UNIVERSITY OF CAMBRIDGE

On the use of Blockchain and Smart Contracts in the Creation of Indelible University Certificates

Carlos Molina-Jimenez

Carlos.Molina@cl.cam.ac.uk

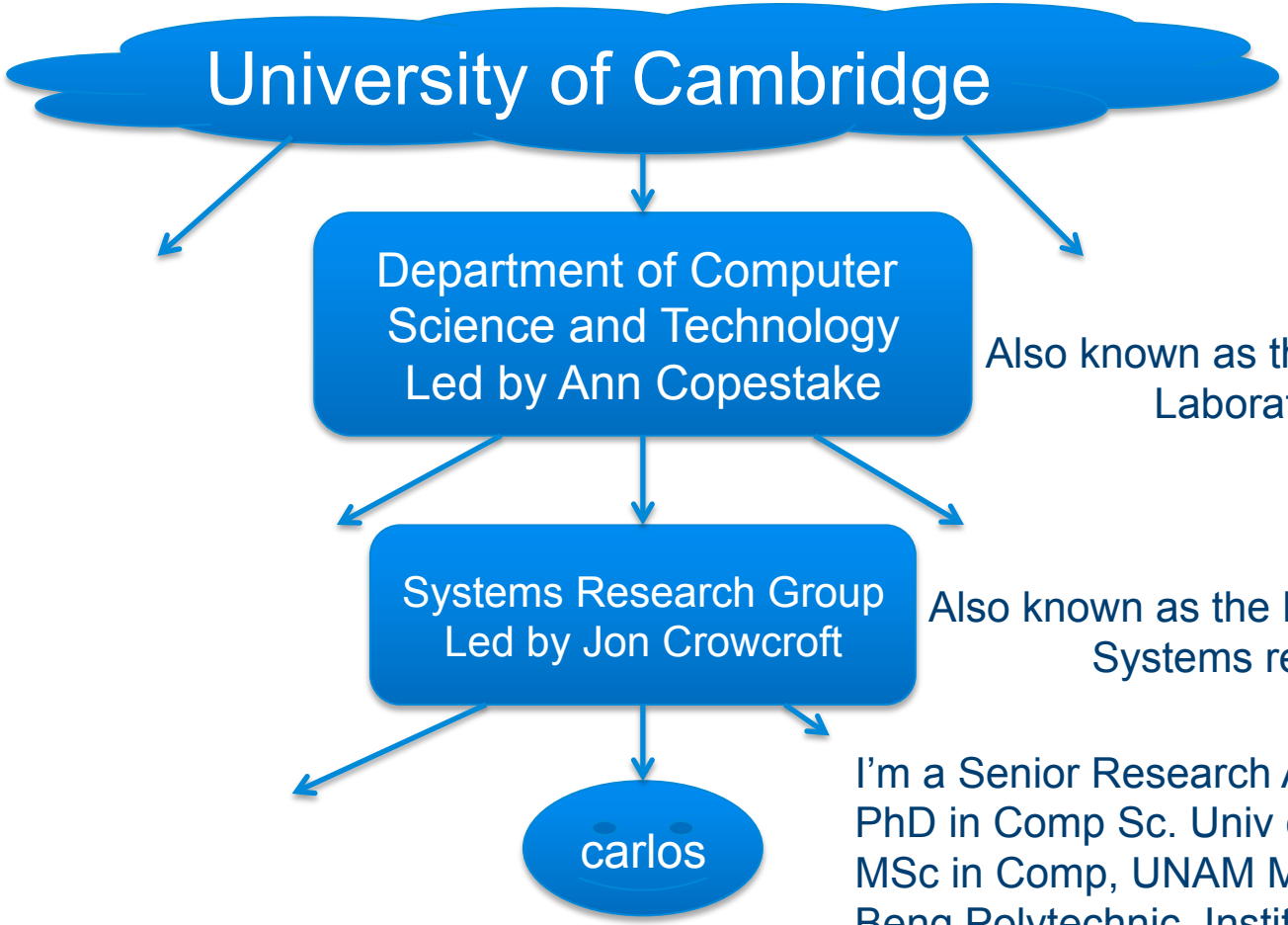
http://www.cl.cam.ac.uk/~cm770/

Department of Computer Science and Technology:

