UNIVERSITY OF CAMBRIDGE

Carlos Molina's Research Interests

Introduction to University of Cambridge and its Department of Computer Science and Technology (the Computer Laboratory)

Carlos Molina-Jimenez

Carlos.Molina@cl.cam.ac.uk

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

Unijui 17 Oct 2019

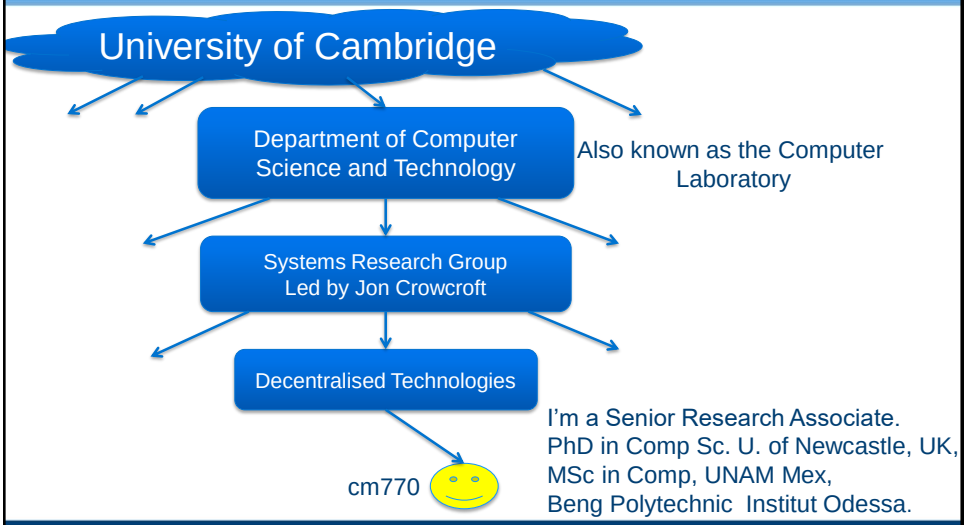
We Live in a Centralised World

- Governments, banking services, health services, Internet services, and other services are centralised systems.
- A system is centralised if it includes a single authority that we must trust .
  - It controls and decides its operation and destiny.

Too Much Power and Responsibilties is Bad for your Health

- Many systems and unnecessarily centralised.
- Let **us break centralised systems** before their single points of authority accidentally or intentionally break them.
- Why and How?
- I have some ideas.
  - Before discussing them, let me tell you about myself.

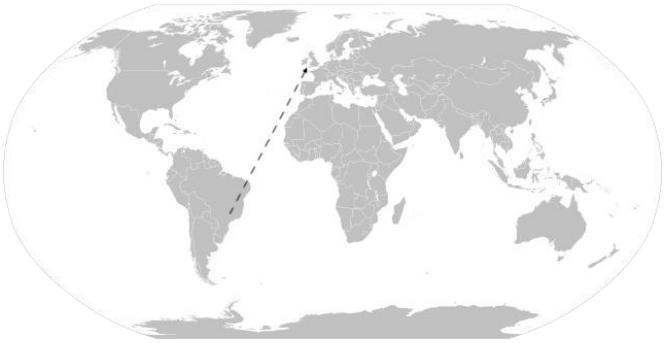
My Research Group and Background



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

The University of Cambridge is in GB

- Founded in 1209, Cambridge is the second-oldest university in the English speaking world.
  - Located in GB.



The University of Cambridge is not far from London

- Located in GB, in the city of Cambridge.
- About 50 min from London by train (30 pounds return).

The University of Cambridge and the City

University of Cambridge: how big is it?

UNIVERSITY OF CAMBRIDGE

- 19 955 students.
  - 12 340 undergraduates.
  - 7 610 postgraduates.
- Academic staff 3 615 (Vice-Chancellor Stephen Toope).
- It has 31 colleges: Trinity, Saint John's, King's, Queen's, etc.
- 117 Nobel Laureates.

The University of Cambridge: Trinity College

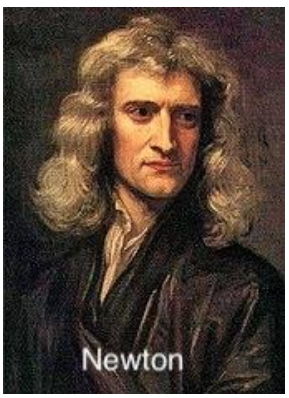
UNIVERSITY OF CAMBRIDGE

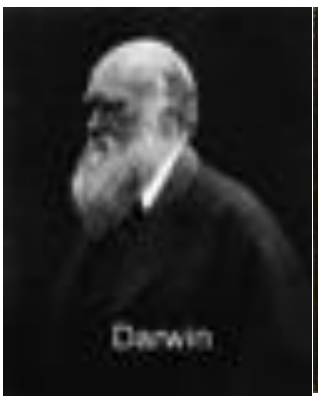
The University of Cambridge: Kings's College

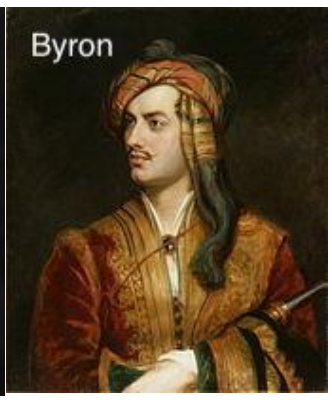
UNIVERSITY OF CAMBRIDGE

The University of Cambridge: Queen's College

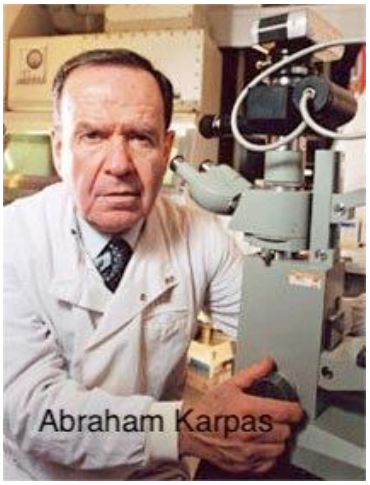
The University of Cambridge: people (1)







The University of Cambridge: people (2)

