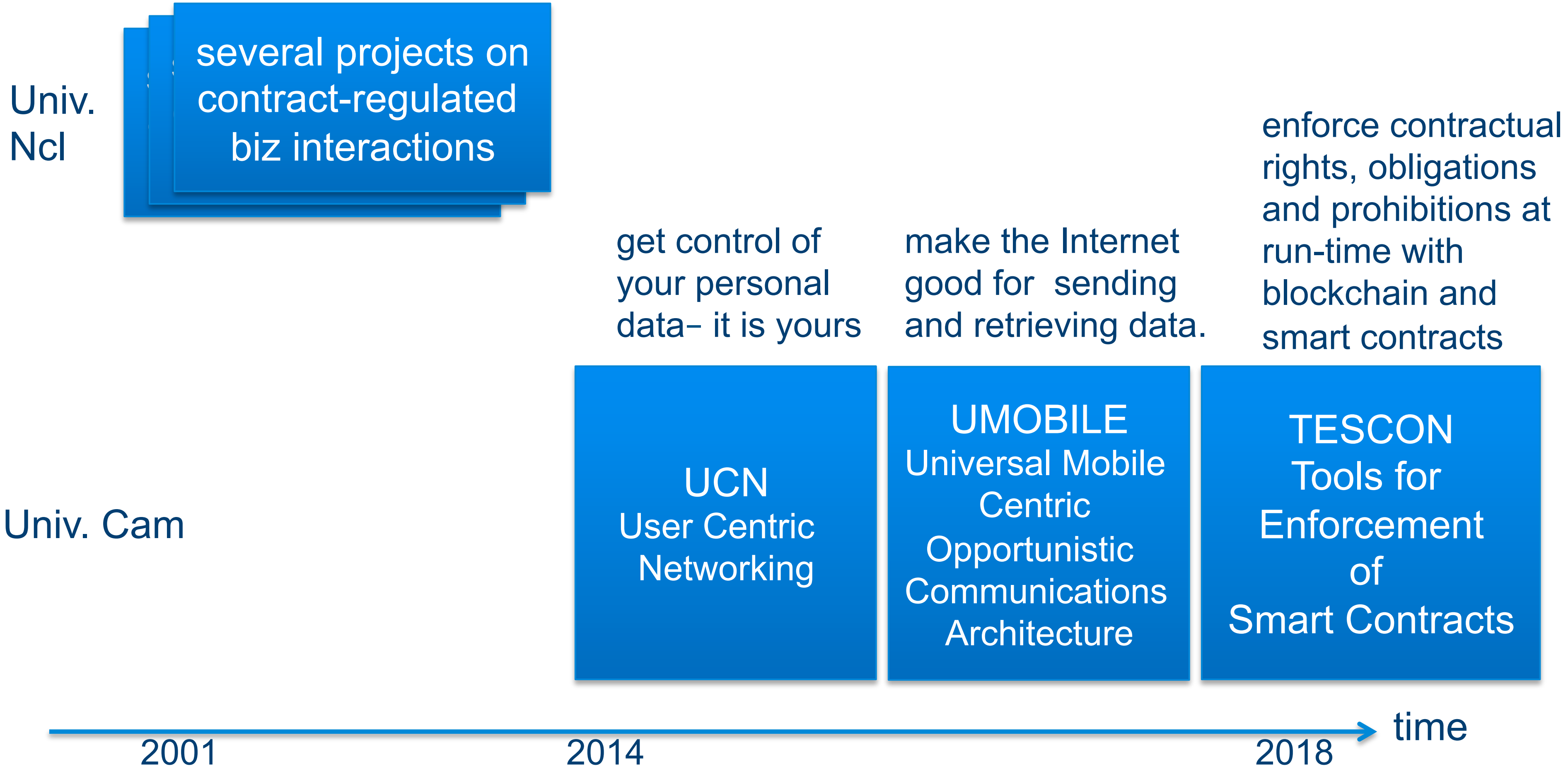
carlos

Also known as the Computer Laboratory

Also known as the Network and Operating Systems research group

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

make the Internet good for sending and retrieving data.

UMOBILE
Universal Mobile Centric Opportunistic Communications Architecture

enforce contractual rights, obligations and prohibitions at run-time with blockchain and smart contracts

TESCON
Tools for Enforcement of Smart Contracts

Why blockchain and smart contracts?

