Demystifying the Buzzwords:
Blockchain and Smart Contracts

L-Università ta' Malta
Centre for Distributed
Ledger Technologies

The good old days of services-with-a-smile

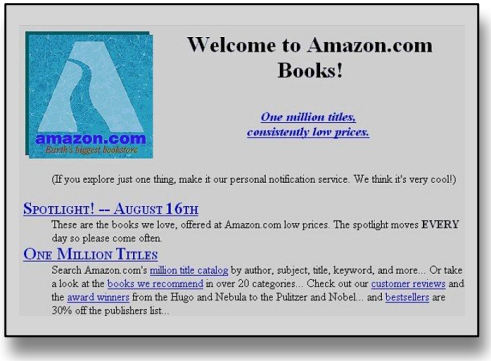
Pre-1995: Services at geographical locations (and some tele-services)

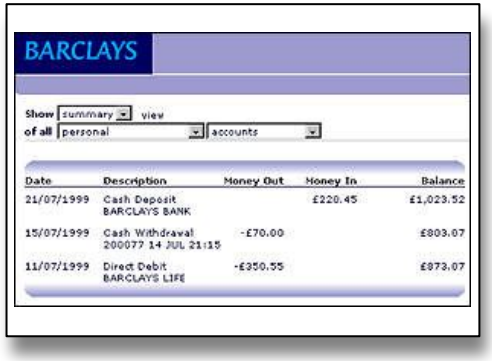
Along came the Internet

Mid-90s:

Start of the Internet Revolution (e-Services)

Services made available from your office/home



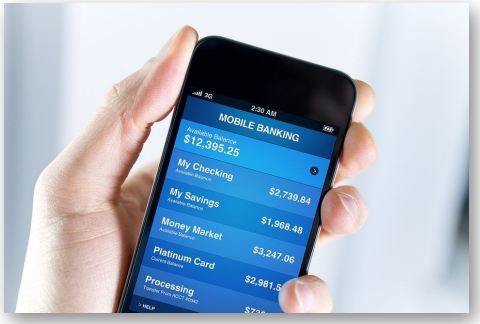


In our pockets

Mid-2000s:

Start of the mobile revolution (m-Services)

Services made available, wherever you are



Blockchain? What the heck is Blockchain?

Mid 2010s:

Start of the blockchain revolution

How does this change the way we interact with services?

Blockchain? What the heck is Blockchain?

Mid 2010s:

Start of the blockchain revolution

How does this change the way we interact with services?

It doesn't.

Blockchain? What the heck is Blockchain?

Mid 2010s:

Start of the blockchain revolution

How does this change the way we interact with services?
It doesn't.

So what is changing?

Blockchain? What the heck is Blockchain?

Mid 2010s:

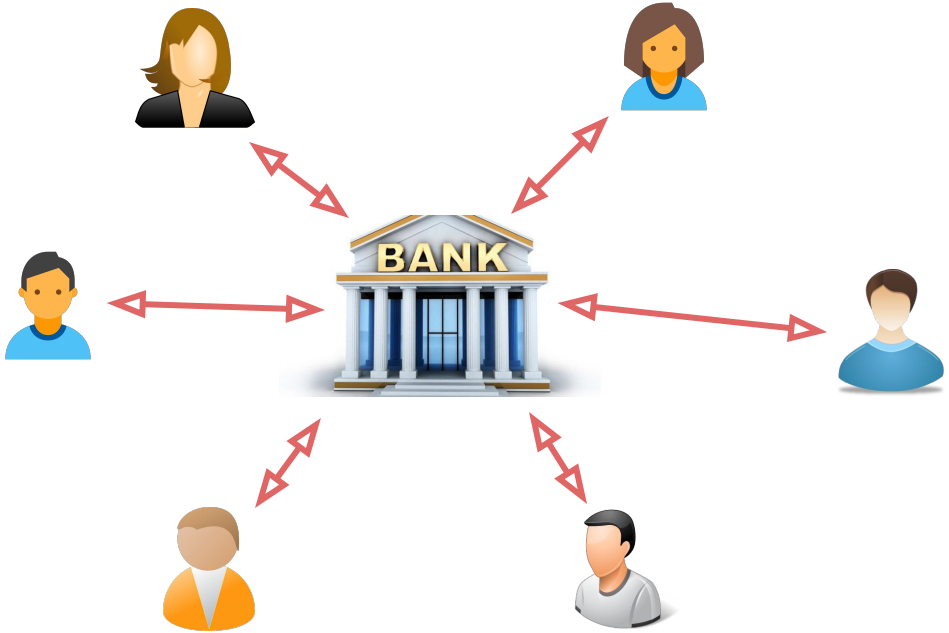
Start of the blockchain revolution

How does this change the way we interact with services?
It doesn't.

So what is changing?
Trust.

How are services provided?

How are services provided?

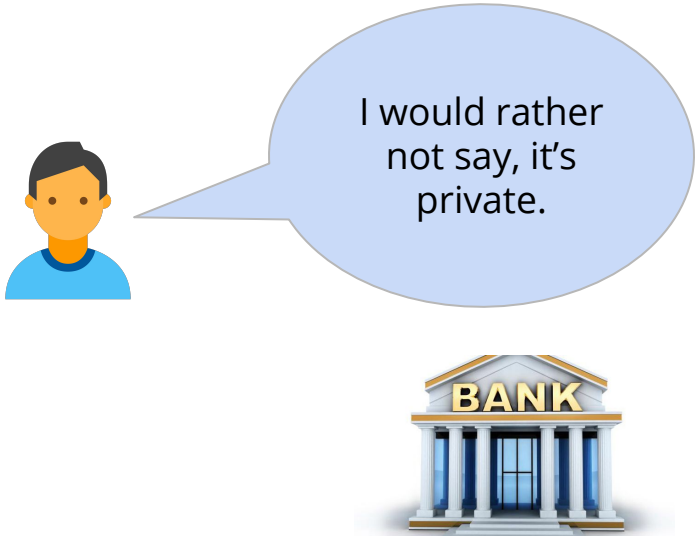


How are payments made now?

How are payments made now?

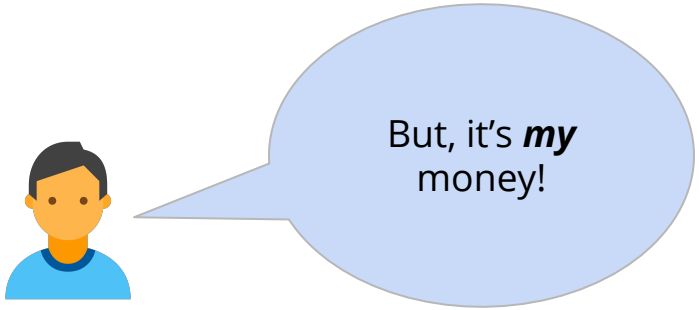
How are payments made now?

How are payments made now?

