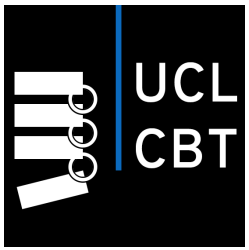
Blockchain, Analytics, and Institutions

Implications for a Changing Business World

Geoff Goodell (University College London)

24 October 2019



g.goodell@ucl.ac.uk

About Us

Financial Computing and Analytics Group
at **University College London**

Our research takes a **complex systems** approach to the interfaces among **technology**, **markets**, and **institutions**.

About Us

Financial Computing and Analytics Group
at **University College London**

Our research takes a **complex systems** approach to the interfaces among **technology**, **markets**, and **institutions**.

Blockchain Technology for Algorithmic Regulation and Compliance (**BARAC**) (2016-2019)

Whitechapel Think Tank (**WTT**)

About Us

Financial Computing and Analytics Group
at **University College London**

Our research takes a **complex systems** approach to the interfaces among **technology**, **markets**, and **institutions**.

Blockchain Technology for Algorithmic Regulation and Compliance (**BARAC**) (2016-2019)

Whitechapel Think Tank (**WTT**)

Upcoming work includes:

- smart and computable contracts
- global digital marketplaces
- future payments infrastructure
- digital credentials for public services

The Rise of Analytics

Image Source: datapine.com

Devices: More Data Collected Than Ever Before

Networks: More Data Aggregated Than Ever Before

Systems: More Data Analysed Than Ever Before

Markets: More Data Brokered Than Ever Before

We Are What We Measure

Image Source: socialcooling.com

More data means more **measurement**, and data analytics systems create the opportunity to exercise control.

We Are What We Measure

Image Source: socialcooling.com

More data means more **measurement**, and data analytics systems create the opportunity to exercise control.

For example, **market surveillance**: the ability to analyse the behaviour of securities brokers means that we can reduce opportunities for misbehaviour.

We Are What We Measure

Image Source: socialcooling.com

More data means more **measurement**, and data analytics systems create the opportunity to exercise control.

For example, **market surveillance**: the ability to analyse the behaviour of securities brokers means that we can reduce opportunities for misbehaviour.

But the ability to measure **personal activities** means the opportunity to **control mass behaviour**, cheaply and at scale.

(The effect will be profound.)

Ledgers and Transactions

ledger: an information store that keeps final and definitive records of transactions

transaction: smallest unit of a work process resulting in a state change [ISO 26122:2008, definition 3.5]

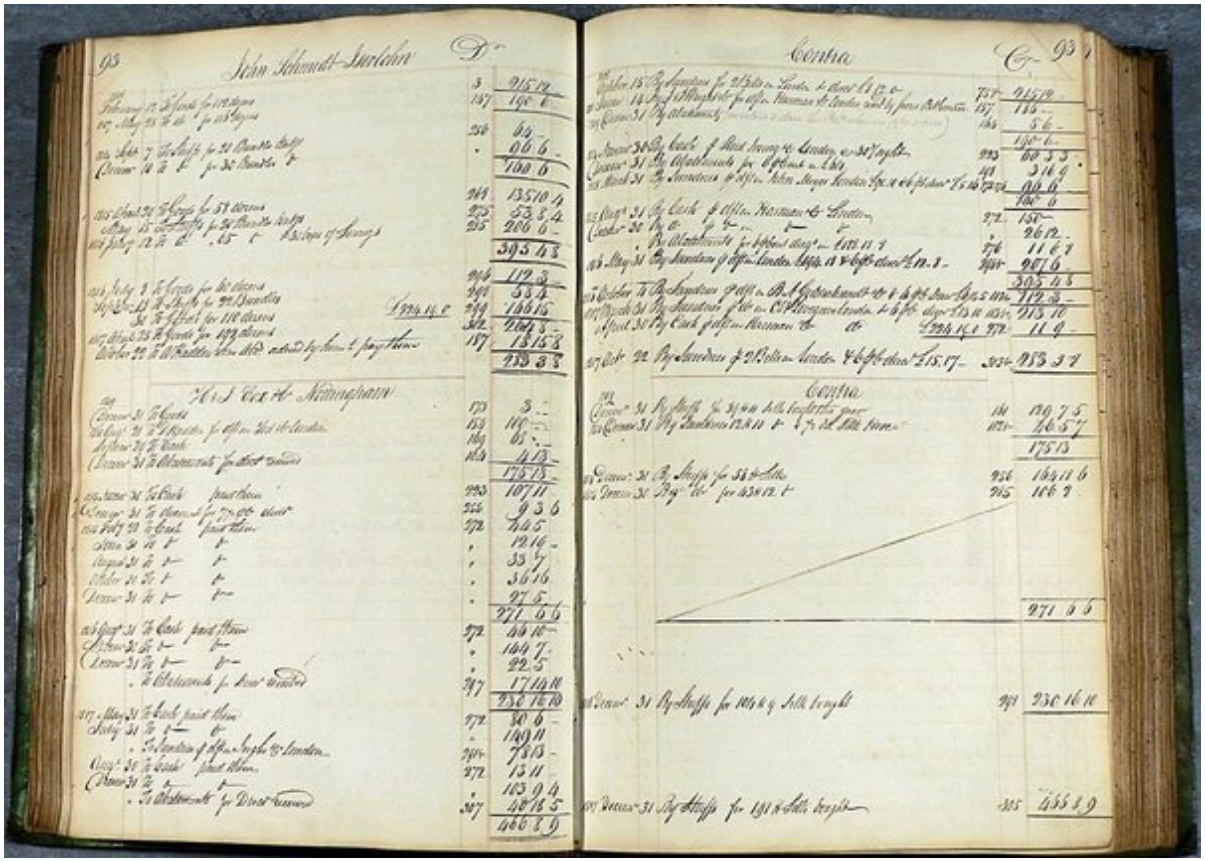


Image: `https://qph.ec.quoracdn.net/main-qimg-bdd086c33e2c34349e7d7400f75b3c51-c`

Networks

network: an interconnected system of things or people [WordNet]