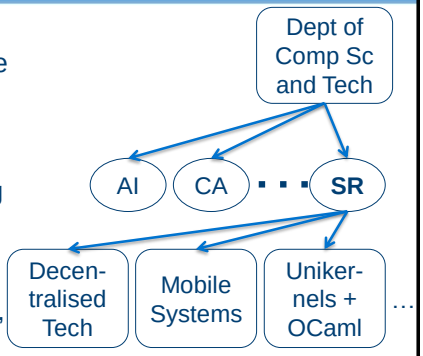


The Department of Computer Science and Technology

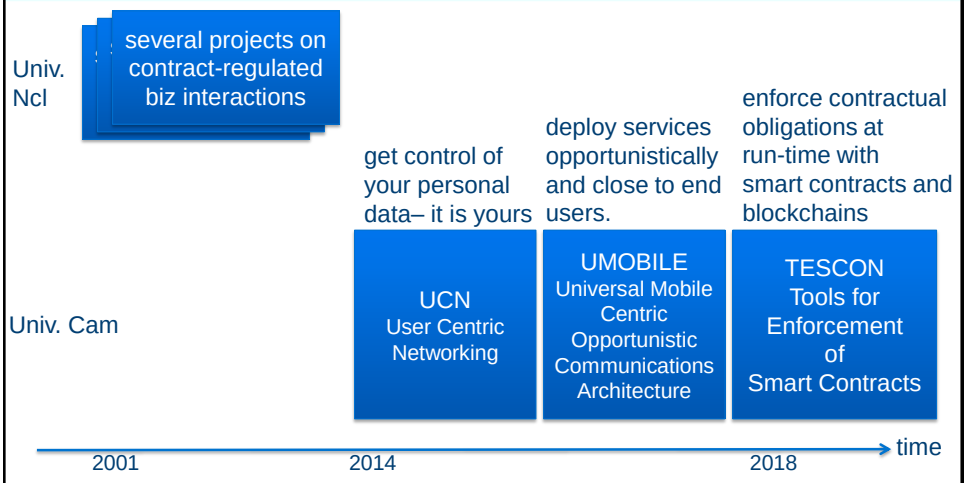
- The Computer Laboratory consists of 41 academic staff, 29 support staff 5 research fellows, 81 post-doctoral research workers and 119 PhD students.

Research Directions in the Computer Lab

- Research groups: Artificial Intelligence (AI), Computer Architecture (CA), Digital Technology, Graphics and Interaction, Natural Language and Information Processing, Programming Logics and Semantics, Security and **Systems Research (SR)**.
  - System Research Group: networks, operating systems, multimedia, mobile and sensor systems, unikernels, distributed systems, decentralised technologies.



My Research Experience



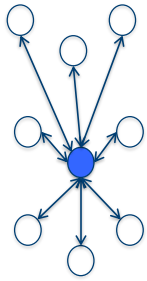
My Current Research Focus

- I'm currently focused on **decentralised technologies.**
  - We have a sub-group working on the topic.
  - It is a sub-group of the Systems Research group.
  - We set it up recently to be led by Prof. Jon Crowcroft.

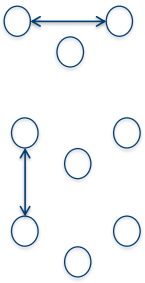
Decentralisation

- What is it?
  - Concept? Architecture? Technology?
- Why does it matter?
  - What are advantages and disadvantages?
  - What are the alternatives?
- Who needs it?
  - Individuals (like me Carlos Molina), companies, governments?

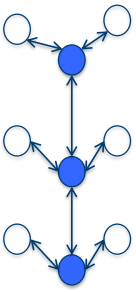
Centralised vs Decentralised Systems



a) Centralised



a) Fully dentralised
(peer to peer or P2P)



a) Decentralised

Authority in control of the system. We must trust it.
Ex. Bank, government,

UNIVERSITY OF CAMBRIDGE

You Need to Trust a Single Authority

- Imagine that Alice is user and that Bob is the single authority of the system (for ex. Internet provider, Health service, Energy supplier).
- Alice must trust Bob that he
  - is capable of keeping the system working correctly.
  - will not abuse his authority: for ex. overcharge or neglect her.
  - will deploy the systems when and where it is need.
    - for ex, that the system will not break down.

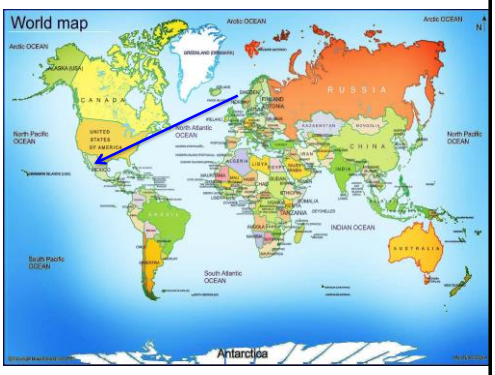
UNIVERSITY OF CAMBRIDGE

Does Centralisation Impact my Life?

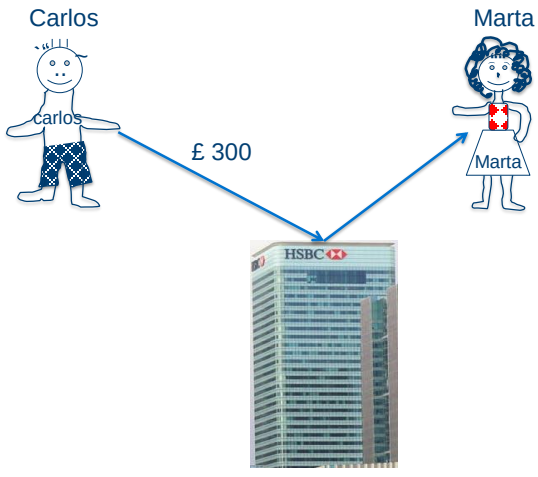
- Yes, it does.

I'd been invited to a XV b/day party!

Contributions in **cash** are very welcome!

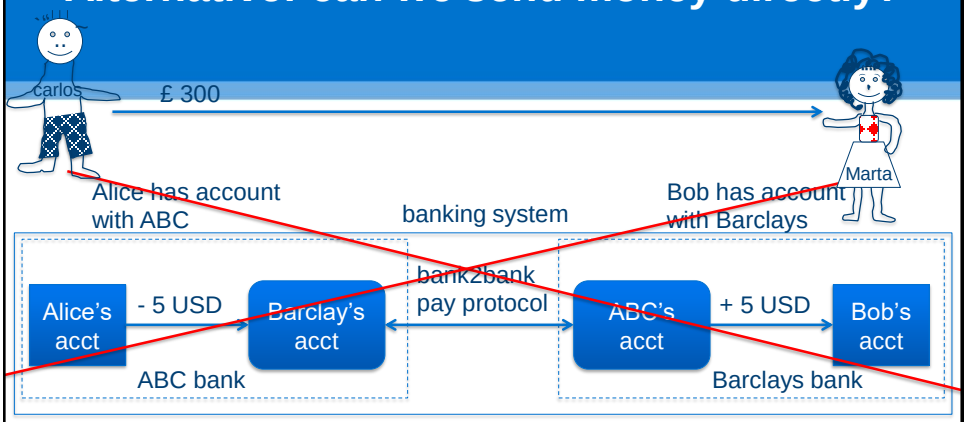


Money Transfer: Traditional Bank-based Solution



This model works fine when there is a bank and Carlos and Marta have bank accounts.

Alternative: can we send money directly?