Computer Laboratory

University of Central Asia, Naryn 18 May 2018

My Research Group



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

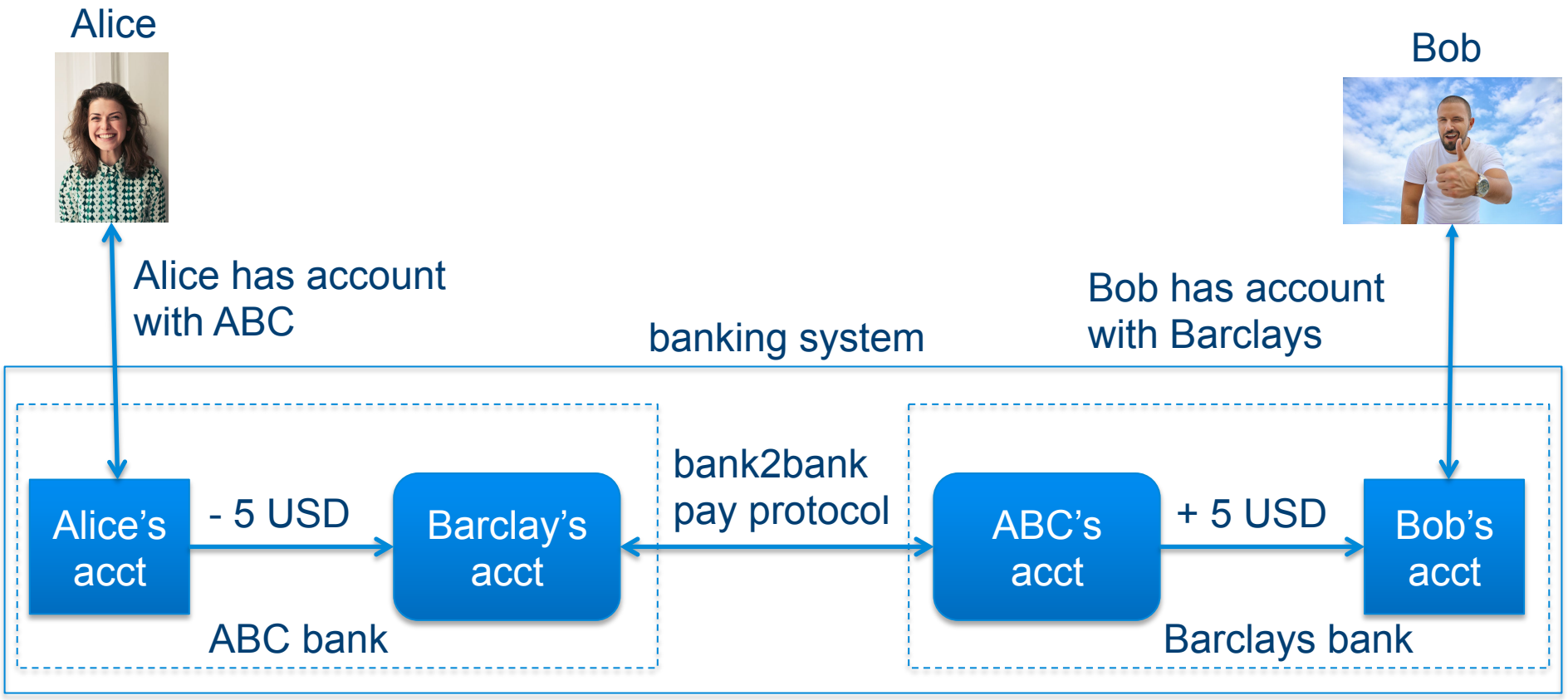
TESCON
Tools for Enforcement of Smart Contracts

2001 2014 2018 time

Why blockchain and smart contracts?

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

Money transfer: Traditional Bank-mediated Approach



Problems with Bank-mediated Transfers

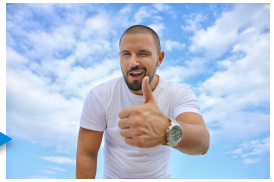
- It takes ages (several days).
- There is a exchange rate that the bank abuses.
- The bank transaction fees (typically 15 to 30 pounds).
- It excludes people without bank accounts.