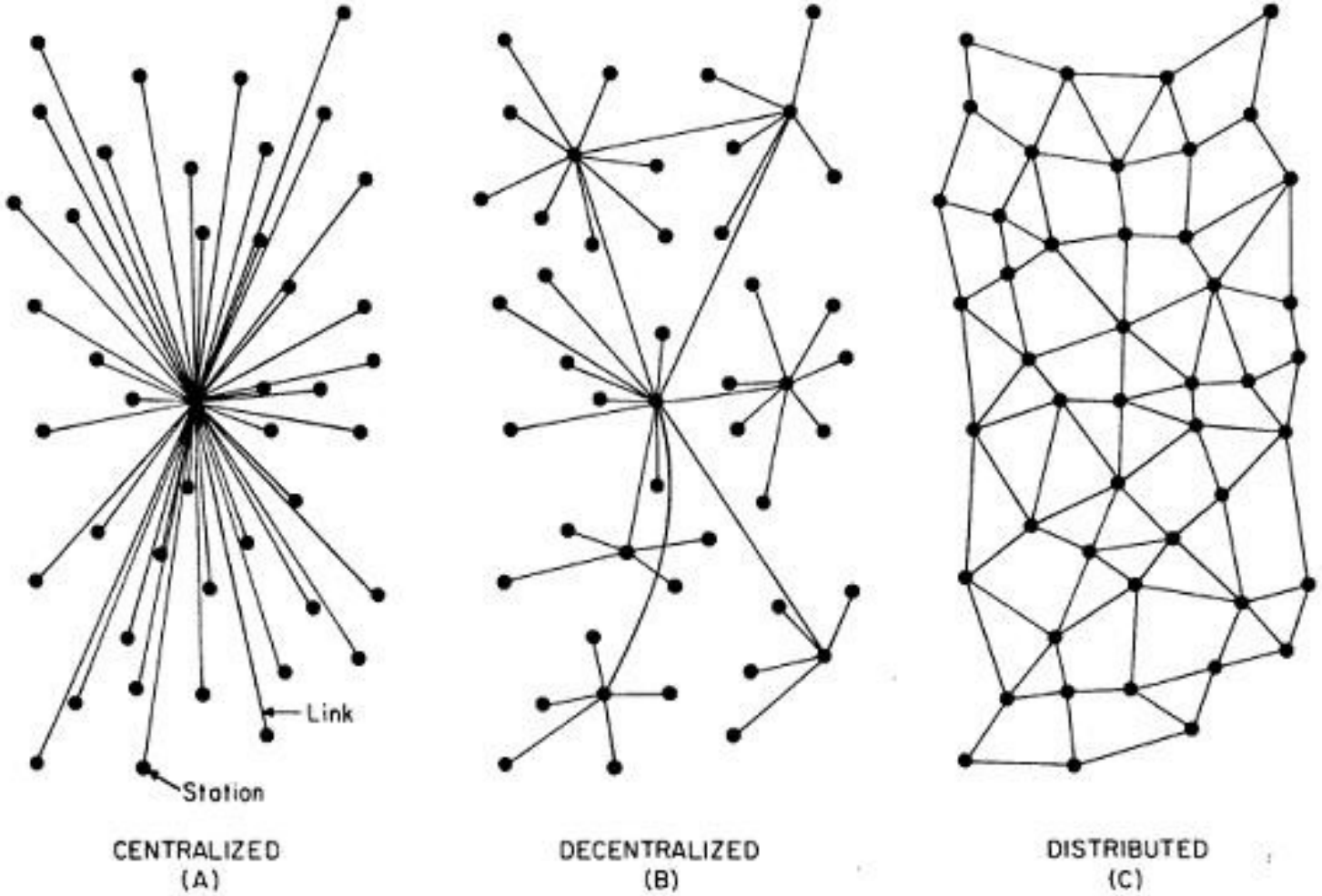


Image: Baran, P. On Distributed Communications. Rand Corporation, 1964.

Risks of Centralisation [Siliski[1]]

[1] Siliski, M. Blockchain Alternatives: The Right Tool for the Job, Medium, 2018-04-10. https://medium.com/swlh/blockchain-alternatives-b21184ccc345

Risks of Centralisation [Siliski[1]]

(1) Censoring or banning users of the system

[1] Siliski, M. Blockchain Alternatives: The Right Tool for the Job, Medium, 2018-04-10. https://medium.com/swlh/blockchain-alternatives-b21184ccc345

Risks of Centralisation [Siliski[1]]

(1) Censoring or banning users of the system

(2) Charging unreasonably high fees to use the system (rent seeking)

[1] Siliski, M. Blockchain Alternatives: The Right Tool for the Job, Medium, 2018-04-10. https://medium.com/swlh/blockchain-alternatives-b21184ccc345

Risks of Centralisation [Siliski[1]]

(1) Censoring or banning users of the system

(2) Charging unreasonably high fees to use the system (rent seeking)

(3) Changing the rules of the system (e.g. start charging a fee)

[1] Siliski, M. Blockchain Alternatives: The Right Tool for the Job, Medium, 2018-04-10. https://medium.com/swlh/blockchain-alternatives-b21184ccc345

Risks of Centralisation [Siliski[1]]

(1) Censoring or banning users of the system

(2) Charging unreasonably high fees to use the system (rent seeking)

(3) Changing the rules of the system (e.g. start charging a fee)

(4) Lying or otherwise intentionally tampering with data

[1] Siliski, M. Blockchain Alternatives: The Right Tool for the Job, Medium, 2018-04-10. https://medium.com/swlh/blockchain-alternatives-b21184ccc345

Risks of Centralisation [Siliski[1]]

(1) Censoring or banning users of the system

(2) Charging unreasonably high fees to use the system (rent seeking)

(3) Changing the rules of the system (e.g. start charging a fee)

(4) Lying or otherwise intentionally tampering with data

(5) Making mistakes, being hacked, or going out of business

[1] Siliski, M. Blockchain Alternatives: The Right Tool for the Job, Medium, 2018-04-10. `https://medium.com/swlh/blockchain-alternatives-b21184ccc345`