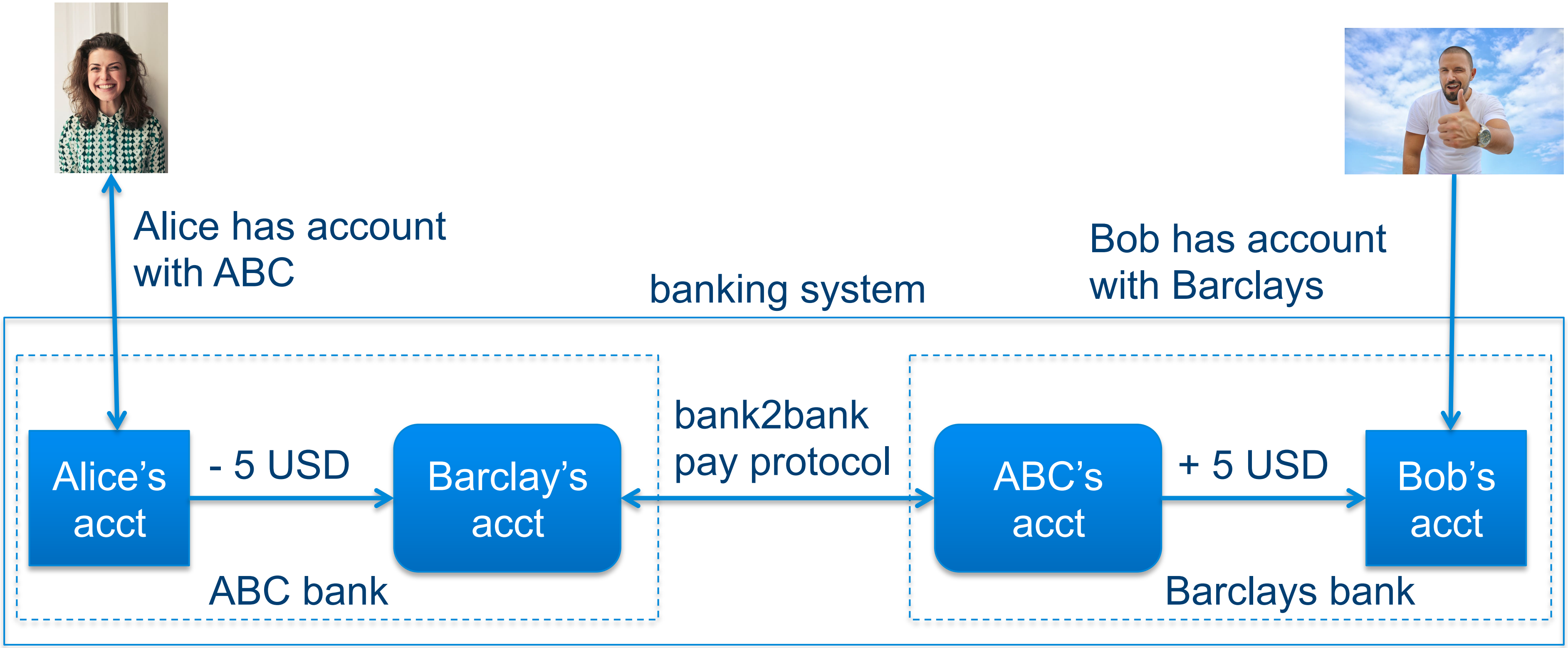
- What is blockchain?
- What is it good for?
- Who needs it?
  - **Me, I need it!!!**

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)
C A N A D A
GREENLAND (DENMARK)
ICELAND
SVALBARD (NORWAY)
R U S S I A
SWEDEN
NORWAY
FINLAND
ESTONIA
LATVIA
IRELAND
North Pacific OCEAN
North Pacific OCEAN
UNITED STATES OF AMERICA
North Atlantic OCEAN
MEXICO
HAWAIIAN ISLANDS (USA)
KAZAKHSTAN
MONGOLIA
C H I N A
JAPAN
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
IRAN
INDIA
MAURITANIA
MALI
NIGER
SUDAN
CHAD
ETHIOPIA
SOMALIA
KENYA
TANZANIA
ANGOLA
NAMIBIA
BOTSWANA
SOUTH AFRICA
B R A Z I L
ARGENTINA
CHILE
South Pacific OCEAN
South Atlantic OCEAN
INDIAN OCEAN
A U S T R A L I A
NEW ZEALAND
Antarctica
@Copyright MapsNWorld.com 2011
Map Not To Scale

Money transfer: Traditional Bank-mediated Approach



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

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.

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 (two or more might be involved) do its job?
  - It has a centralised ledger with records of all the Txs: it knows Alice’s and Bob’s balances.
  - It has a database with Alice’s and Bob’s personal information (name, address, sex, etc.).

Bitcoin to the Rescue– Let us Get Rid of the Bank

- Let us get rid of the bank--- said Satoshi Nakamoto in 2008.
- They built Bibcoin--- an online system that facilitates person-to-person (for ex. Alice to Bob) money transfer in BTC cryptocurrency (10 USA = 0.10 BTC aprox.).
    - person-to-person means directly, without the bank mediating between the two parties. Some people call it pee-to-peer.
- No banks in the middle means goods things
    - 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,….