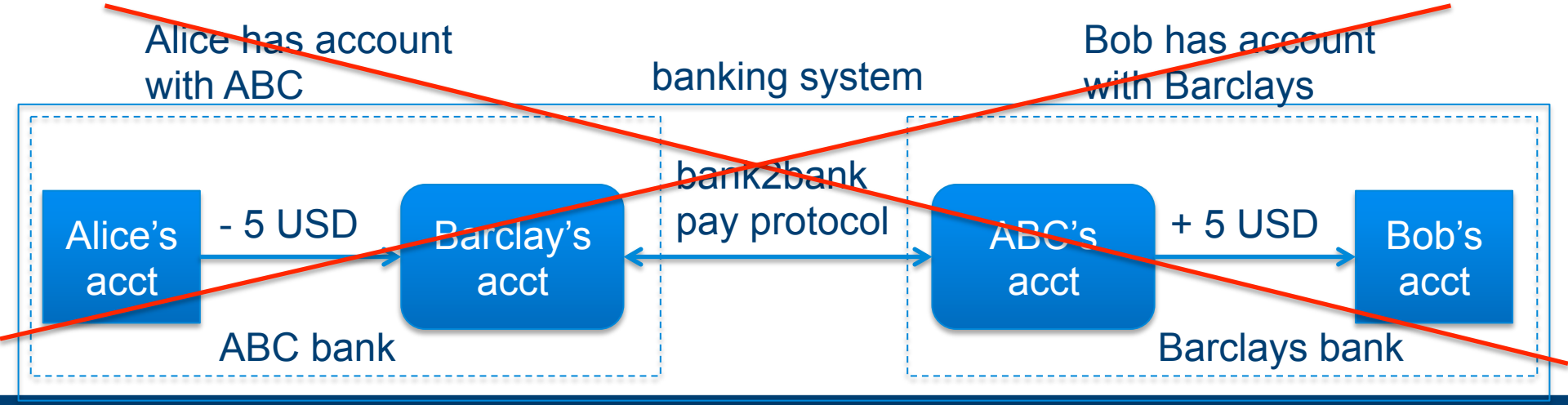
What Role does the Bank Play?

- 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 transactions: 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 Said Satoshi in 2008.

5 BTC

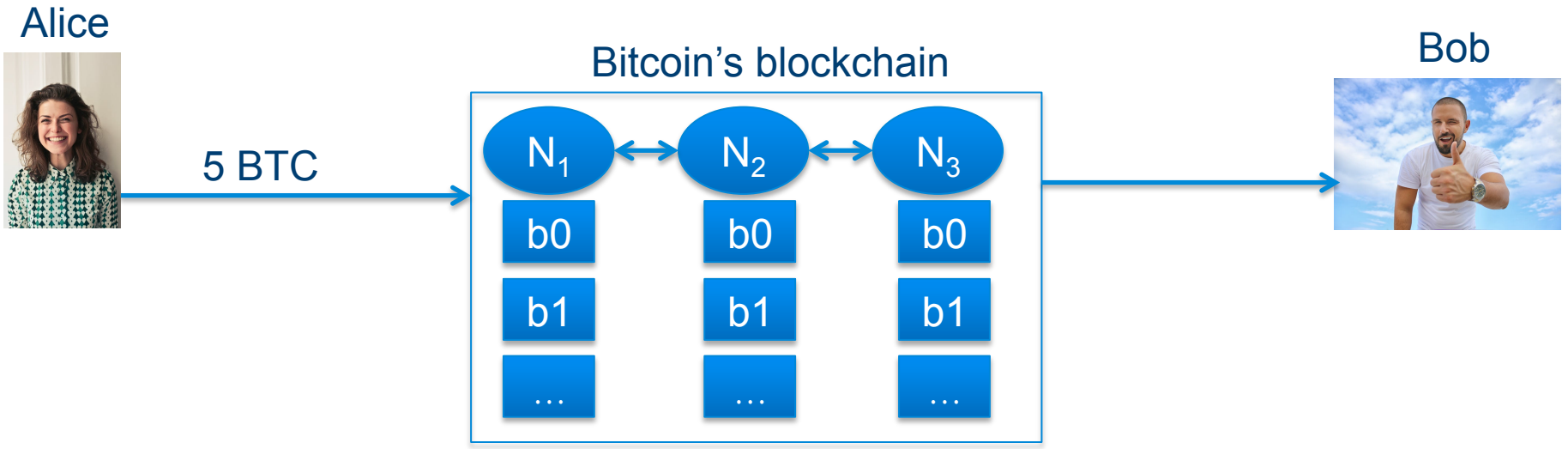




No Bank in The Middle

- 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,….