Distributed Ledgers

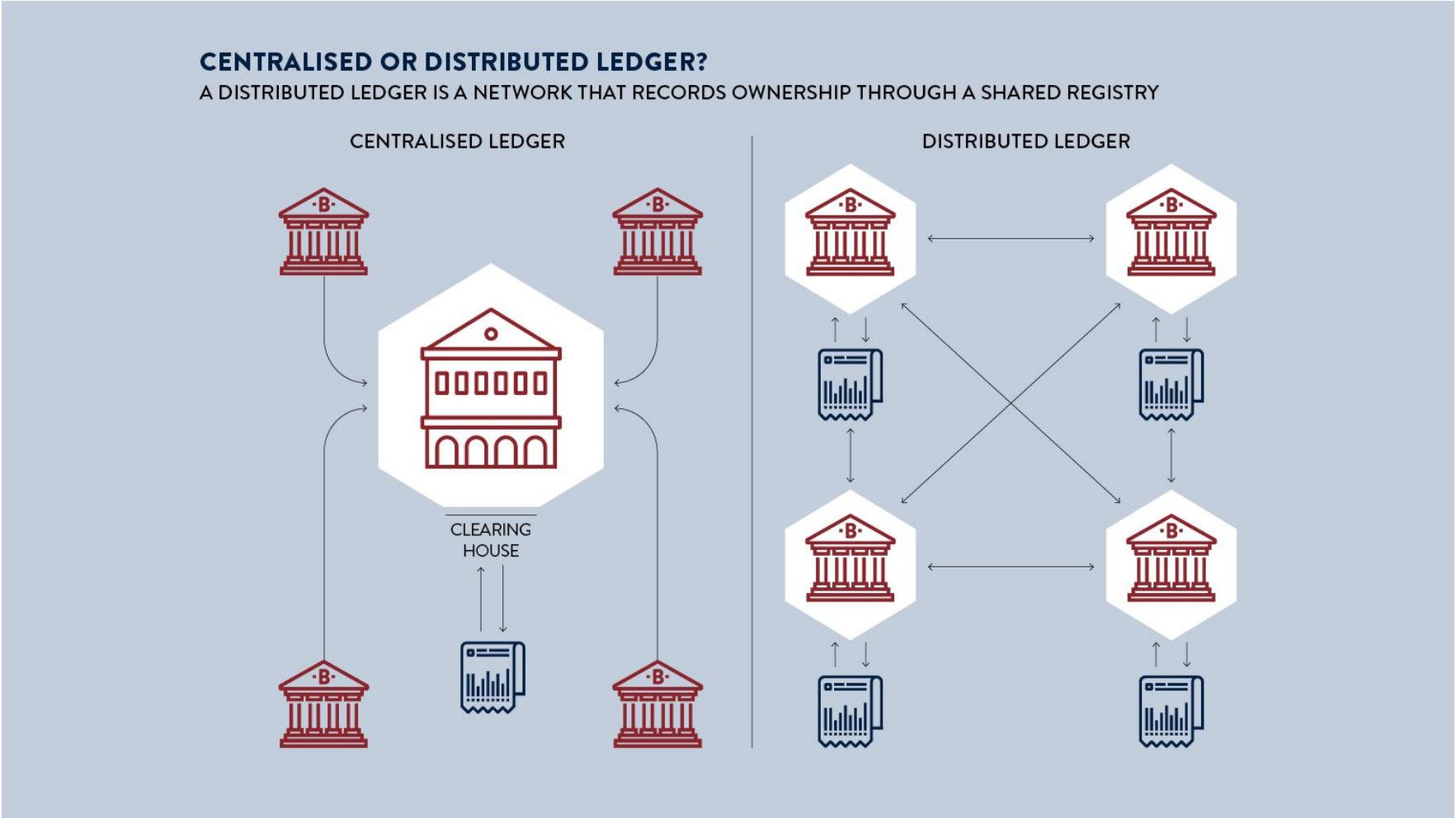


Image: raconteur.net

Motivation for Distributed Ledgers

Cryptography is about eliminating **trusted third parties.**

[2] Piscini, E. et al. Blockchain: Democratized trust. Deloitte Insights, 2016-02-24.

Motivation for Distributed Ledgers

Cryptography is about eliminating **trusted third parties.**

Blockchain technology applies **cryptography** to **transactions**.

[2] Piscini, E. et al. Blockchain: Democratized trust. Deloitte Insights, 2016-02-24.

Motivation for Distributed Ledgers

Cryptography is about eliminating **trusted third parties.**

Blockchain technology applies **cryptography** to **transactions**.

Motivating desiderata:

- **Decentralisation:** no single point of trust, no single point of control (no central authority).

[2] Piscini, E. et al. Blockchain: Democratized trust. Deloitte Insights, 2016-02-24.

Motivation for Distributed Ledgers

Cryptography is about eliminating **trusted third parties.**

Blockchain technology applies **cryptography** to **transactions**.

Motivating desiderata:

- **Decentralisation:** no single point of trust, no single point of control (no central authority).
- **Security:** non-repudiation and irreversibility of records.

[2] Piscini, E. et al. Blockchain: Democratized trust. Deloitte Insights, 2016-02-24.

Motivation for Distributed Ledgers

Cryptography is about eliminating **trusted third parties.**

Blockchain technology applies **cryptography** to **transactions**.

Motivating desiderata:

- **Decentralisation:** no single point of trust, no single point of control (no central authority).
- **Security:** non-repudiation and irreversibility of records.
- **Reliability:** resistance to outages and manipulation.[2]

[2] Piscini, E. et al. Blockchain: Democratized trust. Deloitte Insights, 2016-02-24.

Motivation for Distributed Ledgers

Cryptography is about eliminating **trusted third parties.**

Blockchain technology applies **cryptography** to **transactions**.

Motivating desiderata:

- **Decentralisation:** no single point of trust, no single point of control (no central authority).
- **Security:** non-repudiation and irreversibility of records.
- **Reliability:** resistance to outages and manipulation.[2]
- **Auditability:** participants can verify the veracity of records directly, without external querying.

[2] Piscini, E. et al. Blockchain: Democratized trust. Deloitte Insights, 2016-02-24.

What is a Distributed Consensus Algorithm?

Private
distributed ledgers

(Nodes are explicitly authorised to participate.)

Call a vote

Supermajority threshold

Anonymous versus attributable

Public
distributed ledgers

(Anyone can run one or more participating nodes.)

Proof of Work
(i.e., computational power)

Proof of Stake
(i.e., wealth or age)

Proof of Ownership

Proof of Bandwidth

What makes for an appropriate use case? [IBM[3]]

[3] Source: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/#N1014E

What makes for an appropriate use case? [IBM[3]]

(1) Is a **business network** involved?

[3] Source: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/#N1014E

What makes for an appropriate use case? [IBM[3]]

(1) Is a **business network** involved?

(2) Is **consensus** used to validate transactions?

[3] Source: `https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/#N1014E`

What makes for an appropriate use case? [IBM[3]]

(1) Is a **business network** involved?

(2) Is **consensus** used to validate transactions?

(3) Is an **audit trail**, or provenance, required?

[3] Source: `https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/#N1014E`

What makes for an appropriate use case? [IBM[3]]

(1) Is a **business network** involved?

(2) Is **consensus** used to validate transactions?

(3) Is an **audit trail**, or provenance, required?