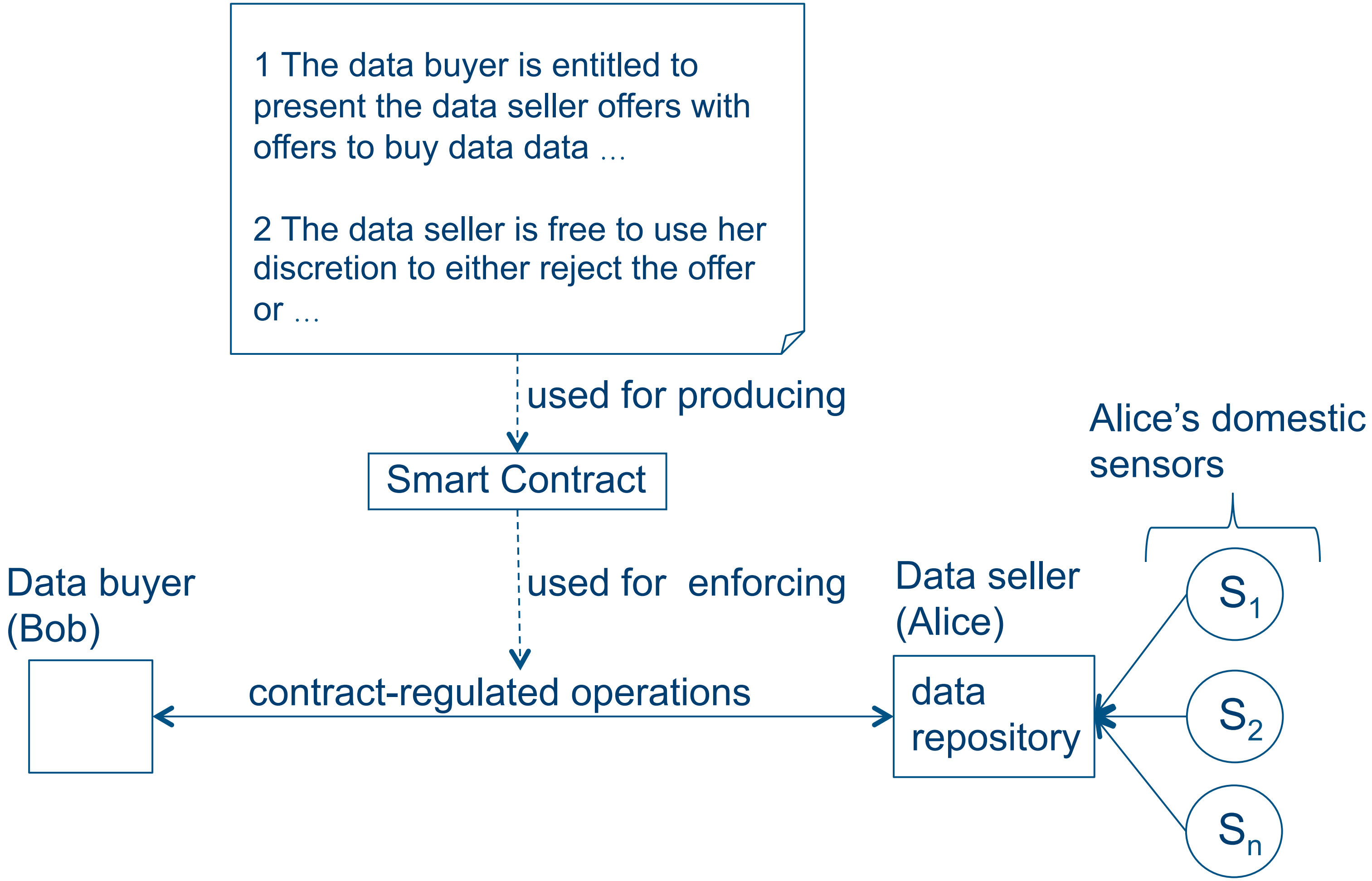
Competition Joins the Race

- Bitcoin shook the banking and financial system.
- Competition appeared quickly
  - Ethereum, Hyperledger, etc.

How does Bitcoin Solve the Problem?

- 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 Txs take place: right amount of money and to the right receiver.

What is a Smart Contract?



1 The data buyer is entitled to present the data seller offers with offers to buy data data …

2 The data seller is free to use her discretion to either reject the offer or …

used for producing

Smart Contract

used for enforcing

Data buyer (Bob)

contract-regulated operations

Data seller (Alice)

data repository

Alice’s domestic sensors

S_1

S_2

S_n

Beyond Bitcoin’s Cryptocurrency

- Bitcoin’s cryptocurrencies was only the first application.
- It was enough to generate commercial and research interest.

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

Bitcoin Offered a Pragmatic Solution to old Consensus Problem?

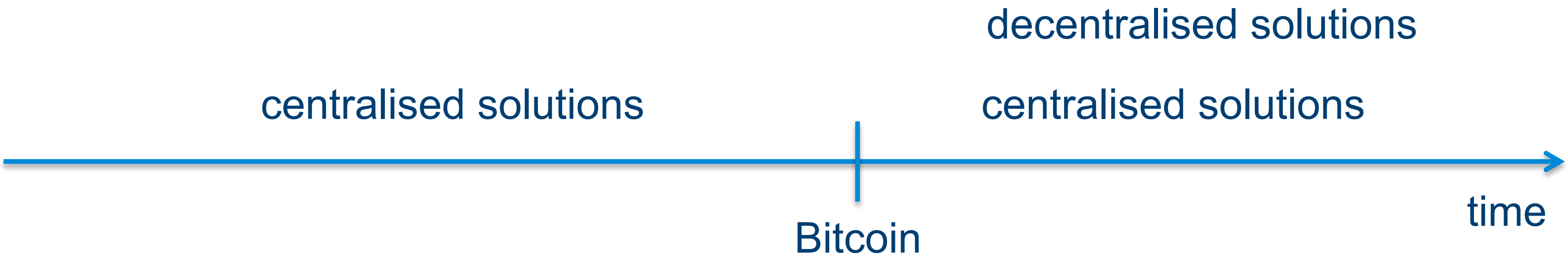
- Bitcoin offers a pragmatic solution to the old and fundamental consensus problem.