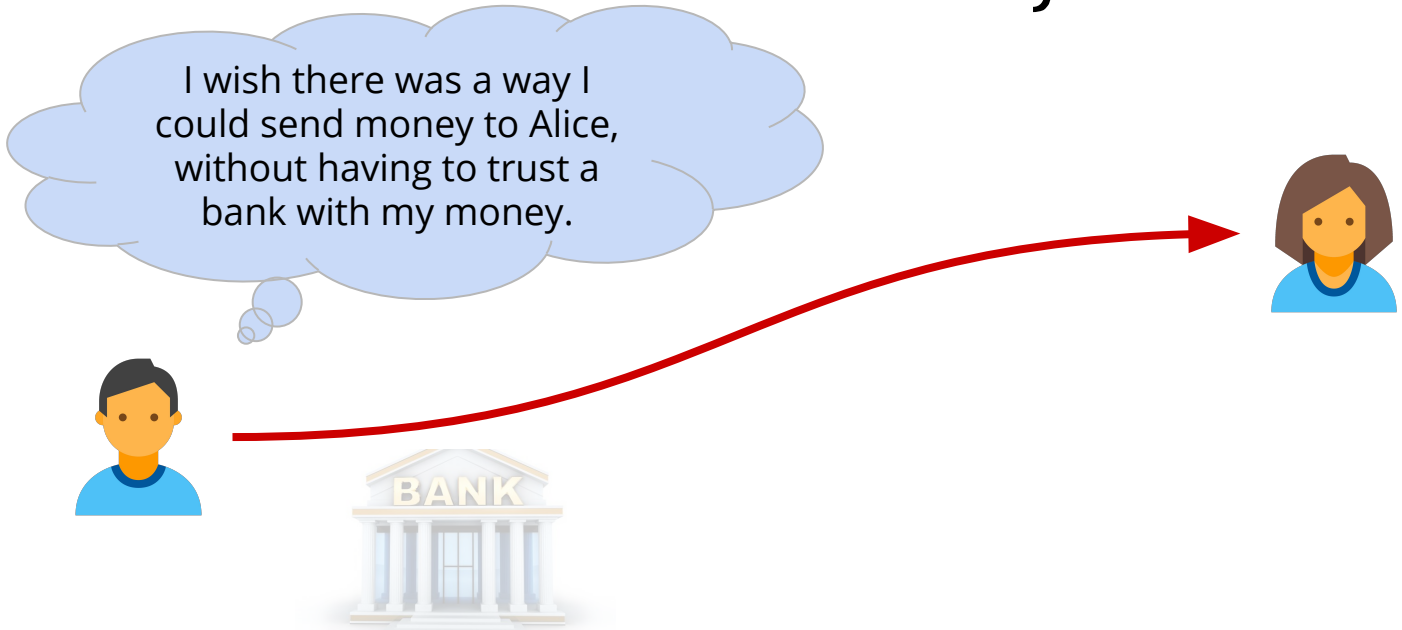


How are payments made now?

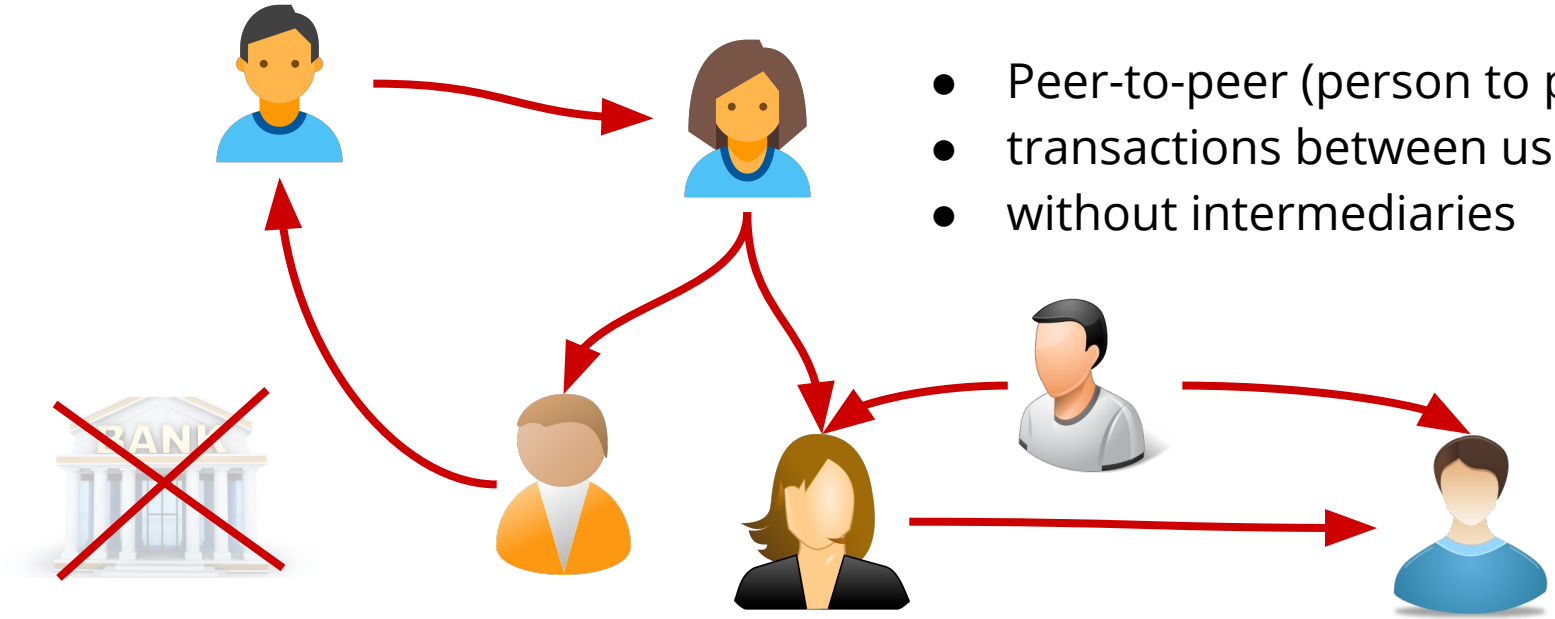
Where it started: Trust and Money



Where it started: Trust and Money

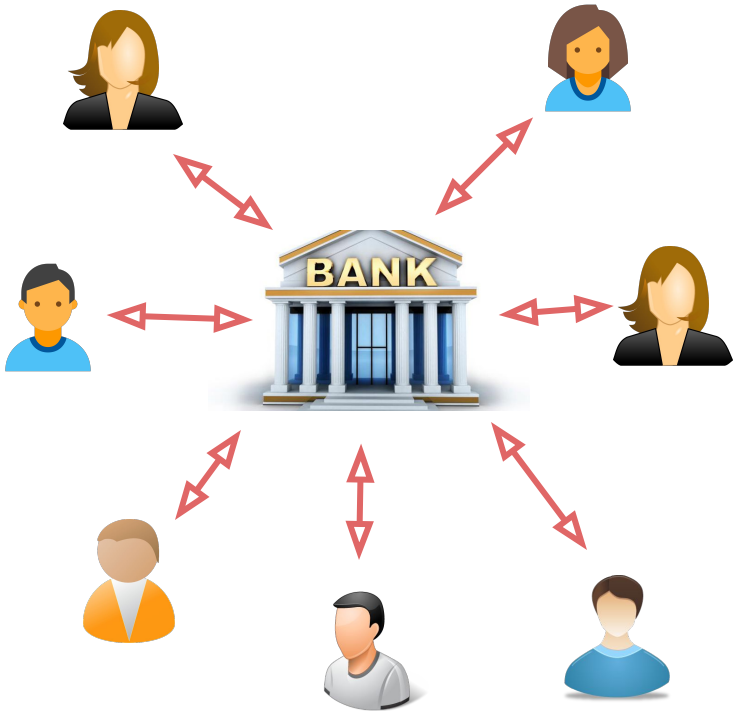


Where it started: Trust and Money



This was Bitcoin's aim:

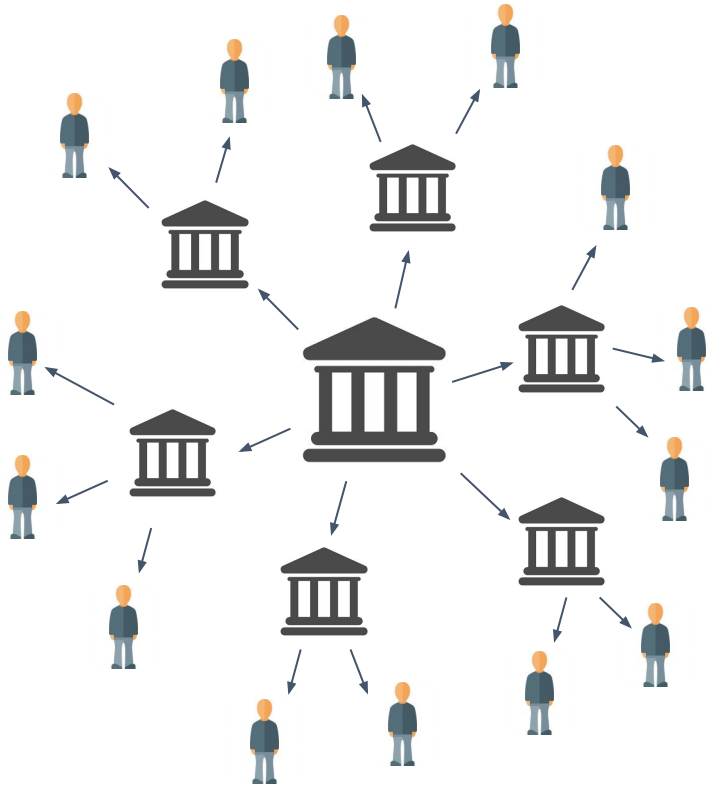
- Peer-to-peer (person to person)
- transactions between users
- without intermediaries



Centralised Digital Money

Easy to do:

- Each bank keeps their own database of all accounts of their clients.
- When **John** sends money to **Mary** and they use the same bank, just **deduct amount from John's** and **add to Mary's.**