(4) Must the record of transactions be **immutable**, or tamper proof?

[3] Source: `https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/#N1014E`

What makes for an appropriate use case? [IBM[3]]

(1) Is a **business network** involved?

(2) Is **consensus** used to validate transactions?

(3) Is an **audit trail**, or provenance, required?

(4) Must the record of transactions be **immutable**, or tamper proof?

(5) Should dispute resolution be **final**?

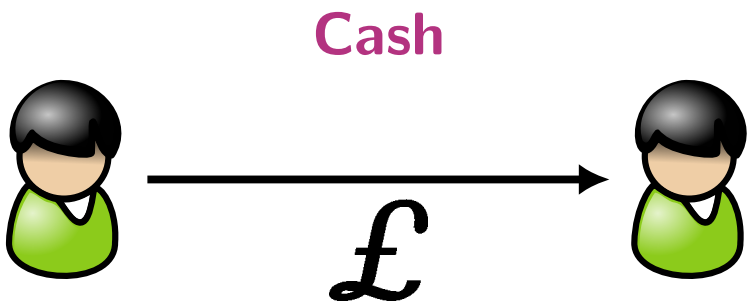
[3] Source: `https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/#N1014E`

Areas of Impact for DLT and Analytics

Payments	**Accountless** electronic transactions of value, including clearance and settlement
Contracts	Contracts that are **automatically executable**, **understandable** by computers, or both
Tax	**Real-time** collection of income tax, improved mechanisms for regulatory **reporting**
Trading	**Asset tracking** for supply chains, **decentralised marketplaces** for retail products
Identity	**Unlinkable** attribute-based credentials, support for **multiple identities** for individuals

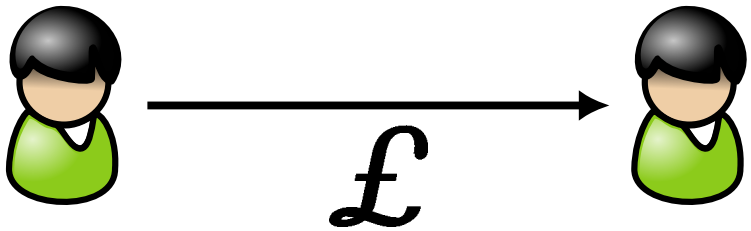
The Future of Payments

The Future of Payments



The Future of Payments

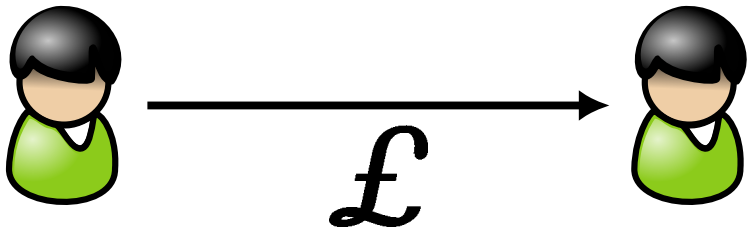
Cash



Direct interaction between transacting parties.

The Future of Payments

Cash

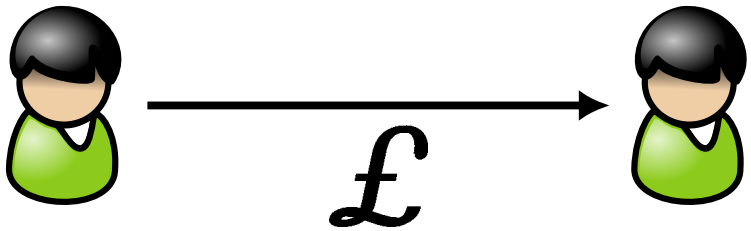


Direct interaction between transacting parties.

Currency is held **locally**.

The Future of Payments

Cash



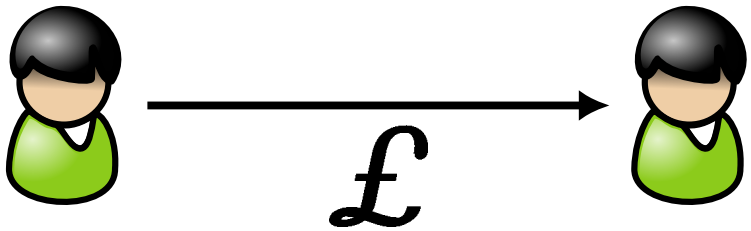
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

The Future of Payments

Cash



Direct interaction between transacting parties.

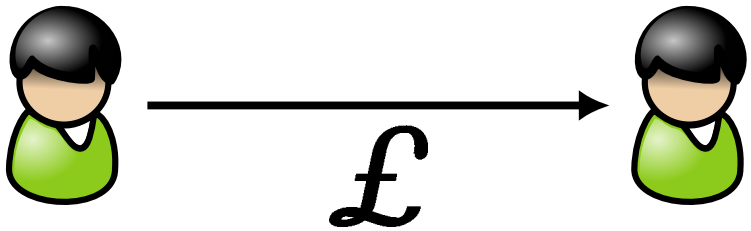
Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

Unlimited **choice** of currency.

The Future of Payments

Cash



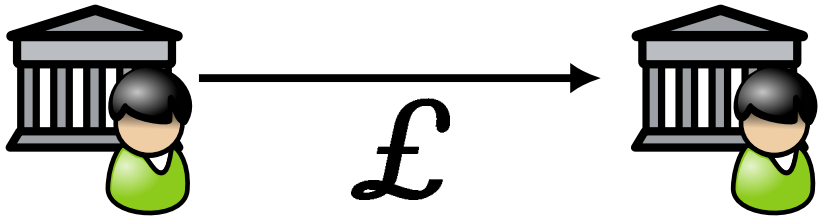
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

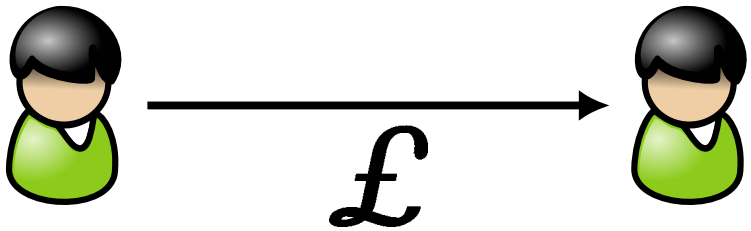
Unlimited **choice** of currency.