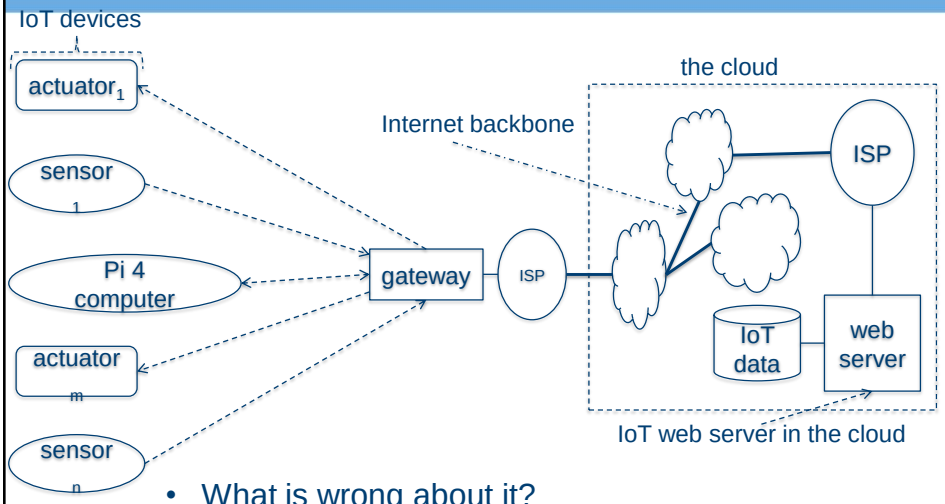


- Yes, said Satoshi Nakamoto (the inventor of Bitcoin) in 2008.
- Bitcoin demonstrated that technology is now advanced enough to build a decentralised cryptocurrency system.
- Let us get rid of the bank!

Why do I want to Get Rid of the Centralised Bank

- They change high fees.
- Bank transactions takes several days to complete.
- Their service fails.
- They have access to my personal data information: address, financial status, sex, shopping habits, etc.
- More relevant:
  - There might not a a bank in my village.
  - If there is one, I might not have a bank account because I am poor.

Centralised Solution to Connect IoT Devices



- What is wrong about it?

Realistic examples where Centralised Systems Fail

- The newly elected Mexican president aims at delivering social money directly to 22 million people directly, i.e., through G2P (Government to People) transactions.
  - Elderly, disable, students, indigenous, etc, people, from neglected social classes.
- This is a technically challenging operation.
  - Most of the beneficiaries live in remote regions like Costa Chica of the Guerrero state.
  - I know the region and can tell you about it.

UNIVERSITY OF CAMBRIDGE

San Marcos Guerrero

San Marcos (12,500 inhabitants).

- head of Municipality of the same name.
- Door to the Costa Chica: land of the neglected population of African descendants.

The Programme Needs to Reach Neglected People

Aim: The Global Picture

centralised government

UNIVERSITY OF CAMBRIDGE

We Need to Reach People from Remote Villages with No Internet

We Need to Deliver Money to People with no Bank Accounts

We Need to Identify People with no Legal Identity

Escuela, Cerro De Pesqueria, San Marcos Gro.

Do we have Technology for building Decentralised Systems?

- Yes, said Satoshi Nakamoto (the inventor of Bitcoin) in 2008.
- He has demonstrated it with a practical implementation.
- How did they build the Bitcoin platform?
- There are several technologies for implementing decentralised systems:
  - edge-cloud,
  - peer-to-peer networks
  - community networks
  - blockchain.
  - etc.

Bitcoin

- Bitcoin is the name of a blockchain platform (a system composed of hardware + software + network) developed for conducting **decentralised financial transactions**, without the bank in the middle.
- Bitcoin is a decentralised financial system.

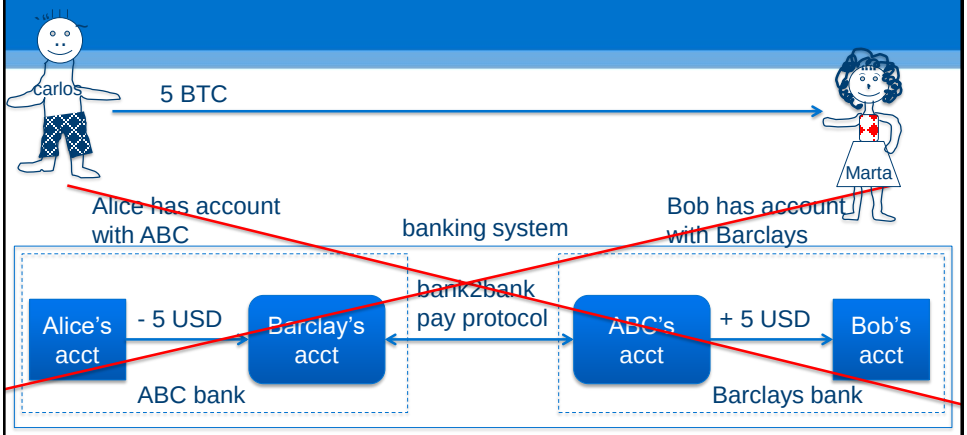
UNIVERSITY OF CAMBRIDGE

Bitcoin– the Blockchain Platform that Shook the World in 2008

- Until 2008 the concept of decentralisation was meaningful only to computer scientist working on distributed systems.
- Satoshi Nakamoto shook the academic, industry and government sectors with his pioneering paper: *Bitcoin: A Peer-to-Peer Electronic Cash System.*
- What is the novelty about Bitcoin?
  - Bitcoin is a creative aggregation of technologies developed in the 1980 including digital money, immutable file systems, cryptography, consensus algorithms.
- **What is all the fuzz about Bitcoin?**
  - It is a decentralised platform that enable its user to send money to each other without the bank in the middle.
  - It inspired the development of decentralised systems in other application domains.

UNIVERSITY OF CAMBRIDGE

Money Sending in Peer to Peer Manner



- Carlos is able to send 5 BTC (the cryptocurrency used in the platform) to Marta though the Bitcoin Platform and without the bank mediating and imposing fees and conditions.

UNIVERSITY OF CAMBRIDGE

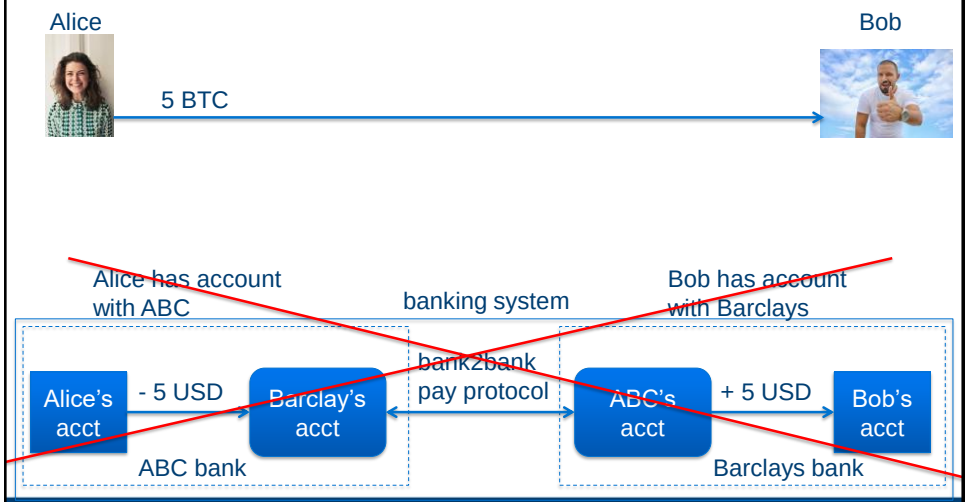
How does the Bank Look After Transactions?