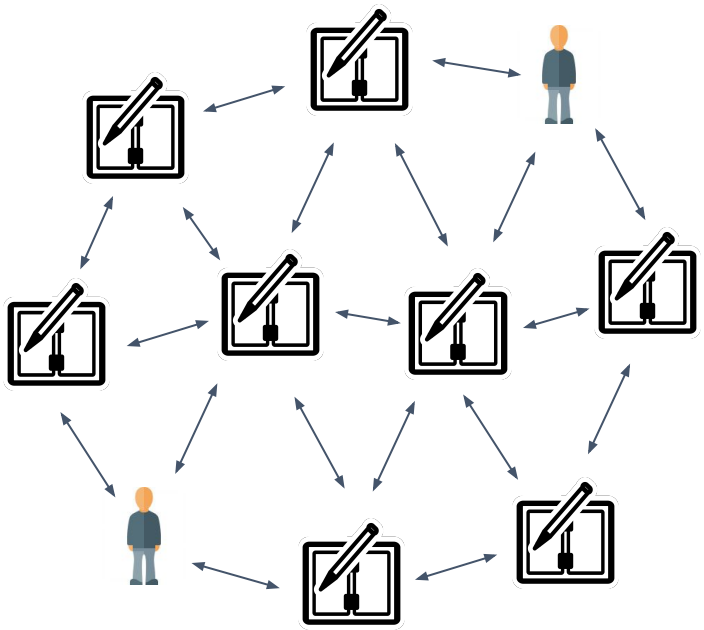


Centralised Digital Money

Easy to do:

- Each bank keeps their own database of all accounts of their clients.
- When **John** sends money to **Mary** and they use the same bank, just **deduct amount from John's** and **add** to **Mary's**.

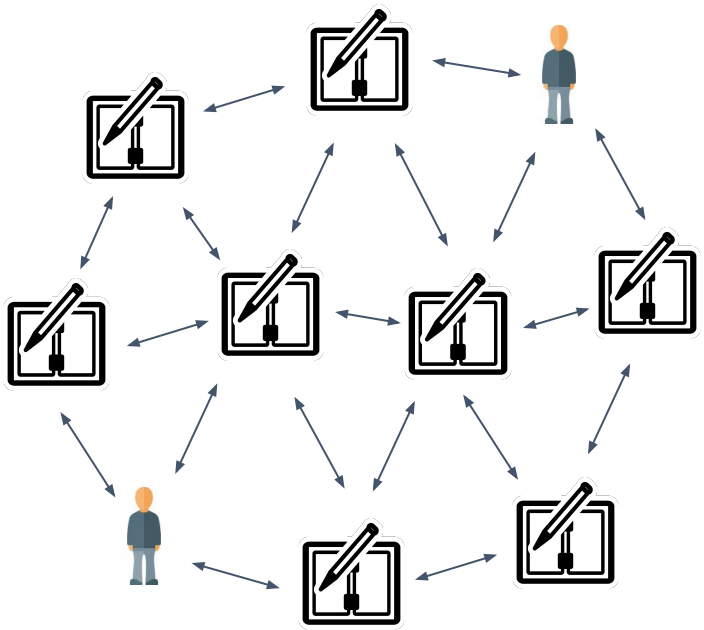
- When **Dave** sends money to **Lucy**, who uses a different bank, actually transfer funds to other bank (or keep IOUs).



Decentralised Digital Ledger

Not easy to do:

- No central authority.
- Every node, needs to have the **complete list of balances of all accounts.**
- When a transaction takes place, we have to update the balances on every node.
- How can we make sure this happens?



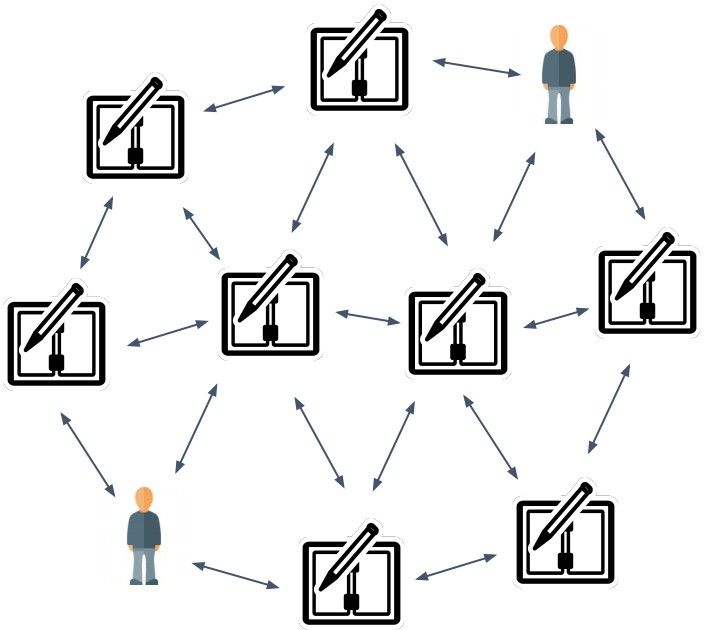
Decentralised Digital Ledger

Not easy to do:

- No central authority.
- Every node, needs to have the **complete list of balances of all accounts.**
- When a transaction takes place, we have to update the balances on every node.
- How can we make sure this happens?

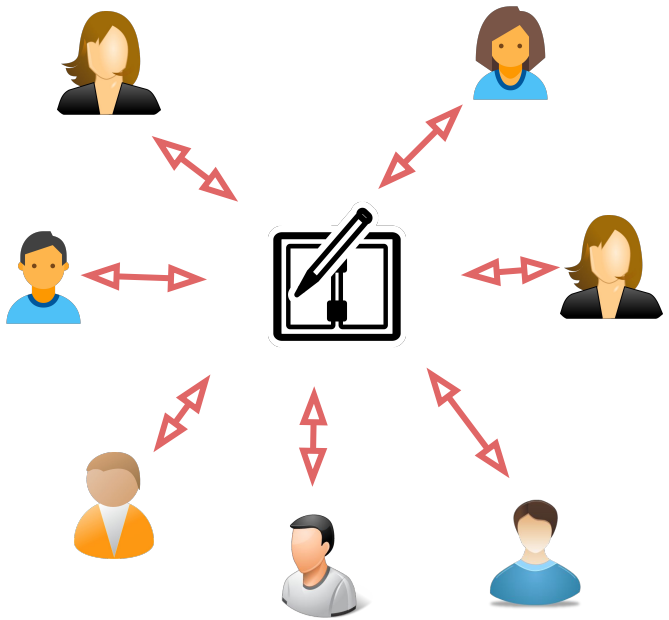
> *"The solution is a cunning ledger called the blockchain".*
>
> The End of Money, New Scientist

Decentralised Digital Money



Every node, has all data and transactions recorded in the blockchain:

- In fact, it is a **ledger**: a list of transactions;
- One can only append transactions to it;
- Transactions that have been recorded can never be changed (immutability).



Decentralised Digital Money

Every node, has all data and transactions recorded in the blockchain:

- In fact, it is a **ledger**: a list of transactions;
- One can only append transactions to it;
- Transactions that have been recorded can never be changed (immutability).

User interaction is (almost) indistinguishable than that using a centralised ledger.