Retail Banking (cards, EFT, etc)



The Future of Payments

Cash



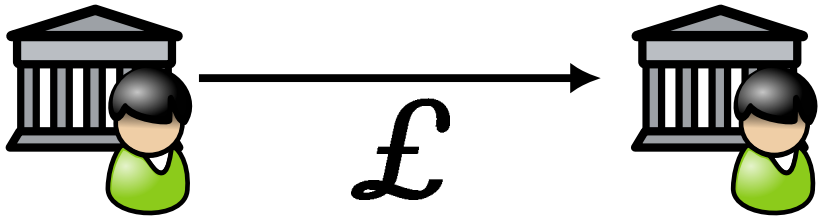
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

Unlimited **choice** of currency.

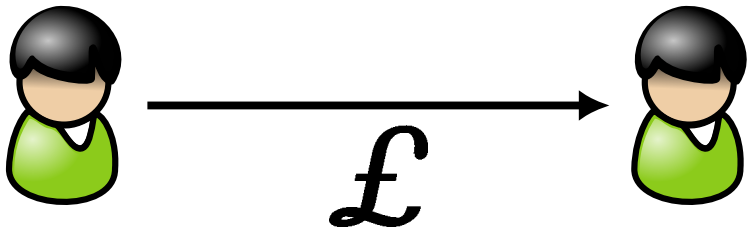
Retail Banking (cards, EFT, etc)



Interaction is actually between **regulated institutions**.

The Future of Payments

Cash



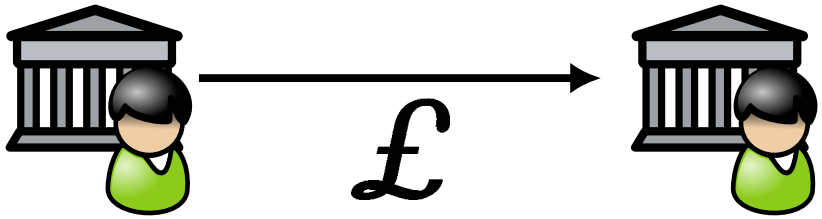
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

Unlimited **choice** of currency.

Retail Banking (cards, EFT, etc)

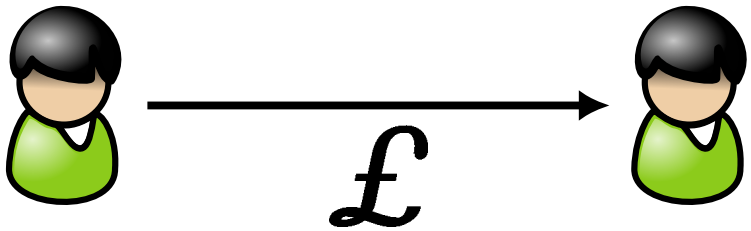


Interaction is actually between **regulated institutions**.

Currency is held **by institutions**.

The Future of Payments

Cash



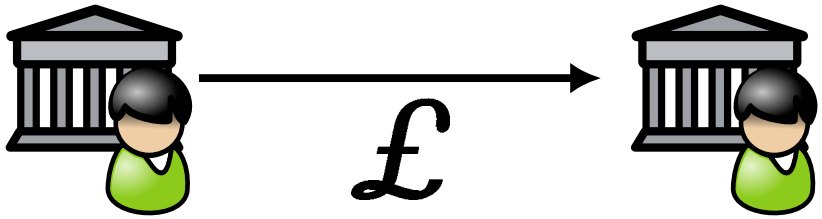
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

Unlimited **choice** of currency.

Retail Banking (cards, EFT, etc)



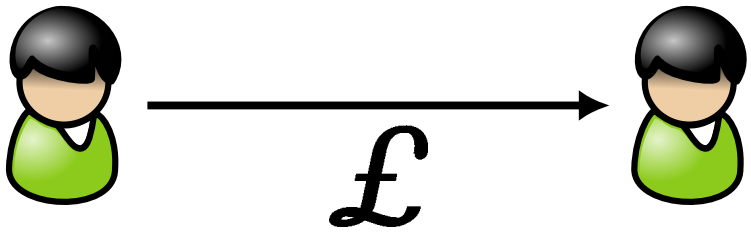
Interaction is actually between **regulated institutions**.

Currency is held **by institutions**.

Transactions may be **intermediated** or **blocked**.

The Future of Payments

Cash



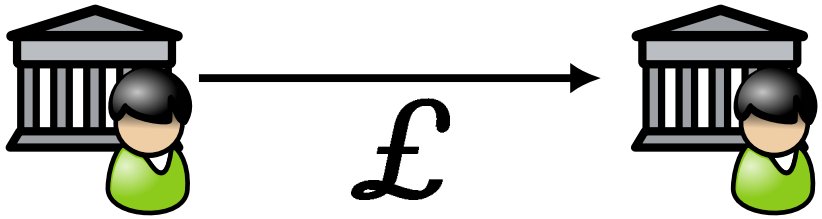
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

Unlimited **choice** of currency.

Retail Banking (cards, EFT, etc)



Interaction is actually between **regulated institutions**.

Currency is held **by institutions**.

Transactions may be **intermediated** or **blocked**.

Choice of currency may be limited by **regulations**.

The Future of Payments

Cryptocurrencies are really about Privacy

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

1982: David Chaum, "Blind Signatures for Untraceable Payments."

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

When Bitcoin launched in **2009**, the **financial crisis** offered an alternative justification (avoiding currency devaluation).

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

When Bitcoin launched in **2009**, the **financial crisis** offered an alternative justification (avoiding currency devaluation).

Privacy-oriented **enhancements** and **alternatives** continued to evolve:

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

When Bitcoin launched in **2009**, the **financial crisis** offered an alternative justification (avoiding currency devaluation).

Privacy-oriented **enhancements** and **alternatives** continued to evolve:

- **2014**: Monero

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

When Bitcoin launched in **2009**, the **financial crisis** offered an alternative justification (avoiding currency devaluation).

Privacy-oriented **enhancements** and **alternatives** continued to evolve:

- **2014**: Monero
- **2016**: Zcash

The Future of Payments

Cryptocurrencies are really about Privacy

A "Pre-History" of Modern Cryptocurrencies

- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

When Bitcoin launched in **2009**, the **financial crisis** offered an alternative justification (avoiding currency devaluation).

Privacy-oriented **enhancements** and **alternatives** continued to evolve:

- **2014**: Monero
- **2016**: Zcash
- **2016**: Mimblewimble

The Future of Payments

The Future of Payments

Digital currencies are like **cash**:

- Accountless, bearer instruments, with cash-like payments
- No permanent record of transaction counterparties (maybe)
- Everyone's money is as good as everyone else's (in principle)

The Future of Payments

Digital currencies are like **cash**:

- Accountless, bearer instruments, with cash-like payments
- No permanent record of transaction counterparties (maybe)
- Everyone's money is as good as everyone else's (in principle)

Cryptocurrencies may threaten monetary sovereignty and may operate beyond public control.