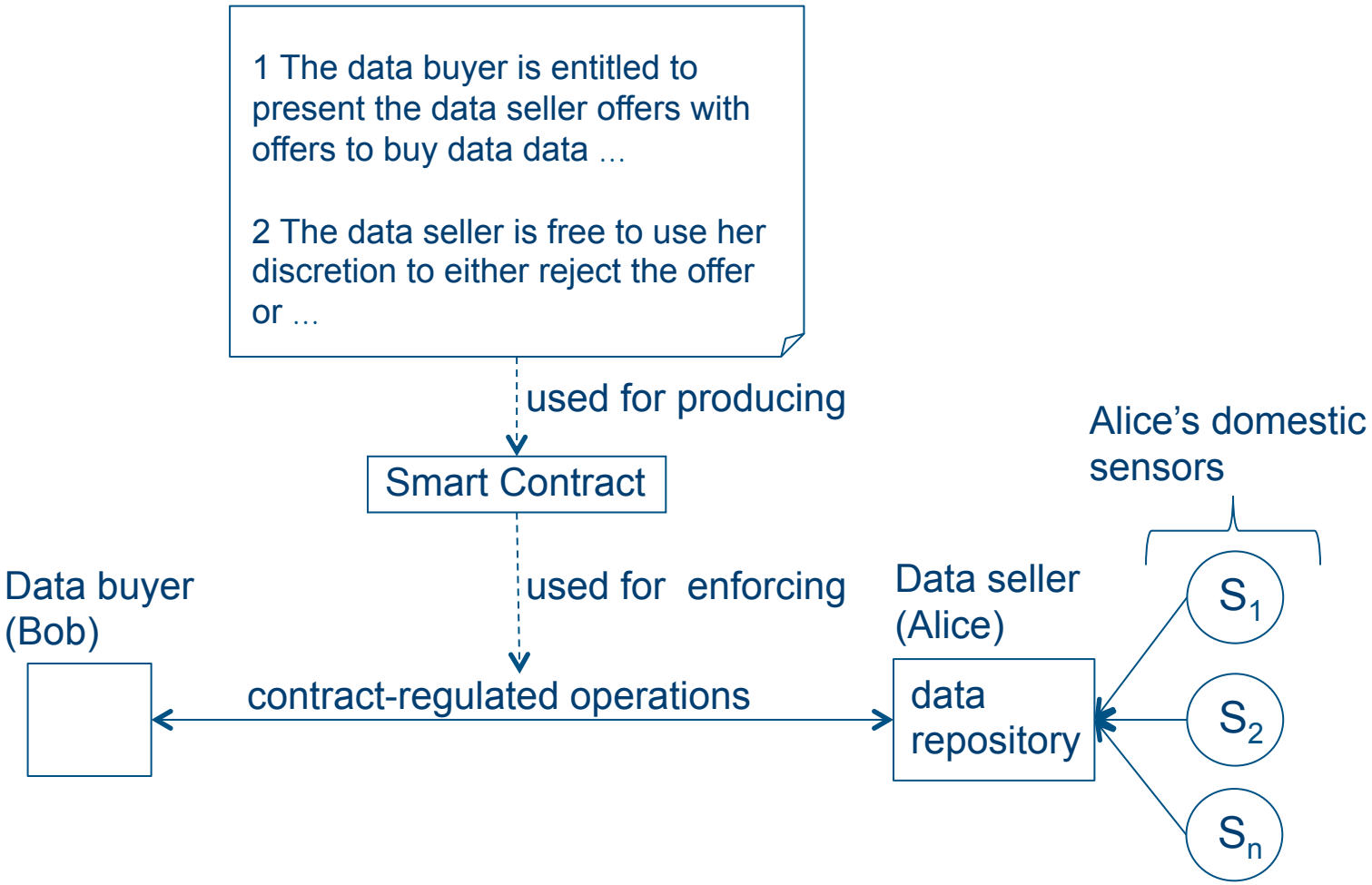
How did Bitcoin get rid of the Bank?



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

What is a Smart Contract?