Bitcoin: It's a Ledger

Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

Bitcoin: It's a Ledger

Joshua:
10 BTC

Gordon:
3 BTC

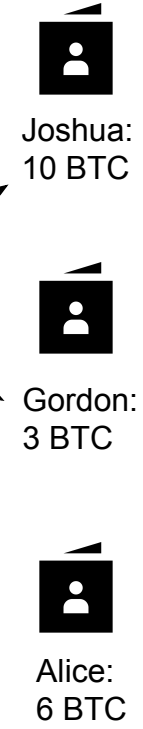
Alice:
6 BTC

Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

Bitcoin: It's a Ledger

From	To	Amount
Joshua	Gordon	3 BTC



Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

Bitcoin: It's a Ledger

From	To	Amount
Joshua	Gordon	3 BTC

Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

Bitcoin: It's a Ledger

From	To	Amount
Joshua	Gordon	3 BTC

Joshua:
7 BTC

Gordon:
6 BTC

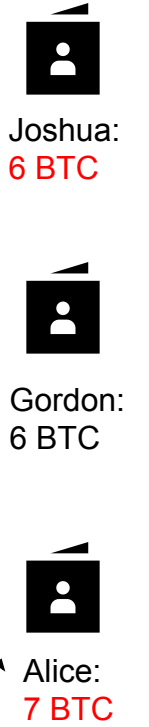
Alice:
6 BTC

Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

Bitcoin: It's a Ledger

From	To	Amount
Joshua	Gordon	3 BTC
Joshua	Alice	1 BTC



Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

Bitcoin: It's a Ledger

From	To	Amount
Joshua	Gordon	3 BTC
Joshua	Alice	1 BTC

Joshua:
6 BTC

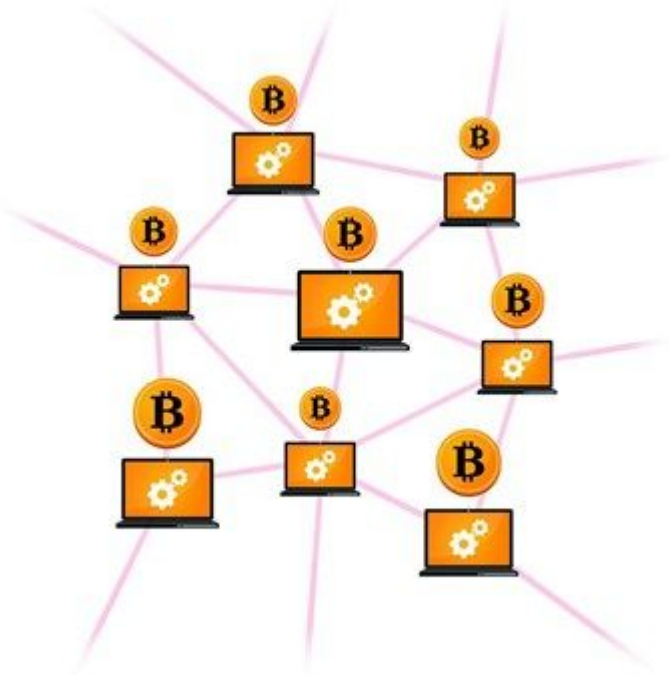
Gordon:
6 BTC

Alice:
7 BTC

Can be seen as a ledger which enforces:

- Only the owner of resources can transfer their resources
- Only one transaction performed at a time
- Old transfers cannot be manipulated or lost

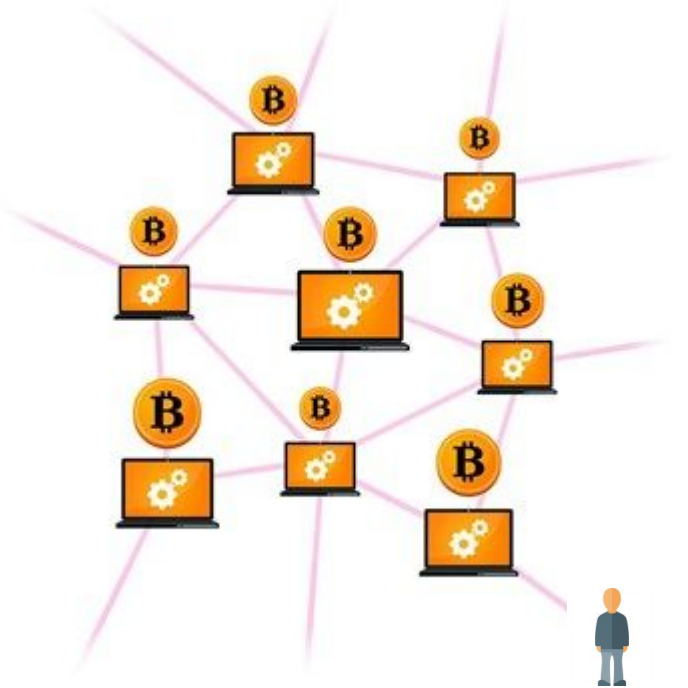
How can I use Bitcoin (or any other blockchain)?



Install a Bitcoin *full node* (a piece of freely available software) on your computer.

- The ‘full node’ will have the whole list of transactions
- You can then send money in a trusted manner by adding the transaction to your node

How can I use Bitcoin (or any other blockchain)?



Or: Communicate with a trusted Bitcoin node, e.g. by using a wallet or exchange

Note: you are trusting the wallet/exchange to perform the transaction

Does everyone see my Bitcoin?

Every ‘node’ or computer in the blockchain, can see all transactions and data

Does everyone see how much Bitcoin you own?

> Yes and No;

Yes: all accounts, all balances, and all transactions are available for all to see

No: Bitcoin only lists your account address (no name associated with account)

Does everyone see my Bitcoin?

Every ‘node’ or computer in the blockchain, can see all transactions and data

Does everyone see how much Bitcoin you own?

> Yes and No;

Yes: all accounts, all balances, and all transactions are available for all to see

No: Bitcoin only lists your account address (no name associated with account)

Key point: all data is available for all on the blockchain to see

Bitcoin is a public blockchain: anyone can download, and be part of the system

Does everyone see my Bitcoin?

Every ‘node’ or computer in the blockchain, can see all transactions and data

Does everyone see how much Bitcoin you own?

> Yes and No;

Yes: all accounts, all balances, and all transactions are available for all to see

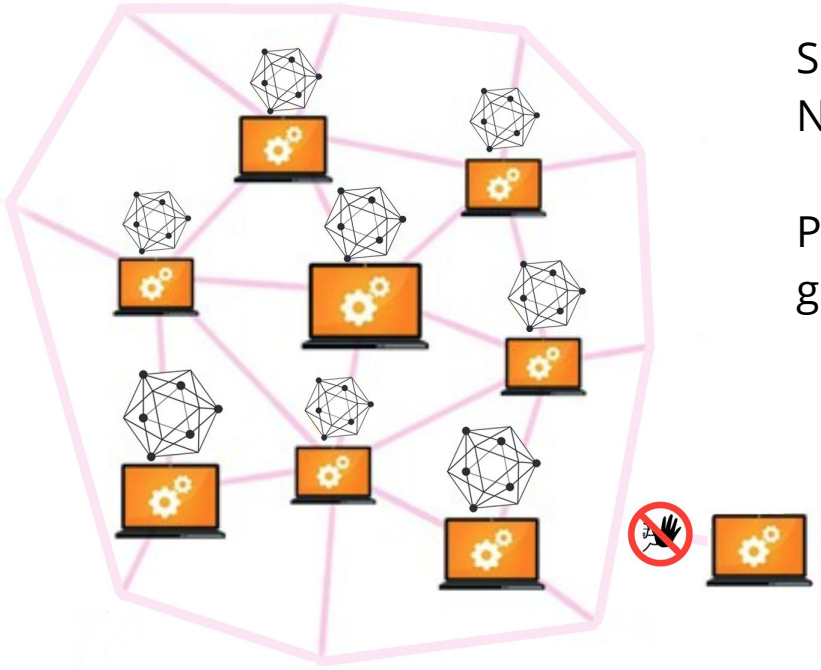
No: Bitcoin only lists your account address (no name associated with account)

Key point: all data is available for all on the blockchain to see

Bitcoin is a public blockchain: anyone can download, and be part of the system

So, what about confidential information?

Permissioned...



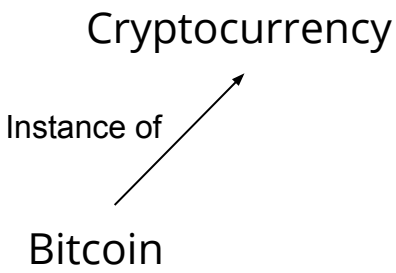
Some systems require more confidentiality;
Not all data should be public

Permissioned/private Blockchains can limit who gets access to the Blockchain (and data)