The Future of Payments

Digital currencies are like **cash**:

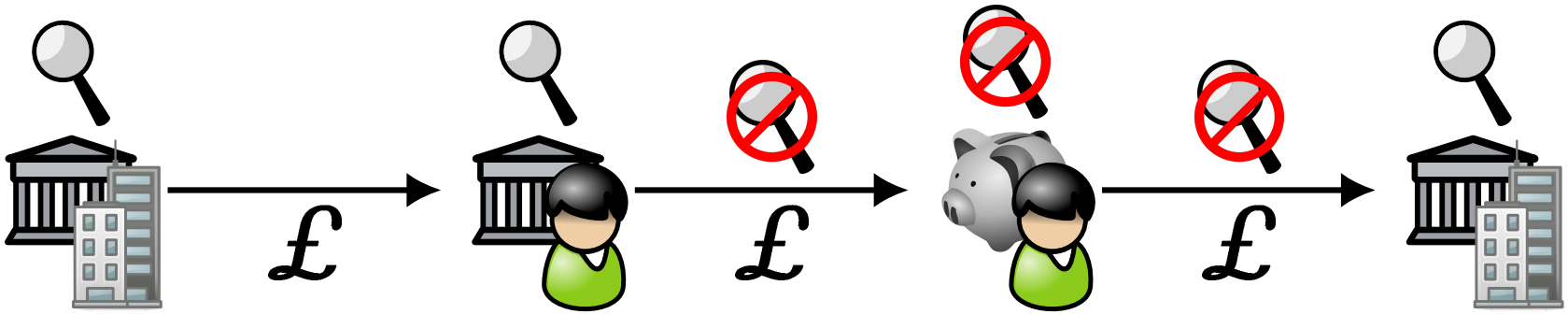
- Accountless, bearer instruments, with cash-like payments
- No permanent record of transaction counterparties (maybe)
- Everyone's money is as good as everyone else's (in principle)

Cryptocurrencies may threaten monetary sovereignty and may operate beyond public control.

What are the **dangers** of forbidding the use of **cash** or digital currency (perhaps issued by a central bank) that is potentially usable for certain purposes (e.g. money laundering, terror finance, organised crime)?

The Future of Payments

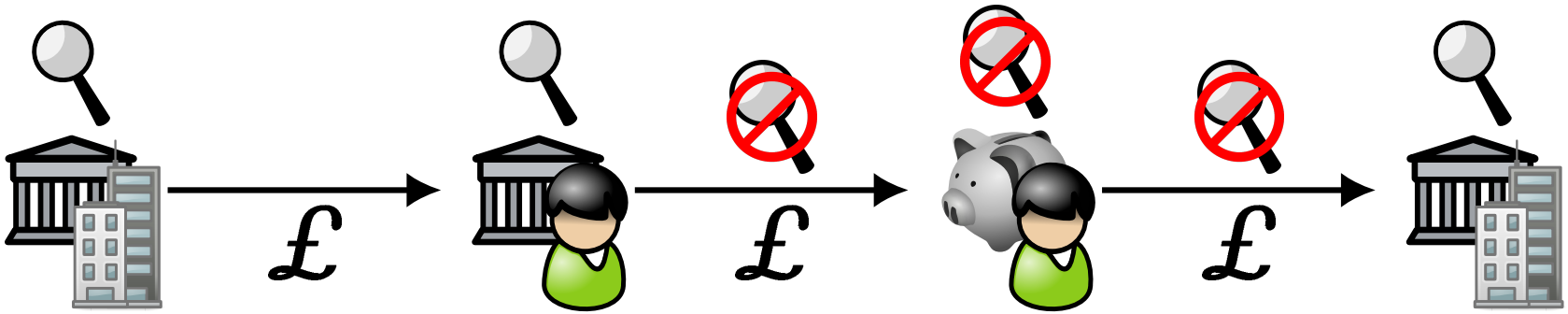
One approach: **Institutionally Mediated Private Value Exchange**[4]



[4] G. Goodell and T. Aste. **"Can Cryptocurrencies Preserve Privacy and Comply with Regulations?"** Frontiers in Blockchain, May 2019. doi:10.3389/fbloc.2019.00004

The Future of Payments

One approach: **Institutionally Mediated Private Value Exchange**[4]

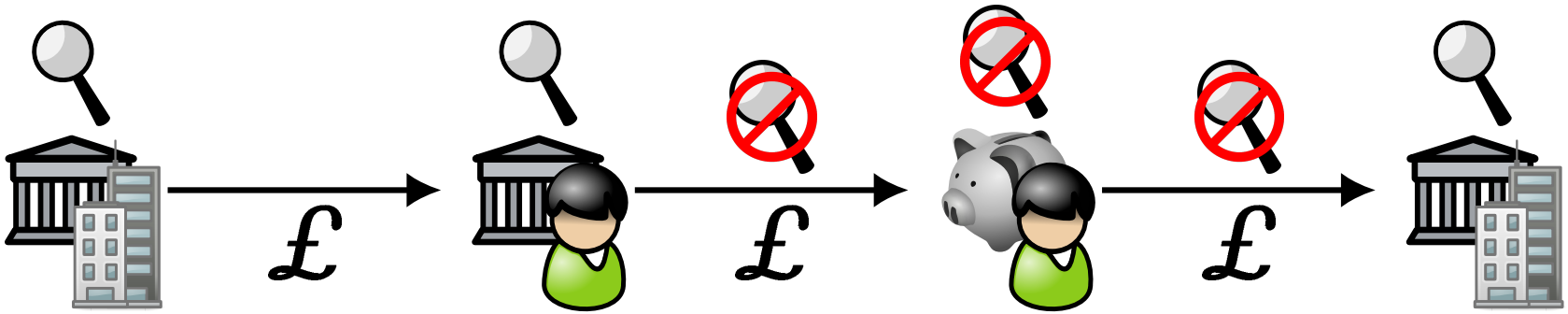


An individual receives funds into her **institutional account** (second icon from left) and transfers them to her **private store** (second icon from right).