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

UNIVERSITY OF CAMBRIDGE

44

Bankless Transfer over Bitcoin

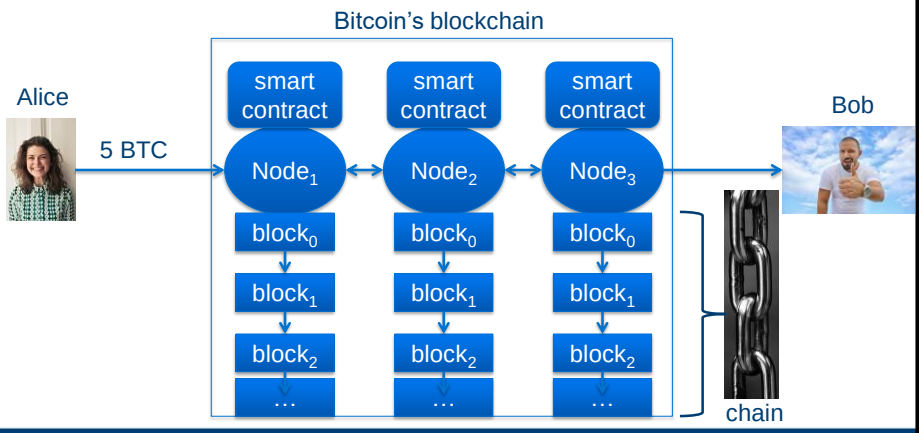


How does Bitcoin Keeps Track of Transactions?--- textual explanation

- 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 a DL for storing blocks that groups transactions and smart contracts that verify conditions to declare transactions valid.



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 other decentralised applications.

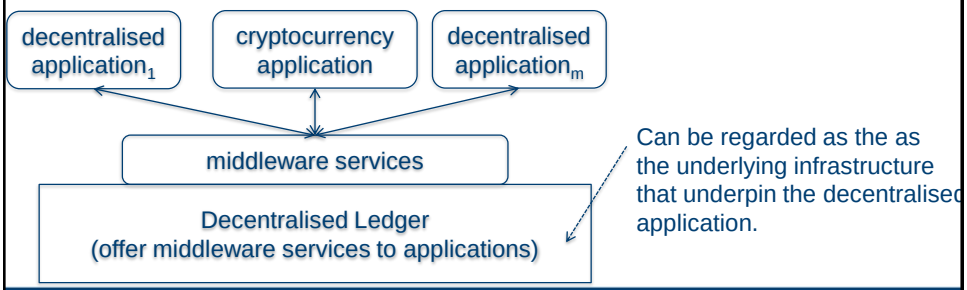
New business models (banking, health, …) and new computation paradigms, new…

Competition Joins the Race

- Bitcoin shook the banking and financial system.
- Competition appeared quickly.
  - Blockchain platforms: Ethereum, Hyperledger, IOTA, Fetch.io, TODAQ, etc.
  - They cover a wide spectrum of application domains, like, cryptocurrencies, IoT devices, real state properties, health-care, energy, etc.
- At the heart of these blockchain platforms is a decentralised ledger.

Services of the Decentralised Ledger (1)

- The DL offer services that can be used for building applications from a wide range of application domains, including cryptocurrencies.



Services of the Decentralised Ledger (2)

- **state-awareness:** keeps track of state evolution and imposes conditions on state changes.
- **indelibility**: collects records and make them immutable for good. New records are appended to the tail.
- **non-repudiation:** a party cannot denied the execution of his actions.
- **transparency:** exposes records for public examination.
- **anonymity (or pseudo-anonymity):** protects the identity of the executors of operations (transactions).
- **ubiquity:** provides access to the system regardless of locations.
- **consensus:** synchronise the state of the replicated components of the system.

Indelible Records on Blockchain

- The society 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).

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

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

smart contract protection

Date: 5May2018
Name: Alice
Title: Computer Eng

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

Some Research

Some topics of current research interest.

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.