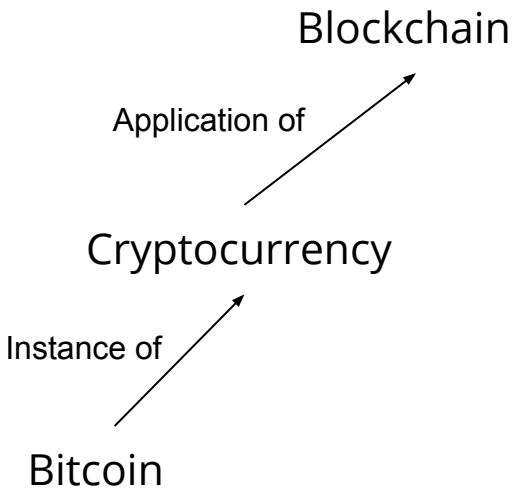
Some Terminology

Bitcoin

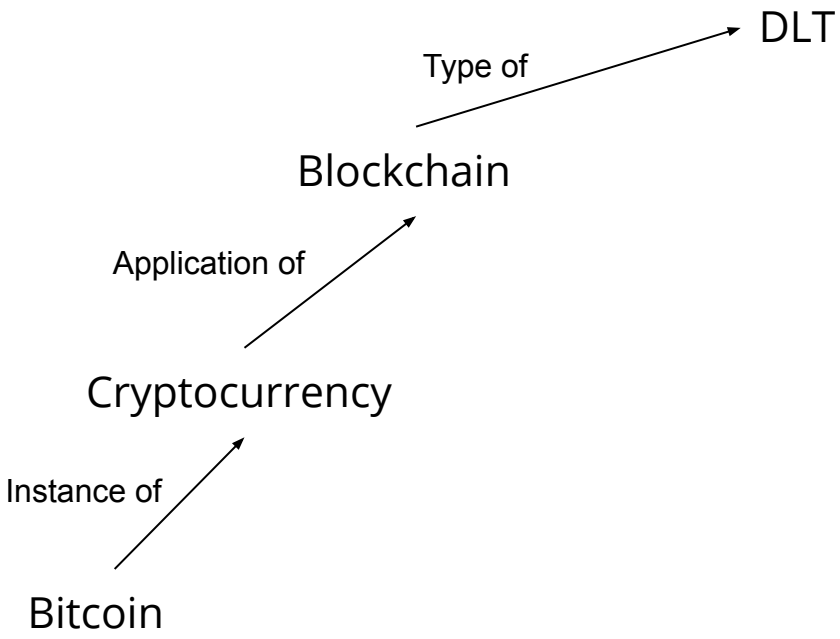
Some Terminology



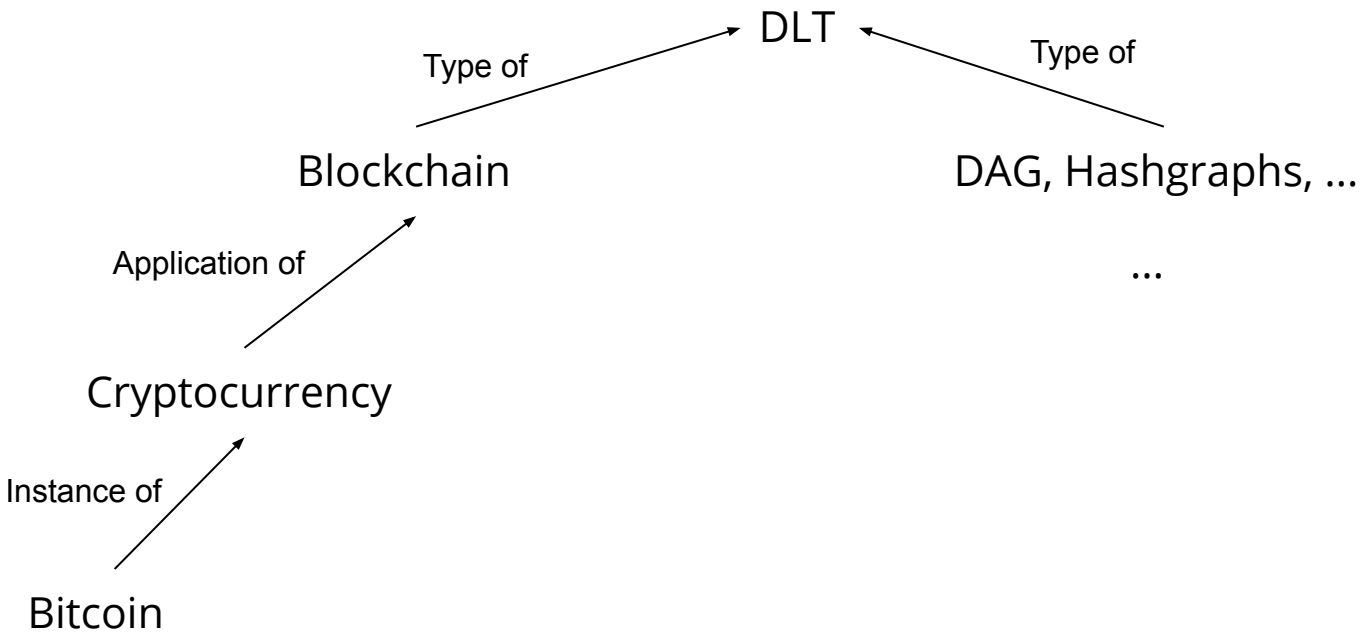
Some Terminology



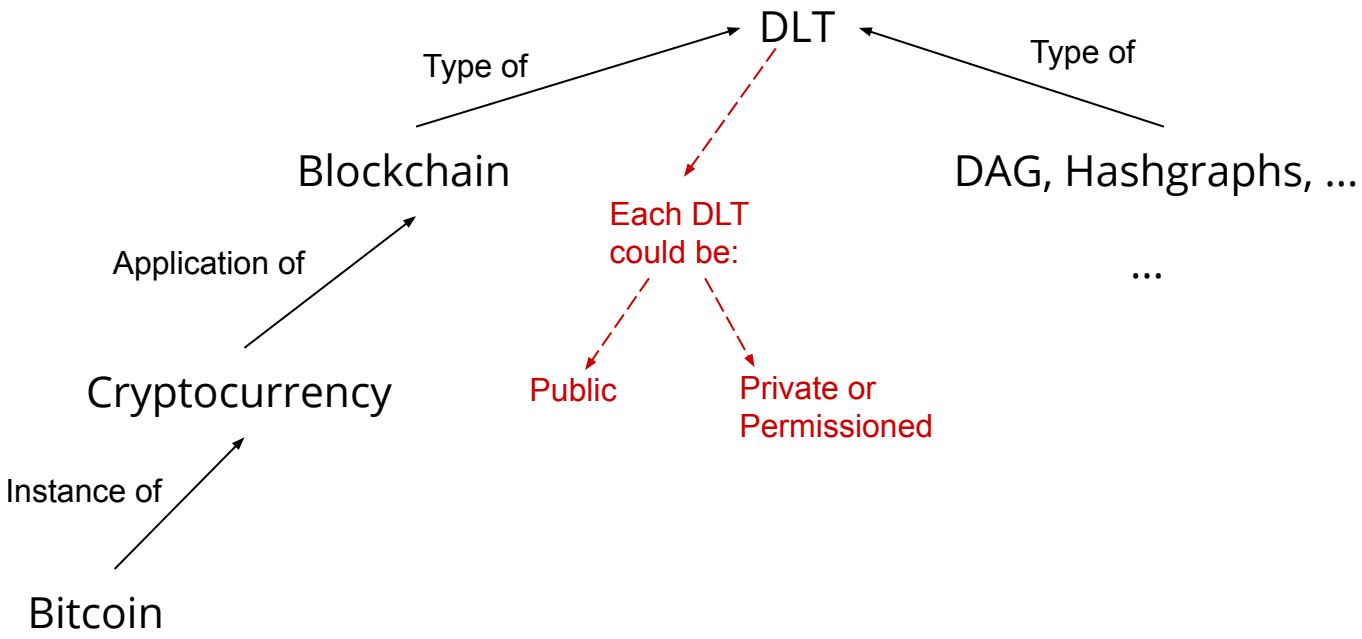
Some Terminology



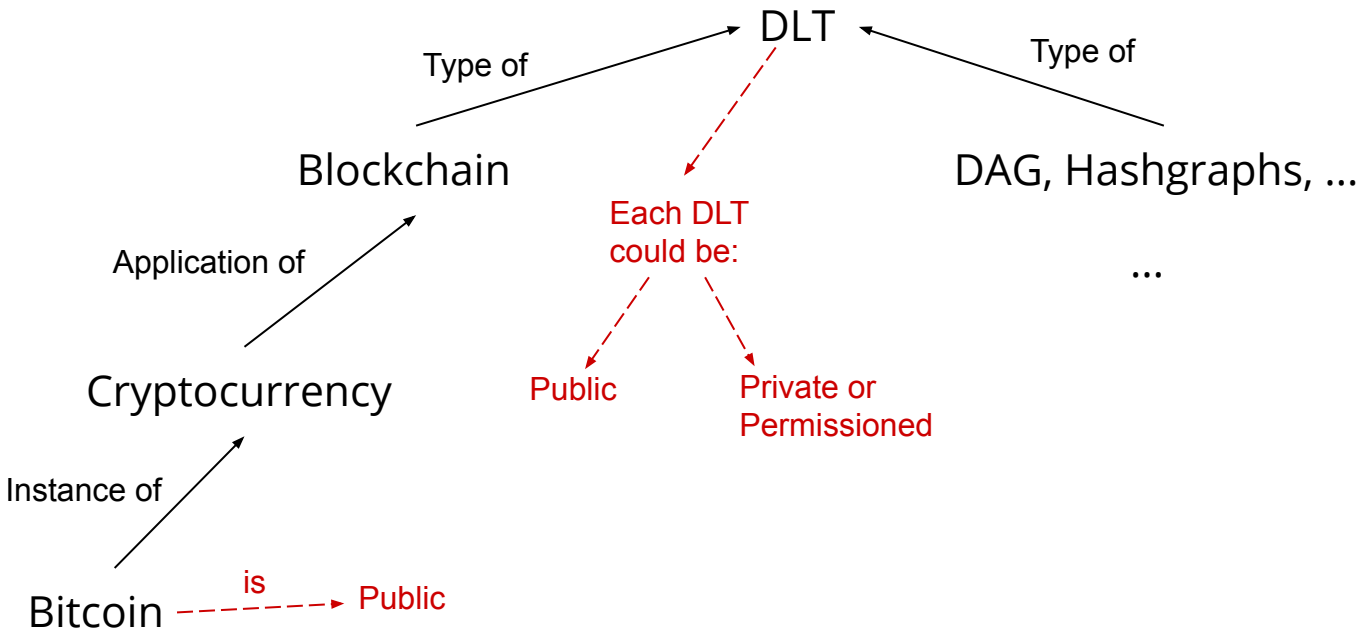
Some Terminology



Some Terminology



Some Terminology



Summary of what blockchain guarantees

- Blockchain is a way of keeping a distributed ledger keeping track of a digital resource such that:
  - Single ownership
  - No overspending
  - No double spending

Summary of what blockchain guarantees

- Blockchain is a way of keeping a distributed ledger keeping track of a digital resource such that:
  - Single ownership
  - No overspending
  - No double spending
- The ledger also guarantees:
  - Copies of the ledger are kept on different nodes
  - The history cannot be modified

Summary of what blockchain guarantees

- Blockchain is a way of keeping a distributed ledger keeping track of a digital resource such that:
  - Single ownership
  - No overspending
  - No double spending
- The ledger also guarantees:
  - Copies of the ledger are kept on different nodes
  - The history cannot be modified

- And yet, requires no central authority.

But it's not just about money

It's actually all about ownership

Digital assets, and their owners can be stored, and passed around...

But it's not just about money

From	To	Asset
Paul	Joshua	212 Triq il-Belt Floriana

Joshua:
212, Triq il-Belt, Floriana

Gordon:
12 Main Street, Zejtun

Alice:
33, Old Mint Street, Valletta

It's actually all about ownership

Digital assets, and their owners can be stored, and passed around...

For example in a national property register.

E…out money

From	To	Asset
Paul	Joshua	212 Triq il-Belt Floriana

Joshua:
212, Triq il-Belt, Floriana

Joshua sells his property to Gordon

…ip

Digital assets, and their owners can be stored, and passed around…

For example in a national property register.

Gordon:
12 Main Street, Zejtun

Alice:
33, Old Mint Street, Valletta

But it's not just about money

It's actually all about ownership

From	To	Asset
Paul	Joshua	212 Triq il-Belt Floriana
Joshua	Gordon	212 Triq il-Belt Floriana

Joshua sells his property to Gordon

rs can be stored,

perty register.

Tracking of rights and ownership of MPPs

We could keep track of **Malta Parking Passes** (MPPs):

- Everytime you use a bus you get 1 MPP;
- If you do not use an MPP for a whole week you get 3 MPPs;
- You can park in reserved MPP parkings by using up 5 MPP;
- You can trade/sell MPP to anyone.

Tracking of rights and ownership of MPPs