At the Heart of Blochain is Consensus

- Bitcoin offers a pragmatic solution to a very old distributed systems problem: 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).

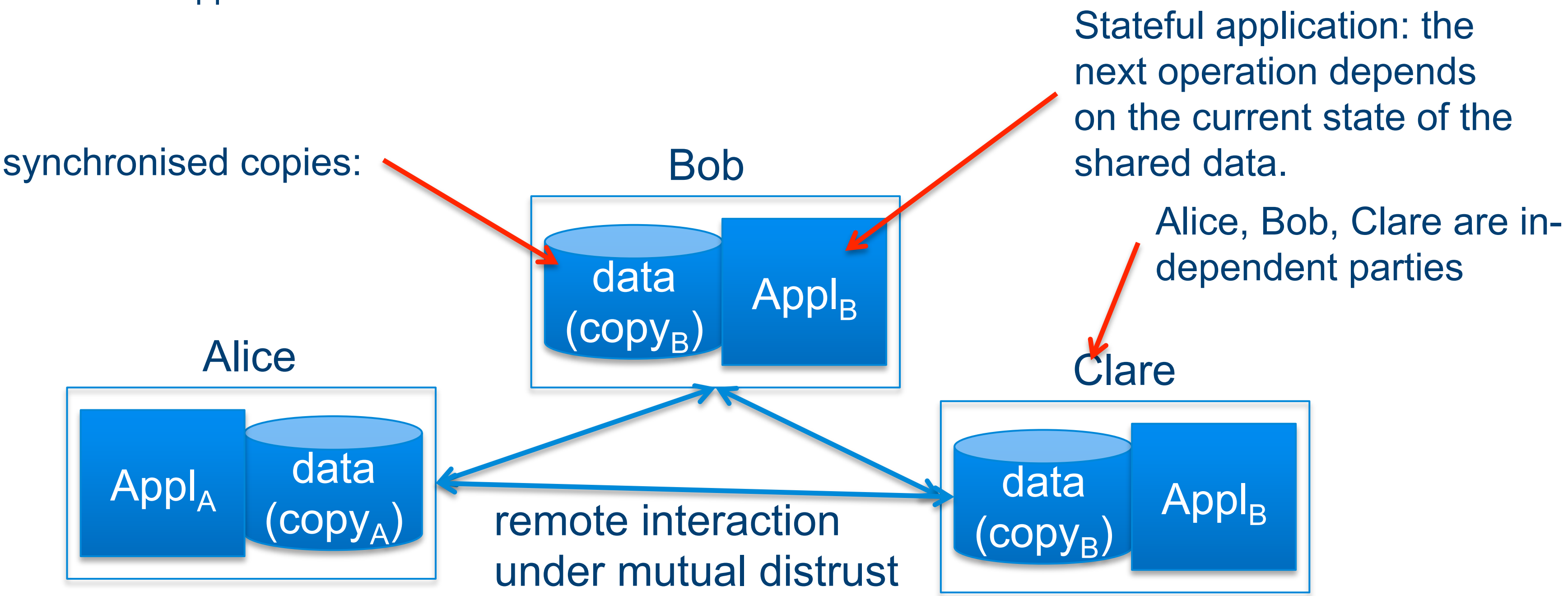
Life Before and After Bitcoin

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



Decentralised Ledger as a Middleware Service

- The descentralised ledger used by blockchain platforms (Bitcoin, Ethereum, Hyperledger, …) can be regarded as a piede of **generic** middleware service.
  - Generic: that can be used for supporting a large class of applications. Cryptocurrencies is only one of them.
- What kind of applications?



synchronised copies:

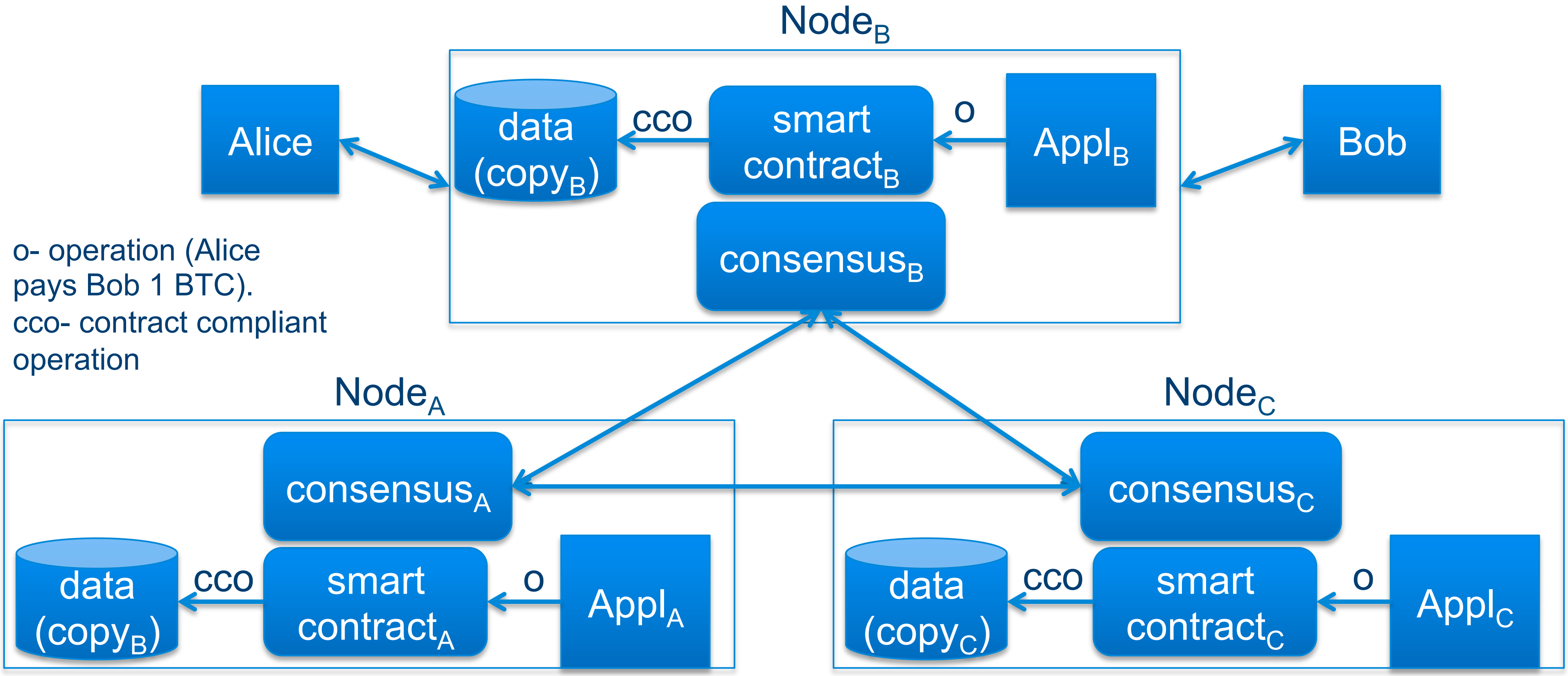
Stateful application: the next operation depends on the current state of the shared data.

Alice, Bob, Clare are in-dependent parties

remote interaction under mutual distrust

Middleware services of the Decentralised Ledger

- Data synchronisations by means of consensus algorithms (ex. Proof of Work).
- Operation enforcement by means of smart contracts.



o- operation (Alice pays Bob 1 BTC).
cco- contract compliant operation

What are Blockchains Good for?

- I believe that it is a piece of science and technology with large potential beyond cryptocurrencies.
  - It can help solve problems that in the past could be solved only in a centralised manner.
  - Centralisation is good because it is simple but
  - Centralisation is bad because of the dependency on the single party placed in the middle.

Examples of Research on Blockchain Applications

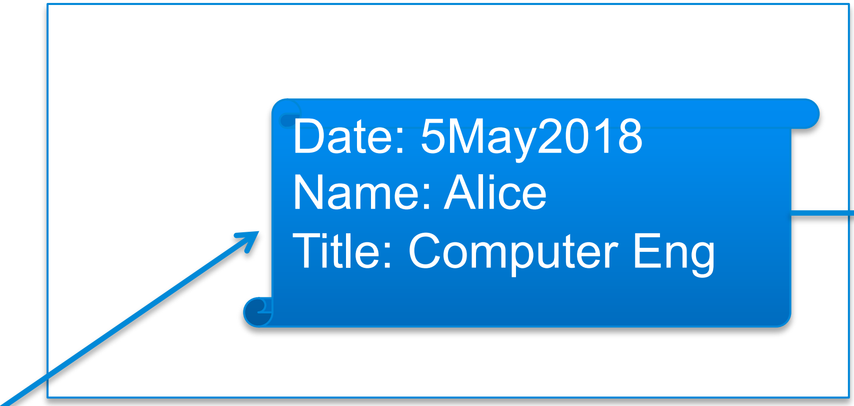
- I will discuss some example that can be mapped into other similar applications.

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).