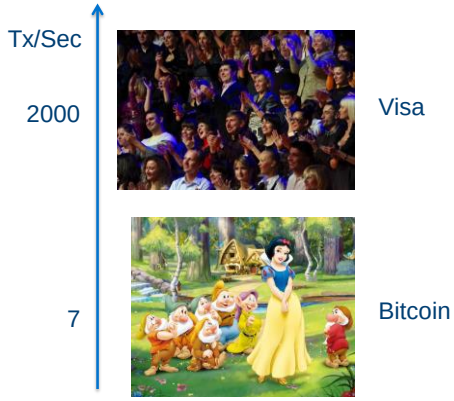
Bitcoin is too slow

- 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

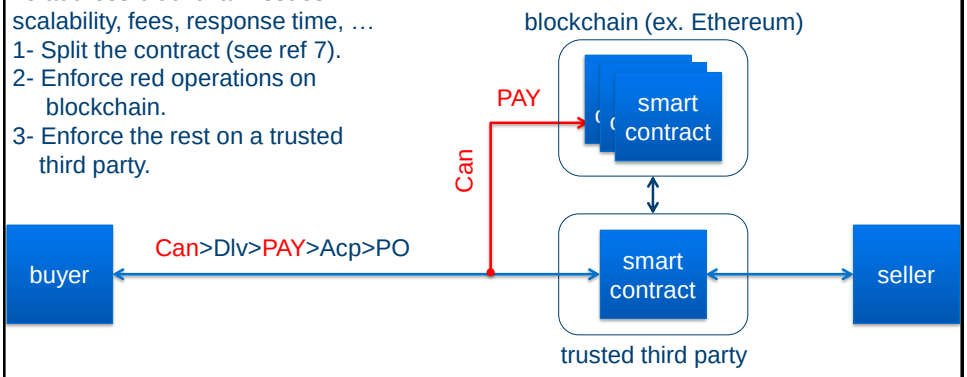
Bitcoin does not Scale Up

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



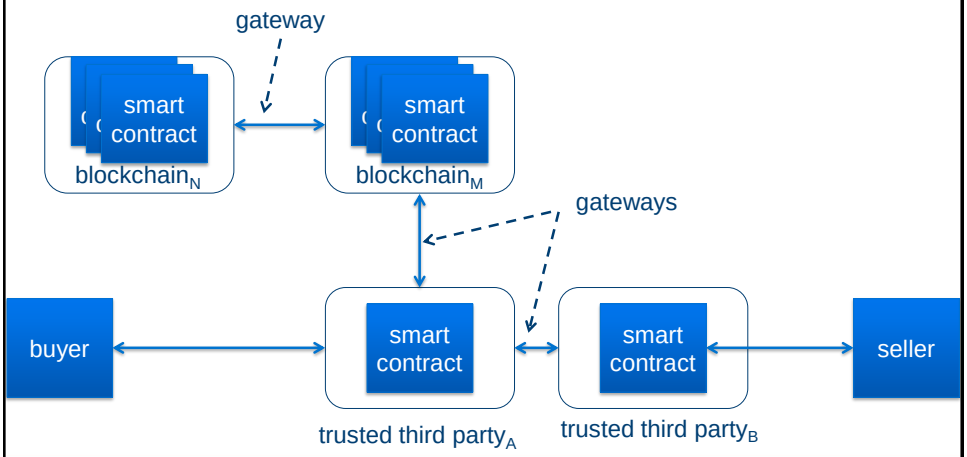
Cambridge Potential Solution to Blockchain Limitations: hybrid approach

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

Future: On and off—blockchain Computation Paradigm



TODA-Q is Developing Technologies for the Digital Economy

- I have been collaborating with TODAQ (pronounced TODA Q).
- They are based in Toronto (https://todaq.net/index.html).
- One of their central arguments
  - In the past individual owned tangible objects only.
    - Houses, cars, bikes, TVs, chairs, watches, horses, cats, …
    - We had technology for trading them: buying, selling, re-selling, given as presents, renting, borrowing, etc.
  - The number of digital objects that an individual owns is already greater than the number of his tangible objects.
    - Photos, music, videos, emails, personal data, …
    - We do not have technology for trading them.

TODAQ Solution

- They are implementing a “blockchain” aimed at trading both tangible and digital objects.
- Their “blockchain” is a set of protocols called TODA.
  - It is a decentralised technology. No mediator interfering in the middle of the two trading parties.
  - Strictly speaking, it is not a blockchain as it is not underpinned by a blockchain data structure.
  - They use a data structure based on **Merkle Trees.**
- Why Merkle trees?
  - To avoid several of the technical problems that afflict Bitcoin, Ethereum and other decentralised platforms that are underpinned by blochain data structure.
  - Scalability: blockchain suffer from scalability.

UNIVERSITY OF CAMBRIDGE

Fundamental TODAQ’s Concepts

- **uniqueness**: Each digital object (for ex a photo of Alice’s cat) is globally unique and identified by a global ID.
  - The creation of a copy of the photo creates another digital object (with a different ID).
- **ownership**: the photo is owned by Alice.
- **transfer of ownership:** if she wishes to, Alice can transfer the ownership of the photo to Bob.
  - They clearly distinguish between transfer of ownership (always a digital document) and transfer of the actual object (it can be tangible or digital).
  - After a successful transfer of ownership (of the difital document, Bob owns the photo.
    - The current physical location of the object is irrelevant.
  - Because Bob owns the photo, he can keep it, transfer the ownership to Clare or back to Alice.

UNIVERSITY OF CAMBRIDGE

E-commerce exchange

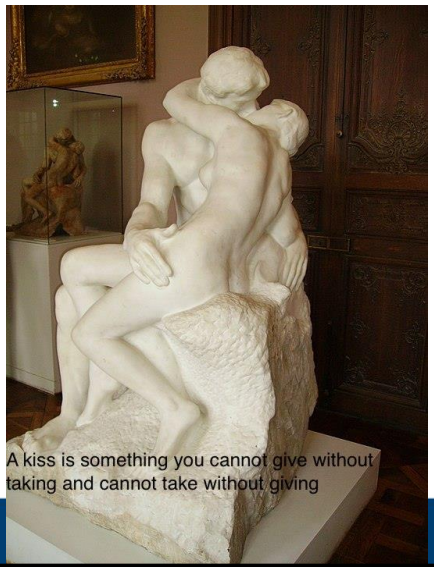
- The aim of a commercial transaction is usually an exchange of one

  item for another.

- For ex, a payment for an item.
- In bartering, an item is exchanged for another item of the same value.
- An important security requirement on exchanges is **fairness**.

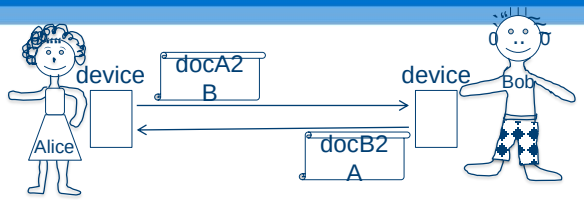
UNIVERSITY OF CAMBRIDGE

Fair Exchange Protocols– a kiss



UNIVERSITY OF CAMBRIDGE

Fair Exchange Assumptions



- Assumptions:
  - Alice and Bob operate independently.
  - Their devices are logically and physically separated.
  - Docs are transferred by means of executing two complimentary operations *give* and *take* operations. Ex. *% give docA2B* and *% take docA2B*.

UNIVERSITY OF CAMBRIDGE

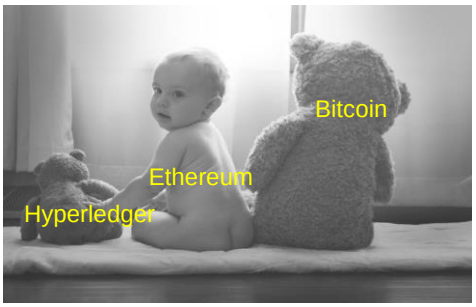
Conclusions

- Decentralised technologies open new business and research opportunities.
  - New applications can and will be developed based on decentralised architectures.
    - These new applications will co-exist with their centralised equivalents and compensate each other.
      - By the way, to clarify, I don't want to get rid of the bank, I only want to build another alternative system.
  - Use them carefully: only where you need them.
  - They are only emerging.

UNIVERSITY OF CAMBRIDGE

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

The End

- Questions are welcome.

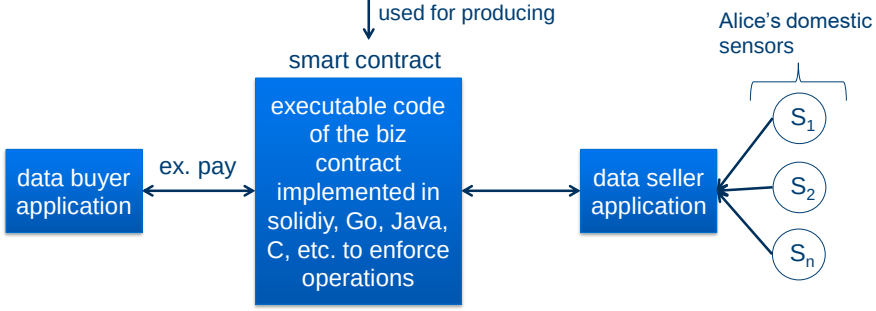
What is a Smart Contract?