Owner	Owns
Joshua	5 MPP
Gordon	1 MPP
Alice	10 MPP
Malta Parking Pass	0 MPP

We could keep track of **Malta Parking Passes** (MPPs):

- Everytime you use a bus you get 1 MPP;
- If you do not use an MPP for a whole week you get 3 MPPs;
- You can park in reserved MPP parkings by using up 5 MPP;
- You can trade/sell MPP to anyone.

Tracking of rights and ownership of MPPs

Owner	Owns
Joshua	5 MPP
Gordon	1 MPP
Alice	10 MPP
Malta Parking Pass	0 MPP

e.g. Alice uses 5 MPP to park in a reserved MPP space.

Tracking of rights and ownership of MPPs

Owner	Owns
Joshua	5 MPP
Gordon	1 MPP
Alice	~~10 MPP~~ 5 MPP
Malta Parking Pass	~~0 MPP~~ 5 MPP

e.g. Alice uses 5 MPP to park in a reserved MPP space.

Tracking of rights and ownership of MPPs

Owner	Owns
Joshua	5 MPP
Gordon	1 MPP
Alice	~~10 MPP~~ 5 MPP
Malta Parking Pass	~~0 MPP~~ 5 MPP

e.g. Alice uses 5 MPP to park in a reserved MPP space.

But, how can you trust that *Malta Parking Pass Ltd.* will really give you 3 MPPs if you do not use your car for a week? Or that you will really get 1 MPP each time you buy a bus ticket?

Smart Contracts

Szabo (1996) machine executable transactions which enforce certain behaviour: *"robust against naïve vandalism [and] against sophisticated, incentive compatible breach"*

Lessig (1999) *"Code is law"*

Ethereum (2013) *"A blockchain with a built-in programming language, allowing anyone to write smart contracts"*

In gods we trust, all others pay cash...

In gods we trust, all others pay cash...

- **Solution 0:** Sign a contract between customer and the company, making the company liable.
- **Solution 1:** Add a trusted third party to enforce the contract – to receive and distribute the funds.
- **Solution 2:** Use a smart contract.

Smart Contracts

- Can store digital assets
- Can execute executable logic
- All this is done in a trustless manner, on the blockchain

contract TenPercent:

Initial company balance is 0.

[A] Payment of *<amount>*:

Anyone may transfer ***<amount>*** in cryptocurrency to this contract –

* 10% is immediately sent to the charity.
* 90% is added to the company's balance.

[B] Withdrawal of *<amount>*:

May be done only by the company and if ***<amount>*** does not exceed its balance –

* Reduce company's balance by *<amount>*.
* Send *<amount>* from the contract to the company's address.

contract TenPercent:

Initial company balance is 0.

[A] Payment of *<amount>*:

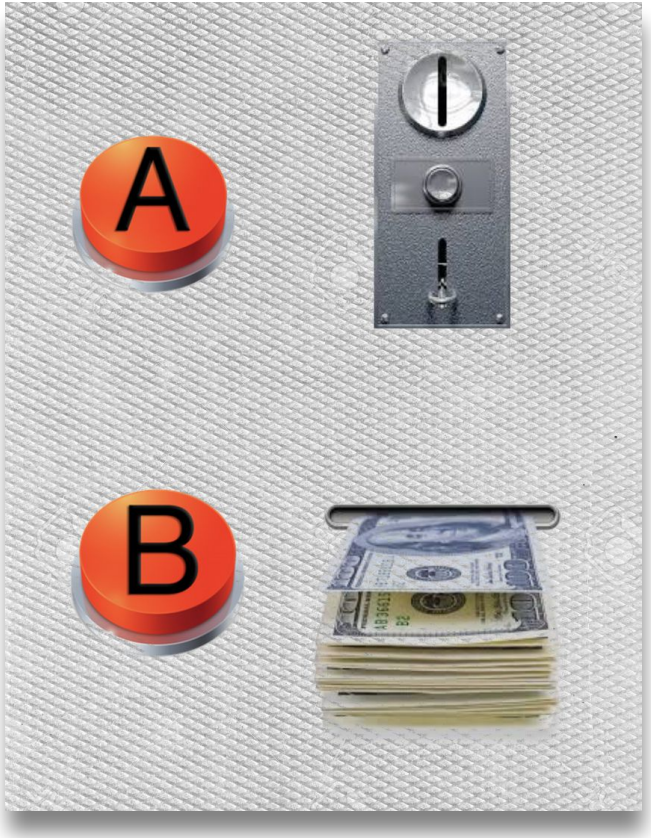
Anyone may transfer ***<amount>*** in cryptocurrency to this contract –

* 10% is immediately sent to the charity.
* 90% is added to the company's balance.