Records: University Certificates on Blockchain

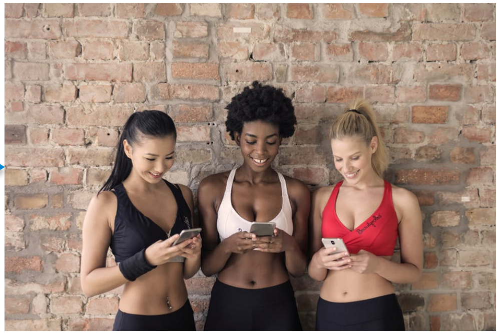
1. Alice passed her final exam.



blockchain

Date: 5May2018
Name: Alice
Title: Computer Eng

read

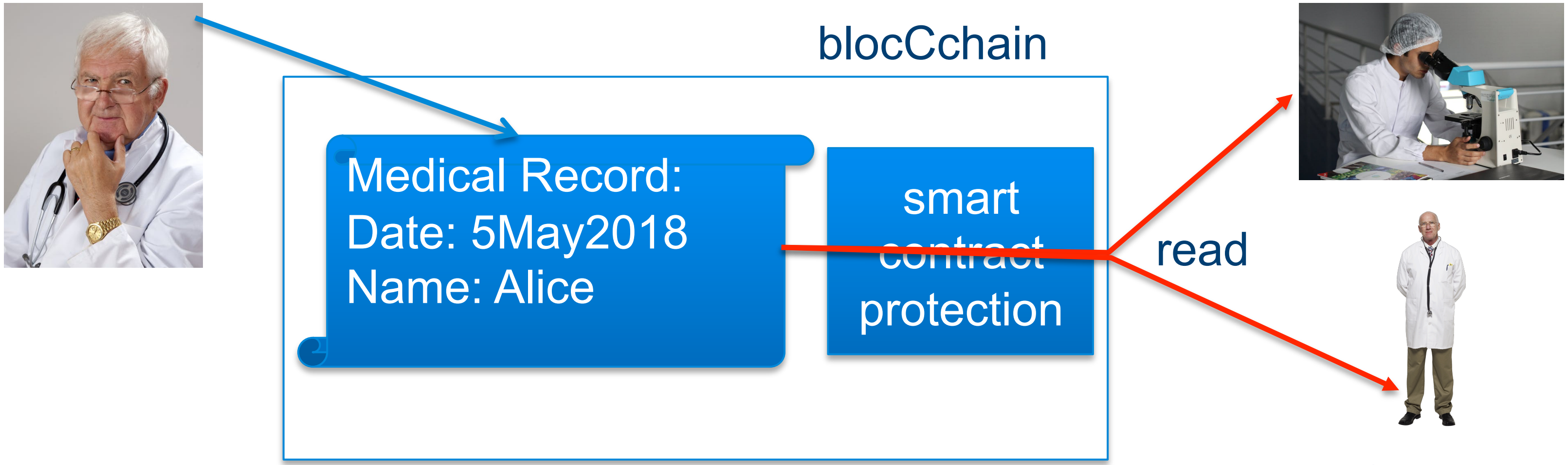


3. Anybody can see it. OK for a uni certificate but what about medical records?

2. Her examiners place certificate in a blockchain

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

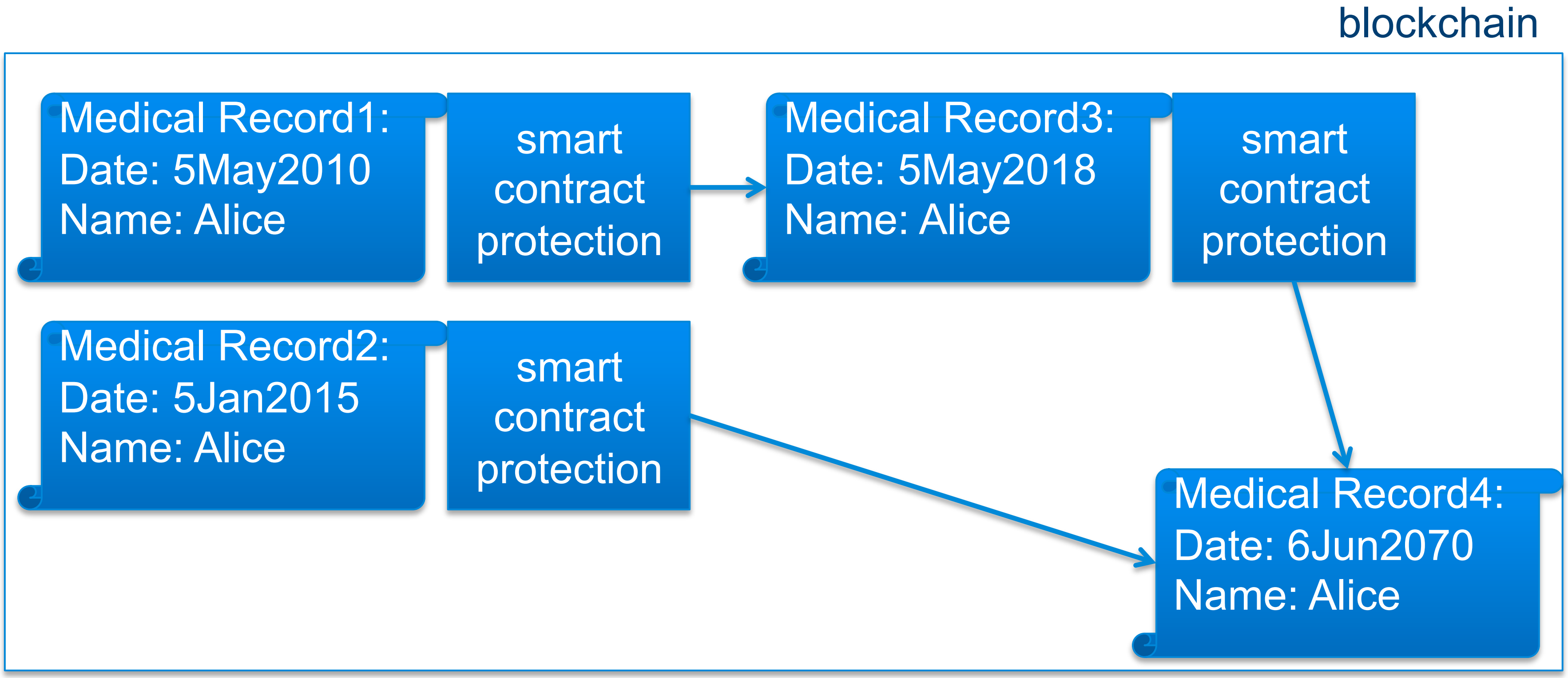
2. Only some people can it it.