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 …

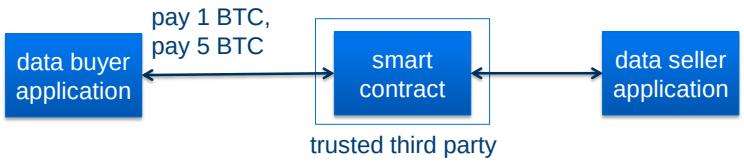
used for producing

smart contract



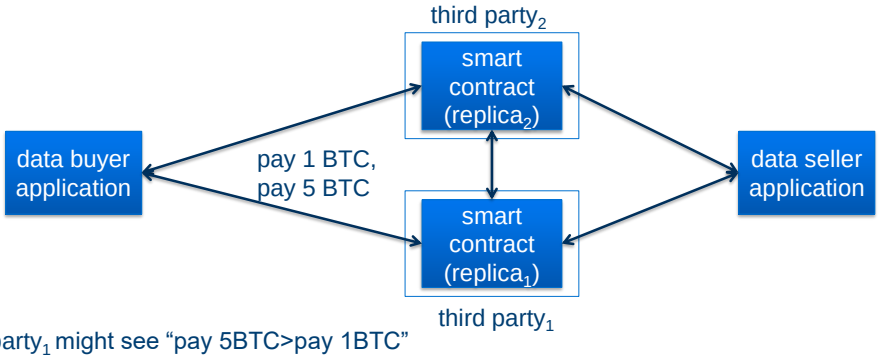
What is a Smart Contract: where to deploy it?

1) In a single trusted third party



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

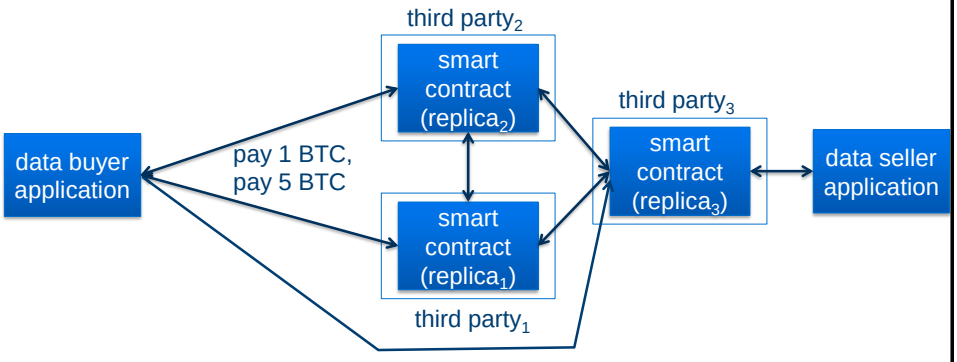
2) If data buyer and data seller cannot find a trusted third party they can use two untrusted third parties.



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)?

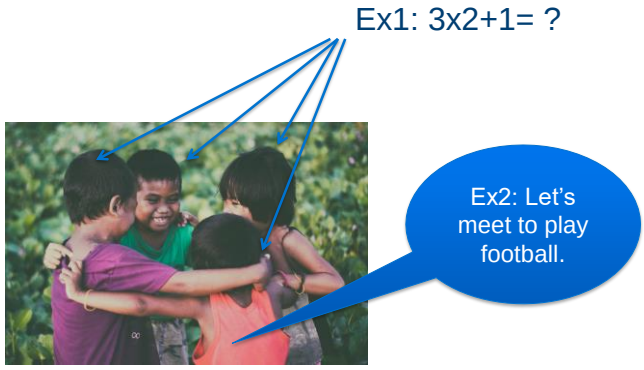
2) Replicate the smart contract in many untrusted parties



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.

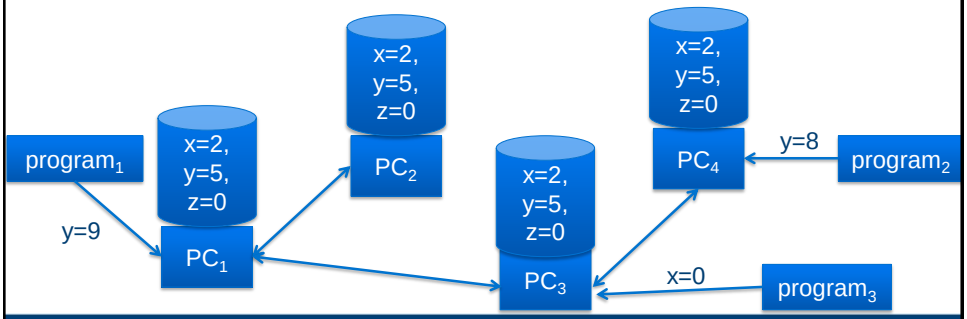
At the Heart of Blochain is Consensus

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



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).

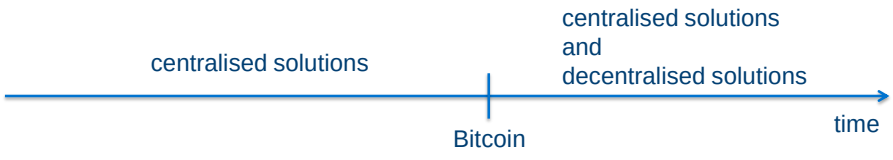


Advantages and Disadvantages of N-party Deployment

- 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

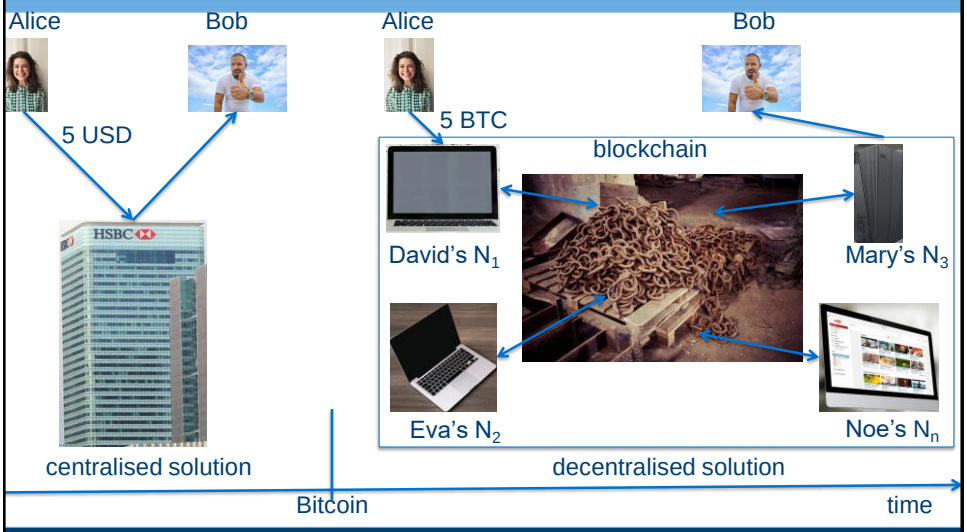
- The solution to this problem took the research community by storm.
- We are devising Bitcoin-based solution to old and new problems.