[B] Withdrawal of *<amount>*:

May be done only by the company and if ***<amount>*** does not exceed its balance –

* Reduce company's balance by *<amount>*.
* Send ***<amount>*** from the contract to the company's address.



contract Guarantee:

Set guarantee status to UNPAID.

[A] Payment of guarantee:

* Anyone may transfer 100 bitcoins to this contract as long as the guarantee is UNPAID.
* Set the deadline to be in 6 months and remember the payer.
* Set guarantee status to PAID.

[B] Extension of deadline:

* May be done only by the contracts department and if the status of the guarantee is PAID.
* If the deadline was never extended, push it back by 3 months.

[C] Register default:

* May be done only by the contracts department and if there is a PAID guarantee.
* Send 100 bitcoins to the contracts department.
* Set guarantee status to DEFAULTED.

[D] Withdrawal of guarantee:

* May be done only by the payer of the guarantee, if there is a PAID guarantee and if the deadline has passed.
* Send 100 bitcoins from the contract to the guarantee payer.
* Set guarantee status to RETURNED.

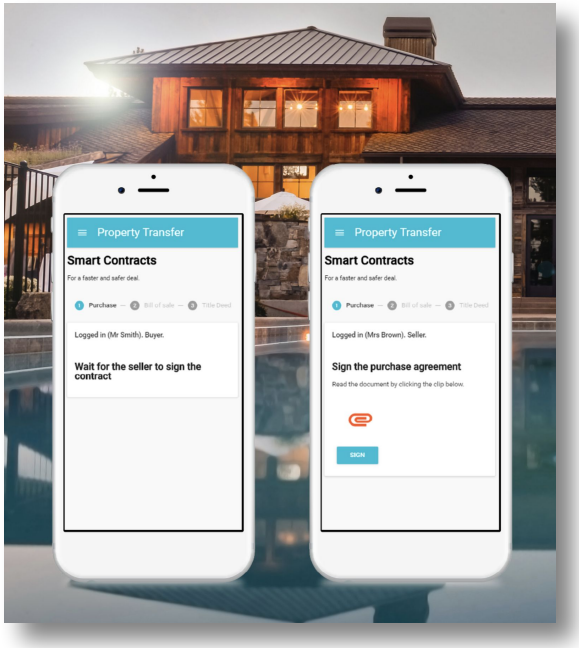
Procurement and guarantees...

- The smart contract is acting as escrow.
- All actions (button presses) are immutably recorded on the blockchain for all to see.
- The seller is guaranteed that:
  - They will get the money if no default is registered before the deadline.
  - The deadline can only be extended once.
  - **The system is transparent.**
- The contracts department is guaranteed that:
  - They can extend the deadline (albeit once).
  - They can declare a default before the deadline.
  - **The system is transparent.**

Do I really need a DLT and smart contracts?

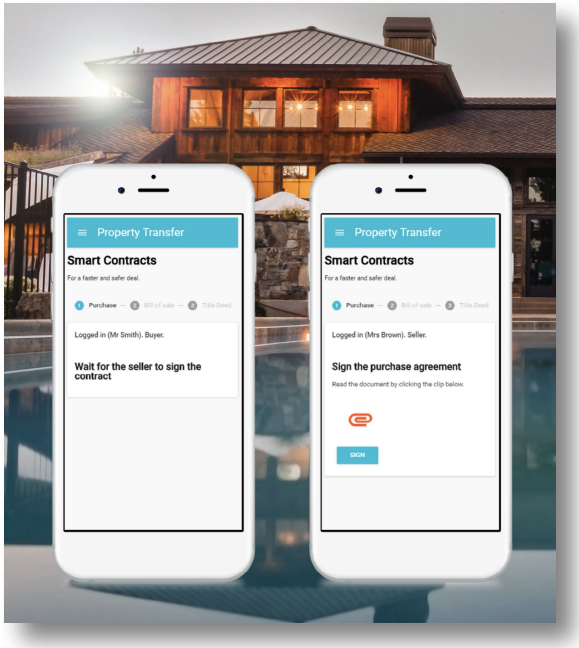
- Do you require trust?
  - Have no centralised trust.
  - Participants control and transfer resources.
  - Participants want proof of contract logic e.g. *they can always take the money back if the deadline has passed.*
- Do you require decentralisation?
- Is it data intensive?
- Why wouldn't a central server be an option?

Applications: Land Registry



- Many registries are still paper based.
- Even digital registries require lots of paper trails with many signed documents.
- Information can go missing; not be input; or input incorrectly or be altered?
- Time consuming process *(checking documentation manually).*

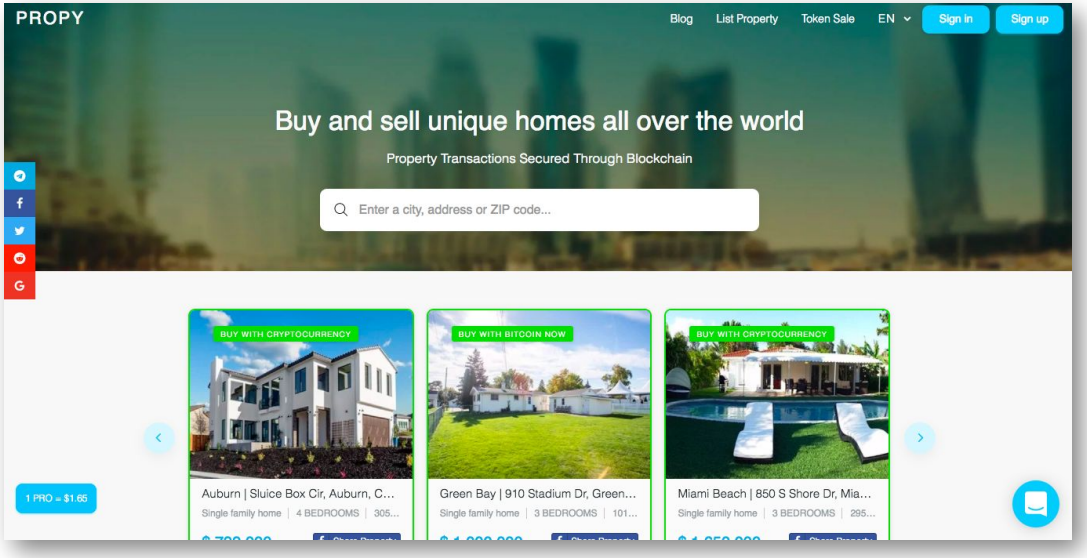
Applications: Land Registry



Using Blockchain ensures that the data is:

- Permanent;
- Tamperproof;
- Decentralised (no single trusted institution);
- Instant (or near instant) processing;
- Reduce *search* time to instant.

Applications: Land Registry



- Decentralised buying and selling of property.
- Minimise intermediary fees.
- No extensive paper trails.

Applications: Improving Transport Networks

You wake up an hour early, and you do not feel tired, so you get up and decide to make your way to work earlier.

Applications: Improving Transport Networks

You wake up an hour early, and you do not feel tired, so you get up and decide to make your way to work earlier.

You let your driverless car know that you are not in a rush to get to work.

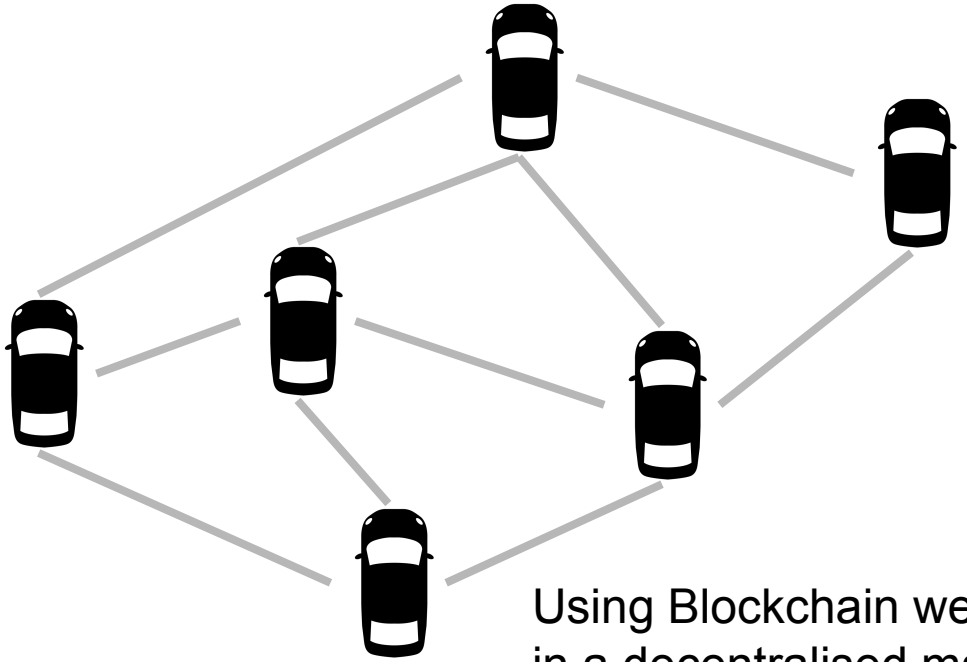
Applications: Improving Transport Networks

You wake up an hour early, and you do not feel tired, so you get up and decide to make your way to work earlier.