Beyond Bitcoin's Cryptocurrency

- Bitcoin's cryptocurrencies was only the first application.
- It was enough to generate commercial and research interest based on blockchain and smart contracts

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

Competition Joins the Race

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

At the Heart of Blochain is Consensus

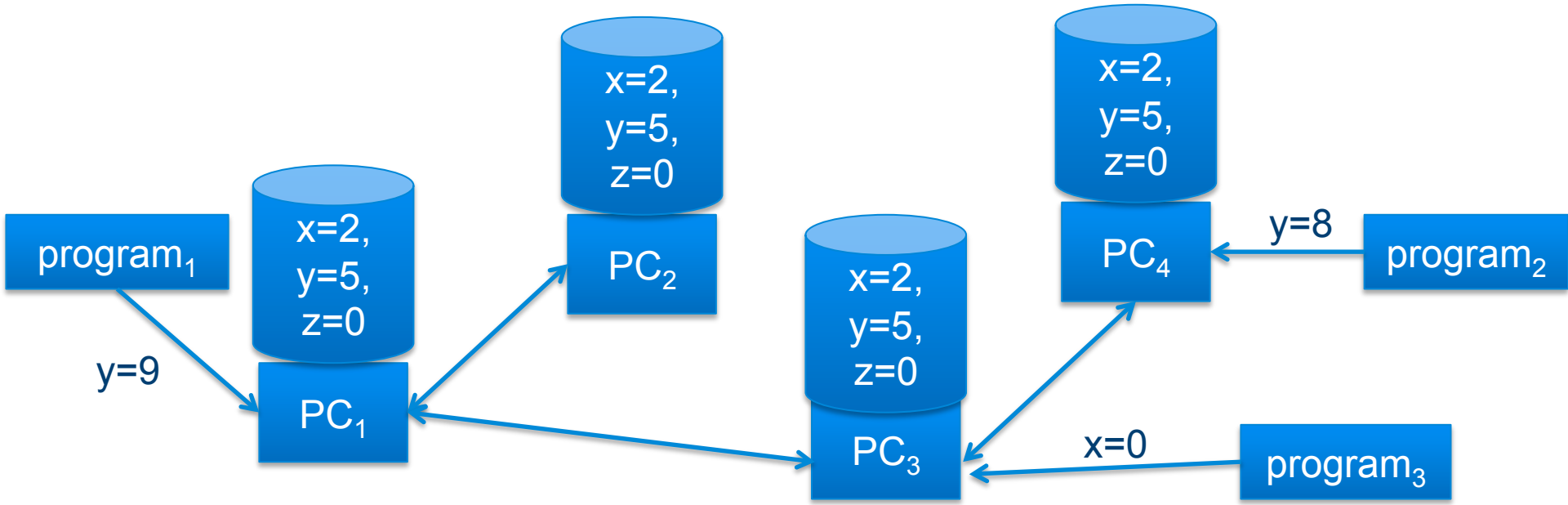
- Bitcoin offers a pragmatic solution to a very old distributed systems problem: consensus--- all about reaching agreements between N remote parties.

Ex1: 3x2+1= ?

Ex2: Let's meet to play football.

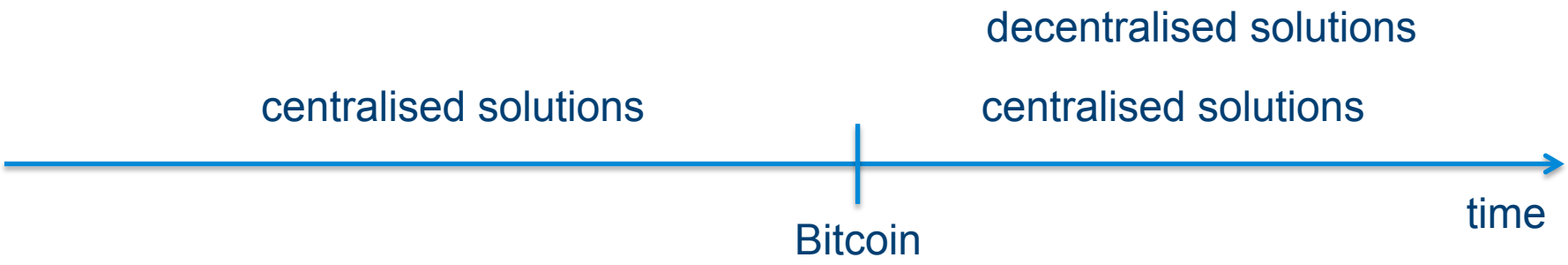
At the Heart of Blochain is Consensus

- 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).