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



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?

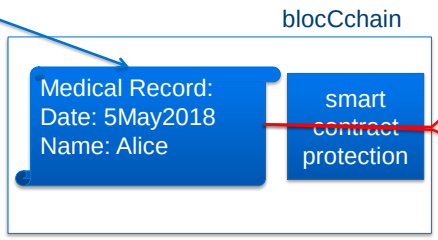
- Universities might disappear, records need to persist.
  - The Polytechnic Institute of Odessa has disappeared! ---changed its name to Odessa National Polytechnic University.
  - Where are the schools documents issued in Crimea?--- are they now in Kiev or Moscow archives?
- Some Mexican politicians 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

Medical Record on Blockchain with a Smart Contract

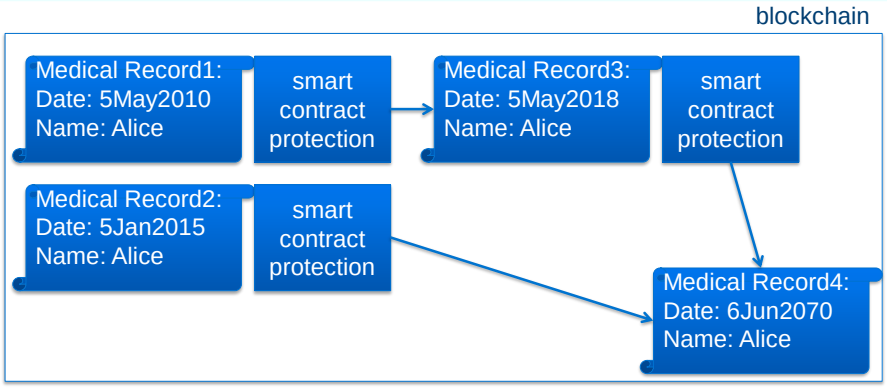
1 Alice's Dr places medical record on blockchain but protected by a smart contract.



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

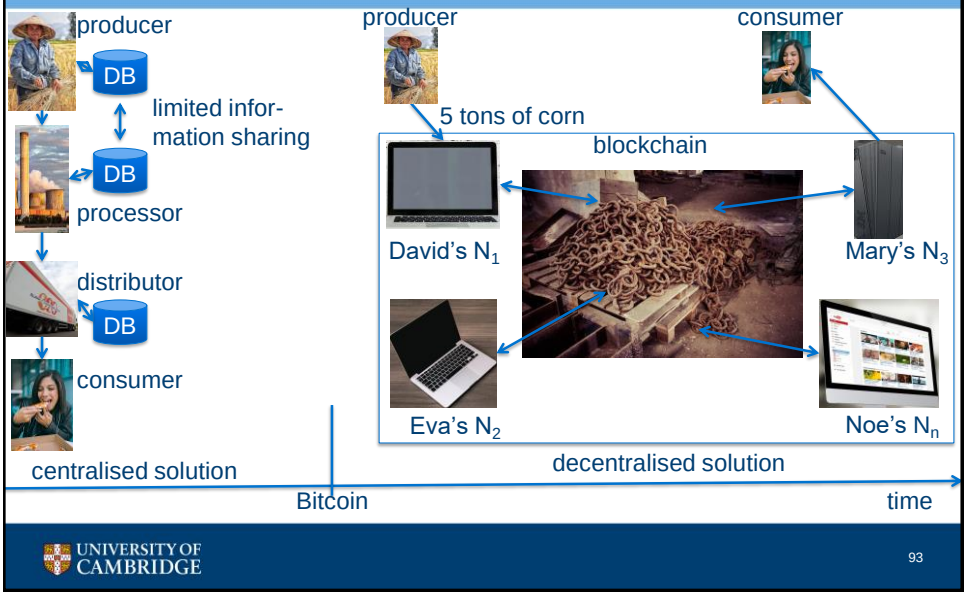


Ex of a contractual clauses

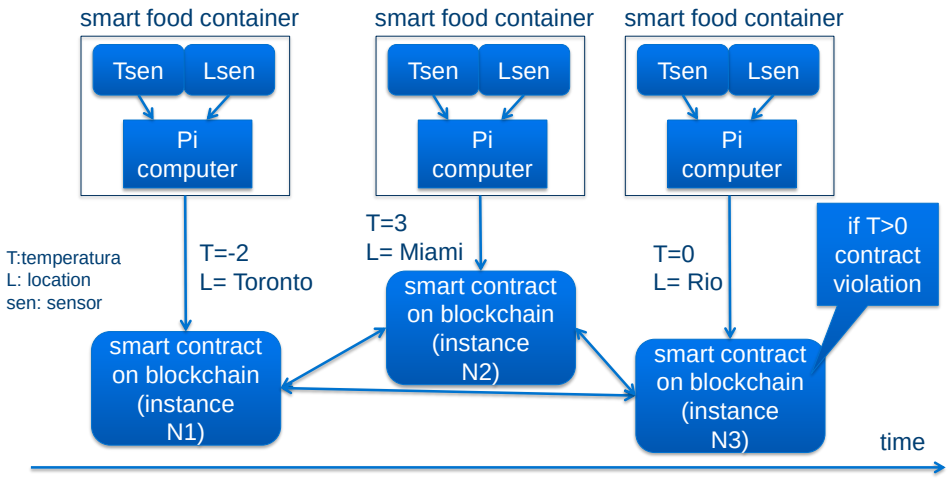
C1: On Alice's 18th b/day create Med Record3.

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

Life before and after Bitcoin: supply chain



Food Policies Enforcement with Smart Contracts

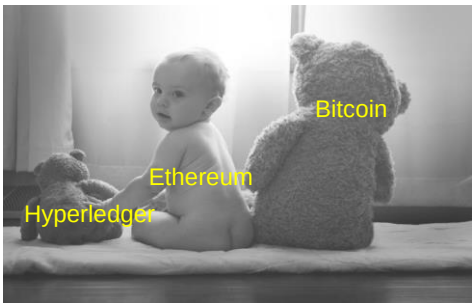


Cheap Liquidity Cryptocurrency Cash in Supply Chain (see sweetbridge.com)

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.