You let your driverless car know that you are not in a rush to get to work.

Your car realises that others are in more of rush, and lets the other cars through.
As an incentive for letting you through the other cars, had offered 10 NTT (national transport tokens)...
Which can be used to buy fuel, or use public transport.

Applications: Improving Transport Networks



Using Blockchain we cars can transfer tokens (or money) in a decentralised manner

Applications: Improving Transport Networks

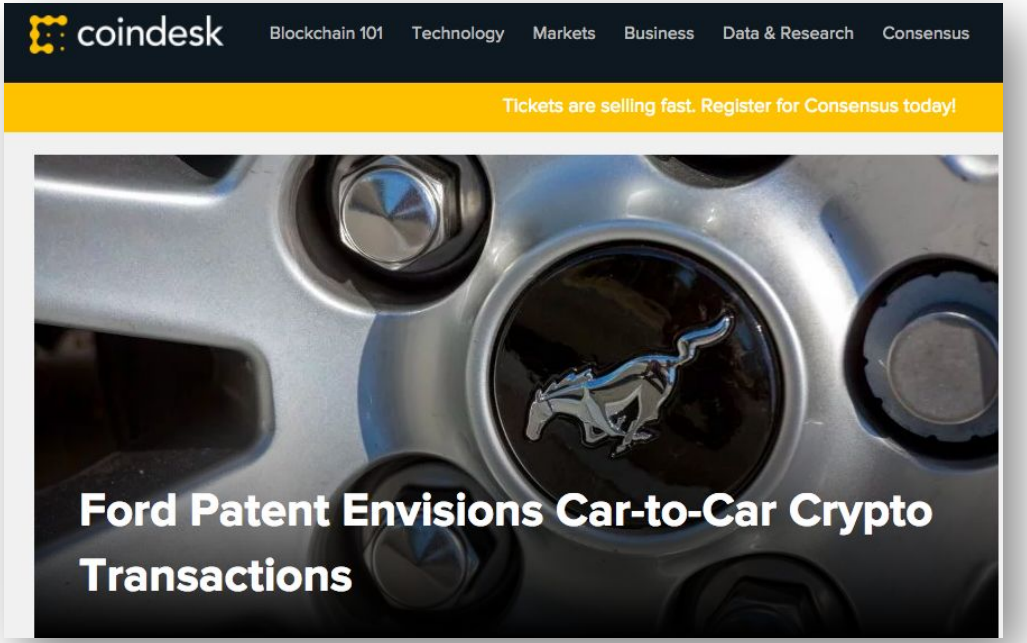
You wake up an hour early, and you do not feel tired, so you get up and decide to make your way to work earlier.

You let y rush to get to work.

Too far fetched?

, and lets the other cars through.
As an incentive for letting you through the other cars, had offered 10 NTT (national transport tokens)...
Which can be used to buy fuel, or use public transport.

Applications: Improving Transport Networks



Ford filed (and were awarded) a patent to do exactly this.

Applications: Certificates on the Blockchain

You go to lectures, study and sit for your exams.

Applications: Certificates on the Blockchain

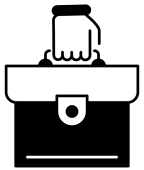
You go to lectures, study and sit for your exams.

You graduate (and celebrate).

Applications: Certificates on the Blockchain

You go to lectures, study and sit for your exams.

You graduate (and celebrate).



And land your first job.

Applications: Certificates on the Blockchain

You climb the ladder of success.

Applications: Certificates on the Blockchain

You climb the ladder of success.

War breaks out in your country.

Applications: Certificates on the Blockchain

You climb the ladder of success.

War breaks out in your country.

You need to leave.

Applications: Certificates on the Blockchain

You settle in a new land and make it your home.

Applications: Certificates on the Blockchain

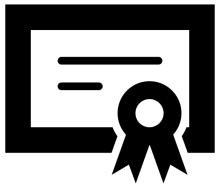
You settle in a new land and make it your home.

You go for an interview.

Applications: Certificates on the Blockchain

You settle in a new land and make it your home.

You go for an interview.



They ask for your certificate.

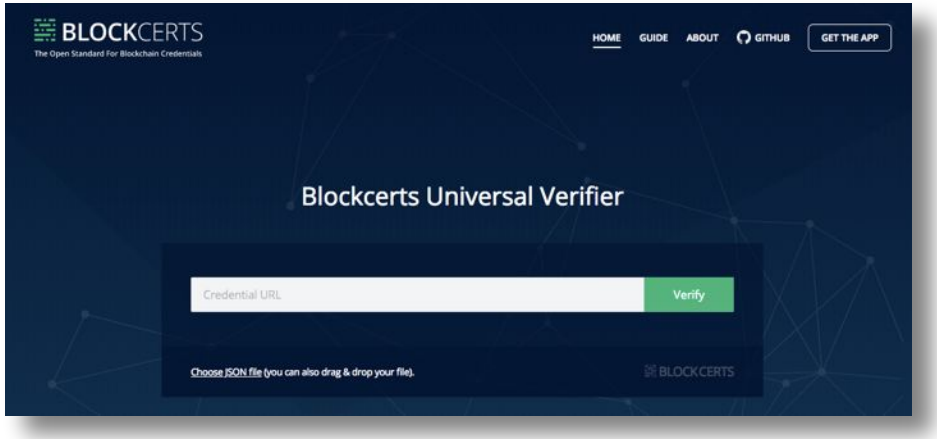
Applications: Certificates on the Blockchain

You settle in a new land and make it your home.

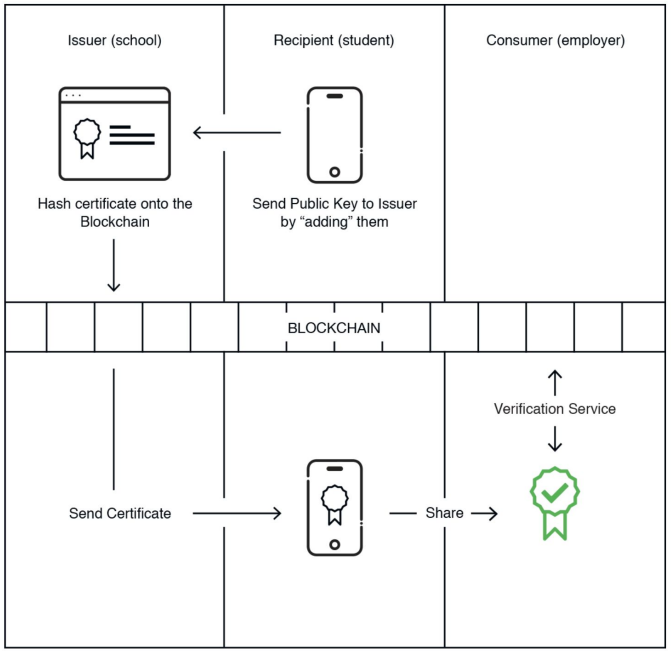
You go for an interview.

They ask for your certificate.
But it was lost in the war, and the registry no longer exists.
So you cannot get a job in your profession.

Applications: Certificates on the Blockchain



Access to certificates is quick and direct (normal certificates need to pay and receive via mail)



Lots of applications... don't worry about the how

Assume that (however it works), blockchain provides:

- Ledger cannot be tampered with
- Available for all to check
- Allows for transfer money or assets without problems
- Only I can transfer my money or assets
- Without requiring a central authority

Want to stay in touch?

Potential to collaborate
Pilot projects
Research proposals and grants
Training courses for the general public and developers

dlt@um.edu.mt
gordon.pace@um.edu.mt
joshua.ellul@um.edu.mt

facebook.com/um.cdlt
Centre for Distributed Ledger Technologies