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.



What are Blockchains Good for?

- I believe that it is a piece of science and technology with large potential beyond cryptocurrencies.
- I will discuss some example of innovative applications that can be built on the basis of blockchain and smart contracts.

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). See Ref [8] and [9].

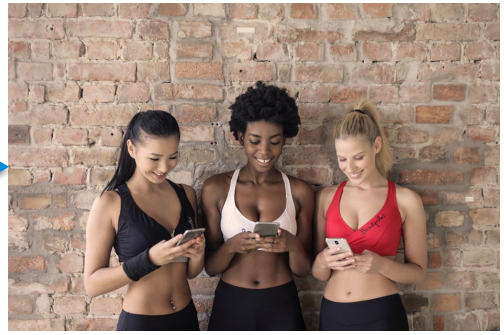
Records: University Certificates on Blockchain

1. Alice passed her final exam.

blockchain

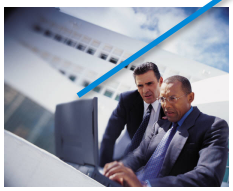
Date: 5May2018
Name: Alice
Title: Computer Eng

read



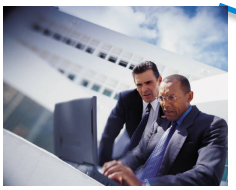
3. Anybody can see it. Is this OK?