[4] G. Goodell and T. Aste. **"Can Cryptocurrencies Preserve Privacy and Comply with Regulations?"** Frontiers in Blockchain, May 2019. doi:10.3389/fbloc.2019.00004

The Future of Payments

One approach: **Institutionally Mediated Private Value Exchange**[4]



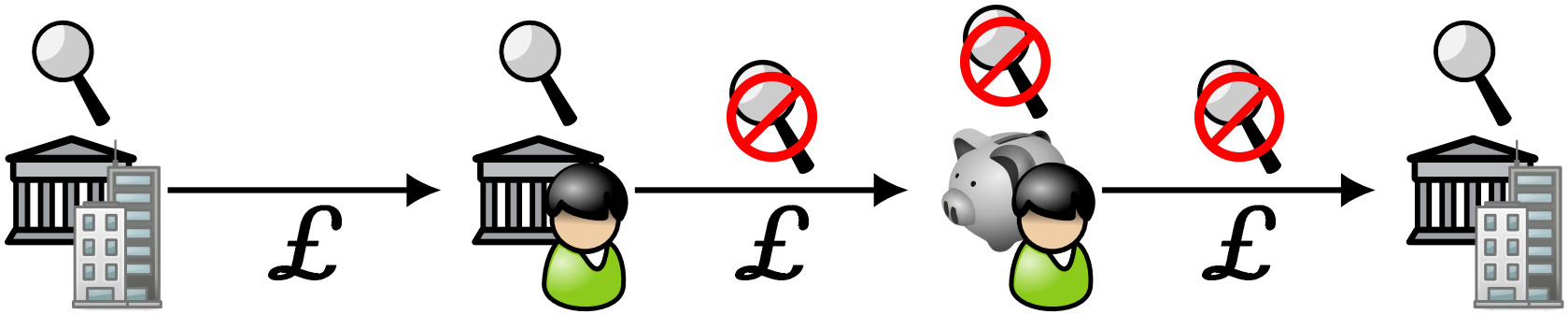
An individual receives funds into her **institutional account** (second icon from left) and transfers them to her **private store** (second icon from right).

The funds might be **central bank digital currency** (**CBDC**, as indicated by the Pound Sterling symbols) rather than cryptocurrency.

[4] G. Goodell and T. Aste. **"Can Cryptocurrencies Preserve Privacy and Comply with Regulations?"** Frontiers in Blockchain, May 2019. doi:10.3389/fbloc.2019.00004

The Future of Payments

One approach: **Institutionally Mediated Private Value Exchange**[4]



An individual receives funds into her **institutional account** (second icon from left) and transfers them to her **private store** (second icon from right).

The funds might be **central bank digital currency** (**CBDC**, as indicated by the Pound Sterling symbols) rather than cryptocurrency.

When she wants to make a payment, she must remit it from her private store to an account held by a **regulated institution** (rightmost icon).

[4] G. Goodell and T. Aste. **"Can Cryptocurrencies Preserve Privacy and Comply with Regulations?"** Frontiers in Blockchain, May 2019. doi:10.3389/fbloc.2019.00004

The Future of Tax

Distributed ledgers might make it easier to identify tax liabilities and prove payments.

Analytics might make it easier to identify tax fraud.

Future payment systems might facilitate **real-time** payment of **income taxes** (not just transaction taxes).

An opportunity to elaborate the social contract beyond narrowly-defined taxation?

Image Source: eveningtelegraph.co.uk

The Future of Contracts

Smart Contracts (aka distributed applications):[5] Formal procedures encoded in language to be interpreted and executed by nodes of a distributed system, so that the original authors (or agreeing parties) are not required to carry out the procedure themselves.

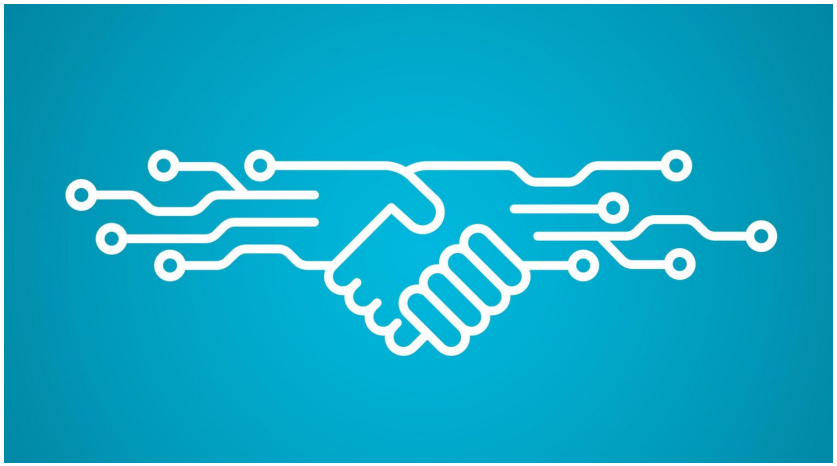
Computable Contracts:[6] interactive and integrated expressions of the intentions of the parties that are understandable by computers as well as by humans.

Image Source: US Army (wikimedia.org)

[5] Szabo, N. "Formalizing and Securing Relationships on Public Networks." First Monday 2(**9**), 1997-09-01.

[6] Clack, C. `http://fincomp.cs.ucl.ac.uk/research/computable_contracts/`

The Future of Trading



Asset tracking in supply chains (e.g. for agricultural products)

Decentralised marketplaces for retail goods and services.

Improved **surveillance** of securities markets.

More efficient **energy markets** and distribution networks.

Image Source: blockgeeks.com

The Future of Identity

Centralised identity and authorisation gives rise to powerful third-party authentication service providers that:

The Future of Identity

Centralised identity and authorisation gives rise to powerful third-party authentication service providers that:

(1) occupy a position of **control** via **surveillance**

The Future of Identity

Centralised identity and authorisation gives rise to powerful third-party authentication service providers that:

(1) occupy a position of **control** via **surveillance**

(2) occupy a position of **control** via **denial of service**

The Future of Identity

Centralised identity and authorisation gives rise to powerful third-party authentication service providers that:

(1) occupy a position of **control** via **surveillance**

(2) occupy a position of **control** via **denial of service**

(3) capture **monopoly rents**

The Future of Identity

Centralised identity and authorisation gives rise to powerful third-party authentication service providers that:

(1) occupy a position of **control** via **surveillance**
(2) occupy a position of **control** via **denial of service**
(3) capture **monopoly rents**
(4) invite **corruption** and **capture**

More **assurance** is **not always better**: the greater the assurance needed, the more narrow and limited the use case must be.