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

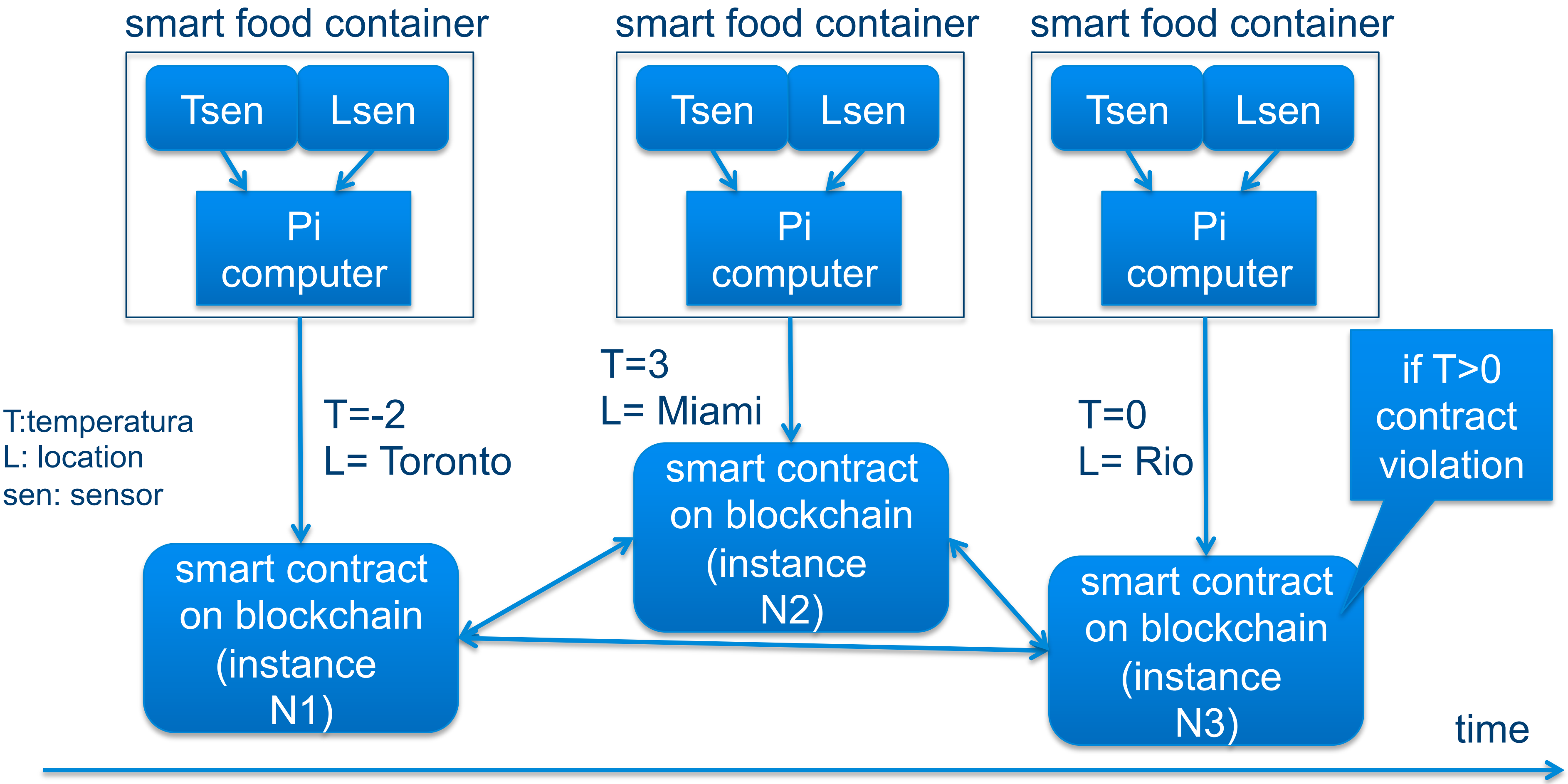


Ex of a contractual clauses

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

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

Food Policies Enforcement with Smart Contracts



smart food container

Tsen

Lsen

Pi computer

smart food container

Tsen

Lsen

Pi computer

smart food container

Tsen

Lsen

Pi computer

T:temperatura
L: location
sen: sensor

T=-2
L= Toronto

T=3
L= Miami

T=0
L= Rio

if T>0 contract violation

smart contract on blockchain (instance N1)

smart contract on blockchain (instance N2)

smart contract on blockchain (instance N3)

time

UNIVERSITY OF CAMBRIDGE

Is Blockchain Here to Stay?