2. Her examiners place certificate in a blockchain



Univ Certificate on Blockchain with a Smart Contract

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



blockchain

Date: 5May2018
Name: Alice
Title: Computer Eng

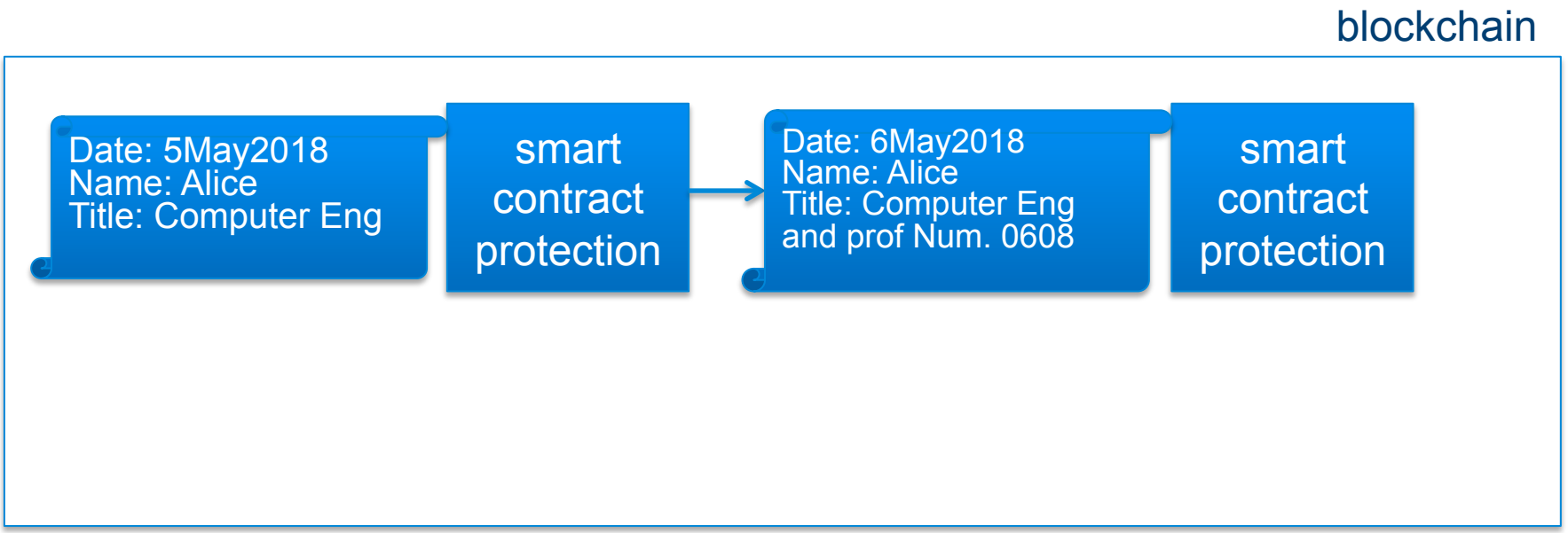
smart contract protection

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

2. Only some people can it it.

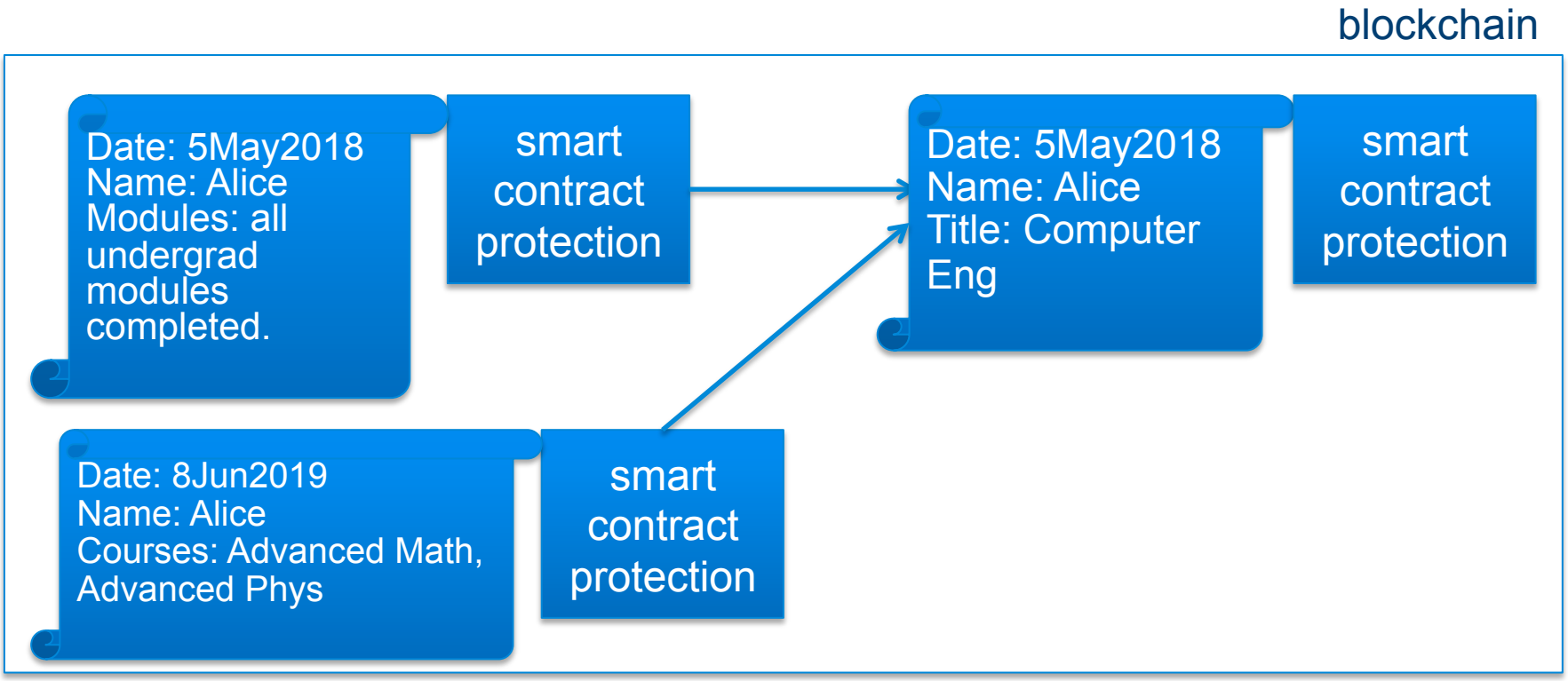
Smart Contracts can Help Create Records from Records automatically and systematically: ex 1



Ex of a contractual clauses

C1: A Comp Eng degree entitles the bearer to a professional number.

Smart Contracts can Help Create Records from Records automatically and systematically: ex 2



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.

Conclusions: 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

The State of the Art

- Some progress has been made in this direction by University of Nicosia (see Ref [10]).
  - The choice of Bitcoin (againts other alternatives like Ethereum that supports a Turing complete language for contract implementation) needs critical examination.
- In my view, the technology is still at research state.

Questions?

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/