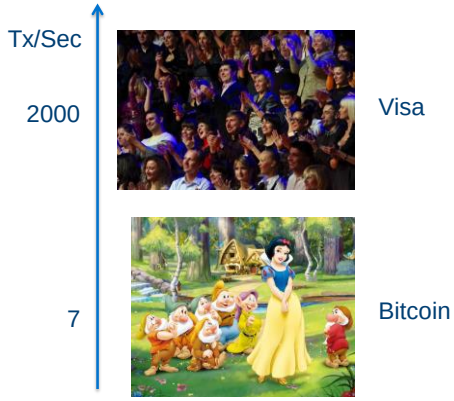
Bitcoin is too slow

- 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

Bitcoin does not Scale Up

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

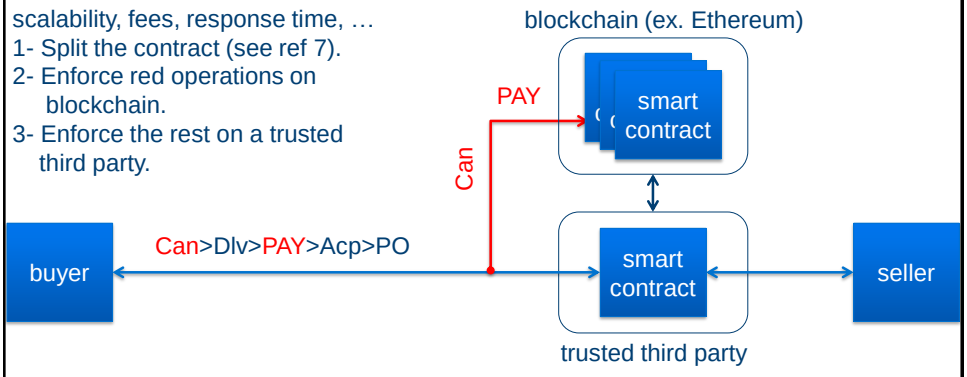


Cambridge Potential Solution to Blockchain Limitations: hybrid approach

- 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

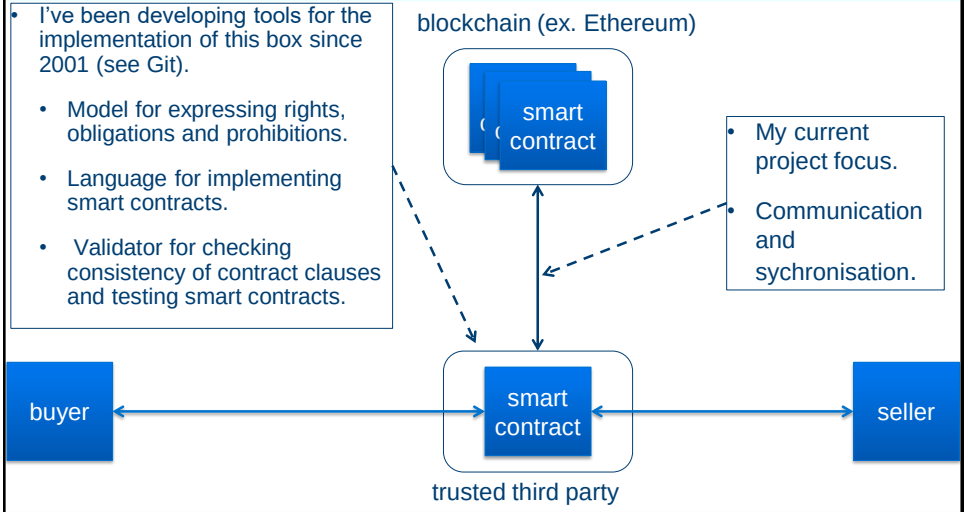
To address blockchain issues:
scalability, fees, response time, …
1- Split the contract (see ref 7).
2- Enforce red operations on blockchain.
3- Enforce the rest on a trusted third party.



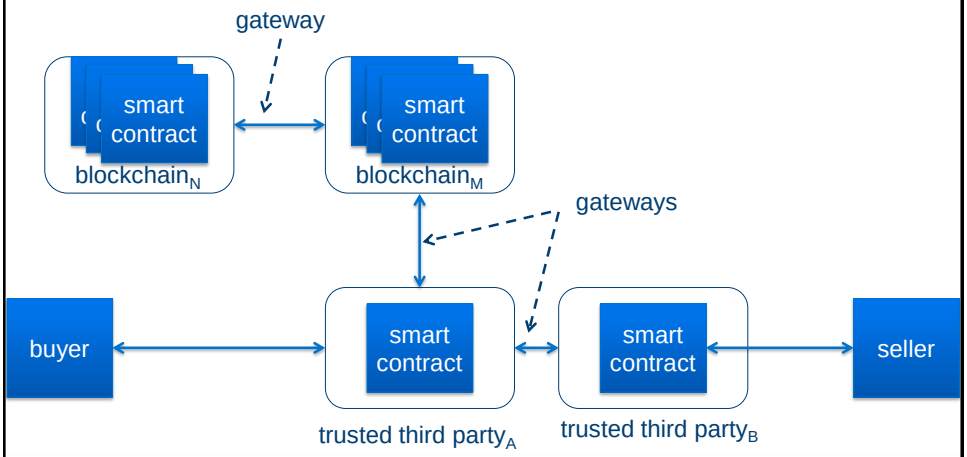
PO=Purchase Order, Acp=Accept, Dlv= Delivery, Can=Cancel,
buyer= buyer's application, seller= seller's application

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.



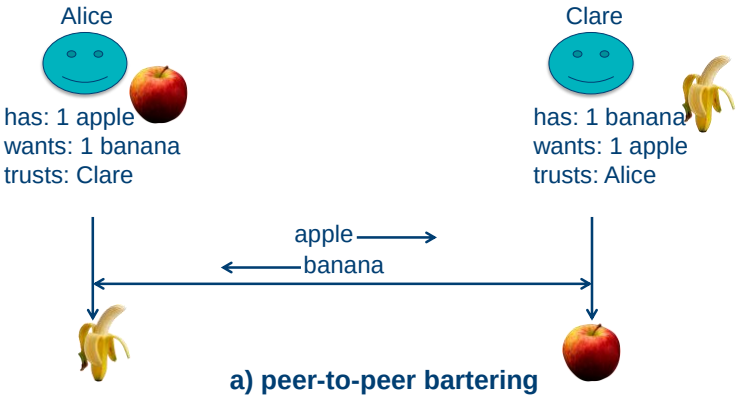
Future: On and off—blockchain Computation Paradigm



A case for a cashless system

- The motivation of the development of Bitcoin was to get rid of the bank.
  - If Alice buys something from Bob, Alice pays Bob in a peer-to-peer maner (that is directly) in cryptocurrency.
- Why don't we get rid of the cryptocurrency to.
  - Let us build a system that enables Alice and Bob to trade in a peer-to-peer manner but without cryptocurrency.
  - Let us go back to bartering.

Bartering



a) peer-to-peer bartering

Bartering: An example of Shared Economy

- Bartering was a successful medieval trading system.
- We abandoned it because it suffers from some technicalities that were hard to solve at that time.
  - Find bartering partners: right time. right place, items of equivalent value etc.
- The ubiquitous presence of the Internet and its instantaneous communication can help solve those problems.
  - I'm in Copacabana beach and have ½ pizza to barter for a glass of beer! Happy to walk to you within a radius of 500 m.

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/

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.