- Yes, Bitcoin, Ethereum and other blockchains have been operating for years and has proved that the idea works?
- Yet, in my view, they is still at experimental stage and looking for the killing application.
  - There are hurdles to clear

Bitcoin Mining is Burning the Planet

- Bitcoin mining (computation required to validate a Tx) 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 Tx consumes 5 000 times more energy than a Visa Tx

Bitcoin is too slow

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

Quick response: real time applications: ex. car sensors

Bitcoin does not Scale Up

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

Tx/Sec

2000

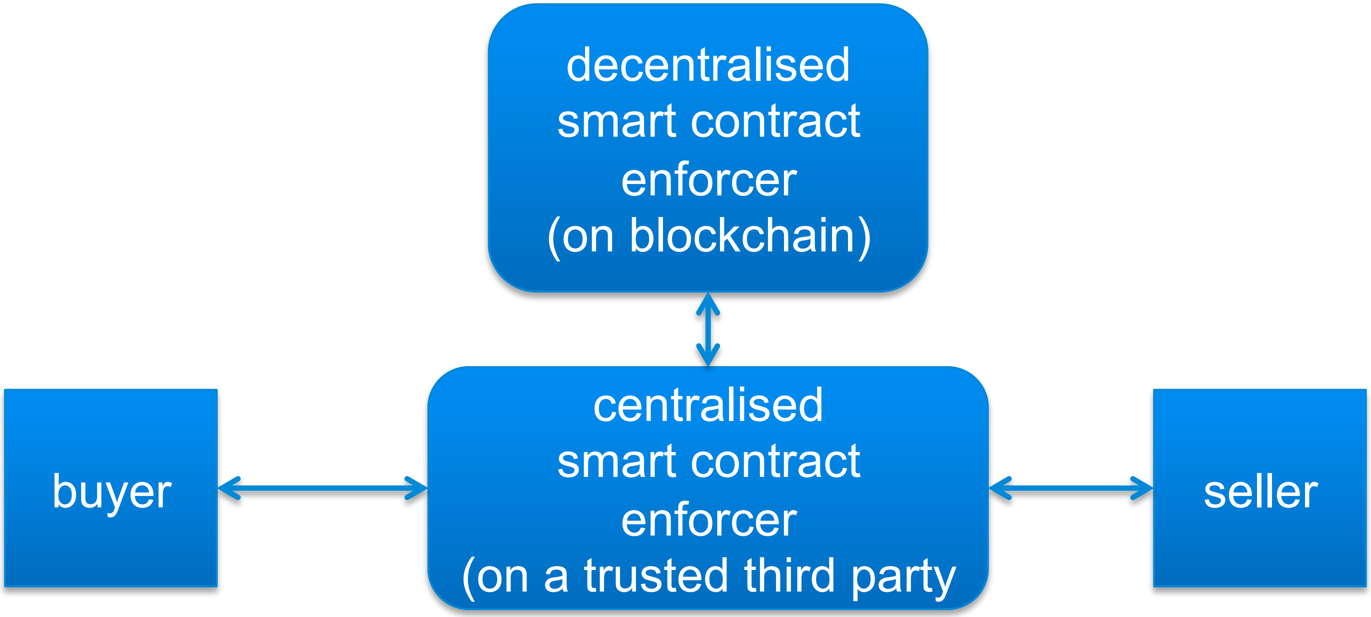
Visa

7

Bitcoin

Cambridge Potential Solution to Blockchain Limitations

- Use a hybrid (combined) solution:
  - centralised smart contract enforcement + decentralised smart contract enforcement.


decentralised smart contract enforcer (on blockchain)
buyer
centralised smart contract enforcer (on a trusted third party
seller

Conclusions

- The Bitcoin paper opened innovative business and research directions.
  - Blockchains and smart contracts (its two core concepts) are generic and can be used in the implementation of applications of several domains.
    - smart contracts and blockchains complement each other, however smart contracts can be used without blockchains and blockchains can be used without smart contracts.
    - Contracts have been the subject of research interest long time before Bitcoin (see http://www.cl.cam.ac.uk/~cm770/).
- Besides blockchain and smart contracts potential, one has to keep in mind that these technologies are currently at research state, thus their actual contribution to business applications is still waiting validation.

Discussion

- Questions and observations are very welcome.

References

- “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satosh Nakamoto, 2008.
- “Mastering Bitcoin”, Andreas M. Antonopoulos, O’Relilly, 2nd Edition 2017.
- “Feeding the Blockchain Beast”, P. Fairley, Spectrum. IEEE Oct 2017
- “On and Off Blockchain Enforcement of Smart Contracts”, Carlos Molina, … Jon Crowcroft, arXiv, May 2018.
- “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.
- Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser, 2015.
- “Trusting records: in Blockchain technology the answers?”, Victoria Louise Lemieux, Records Management Journal, V26, Issue 2016.