Image Source: storify.com

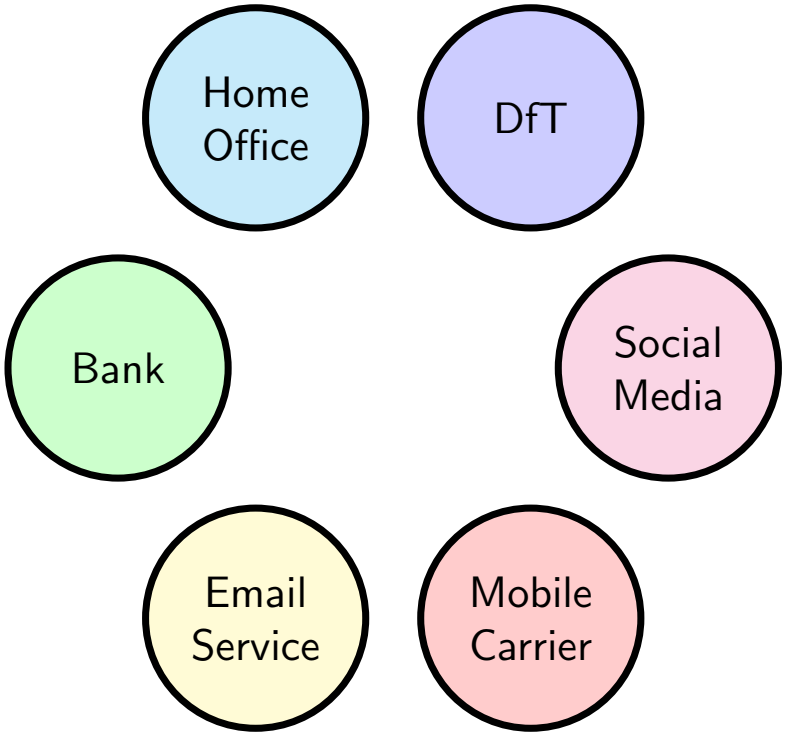
The Future of Identity

A popular approach: **Non-transferable Anonymous Credentials**[7]

[7] Camenisch, J and Lysyanskaya, A. **"An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation."** Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2001: Advances in Cryptology), **2001-04-15**, pp. 93–118. `https://eprint.iacr.org/2001/019.pdf`

The Future of Identity

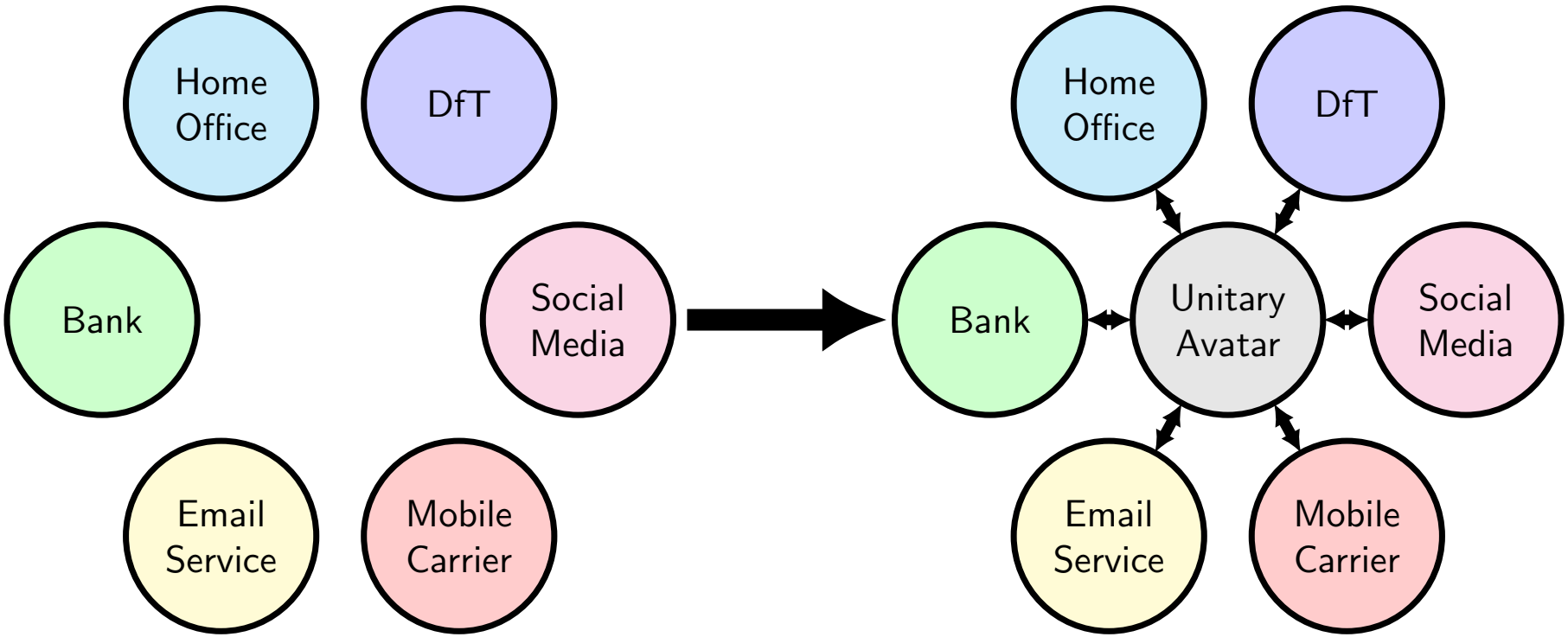
A popular approach: **Non-transferable Anonymous Credentials**[7]



[7] Camenisch, J and Lysyanskaya, A. **"An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation."** Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2001: Advances in Cryptology), **2001-04-15**, pp. 93–118. `https://eprint.iacr.org/2001/019.pdf`

The Future of Identity

A popular approach: **Non-transferable Anonymous Credentials**[7]



[7] Camenisch, J and Lysyanskaya, A. **"An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation."** Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2001: Advances in Cryptology), **2001-04-15**, pp. 93–118. `https://eprint.iacr.org/2001/019.pdf`

The Future of Identity

[8] G. Goodell, T. Aste. **"A Decentralised Digital Identity Architecture."** To appear, Frontiers in Blockchain.

The Future of Identity

(1) If a link between two attributes can be proven, then it can be **forcibly discovered**.

[8] G. Goodell, T. Aste. **"A Decentralised Digital Identity Architecture."** To appear, Frontiers in Blockchain.

The Future of Identity

(1) If a link between two attributes can be proven, then it can be **forcibly discovered**.

(2) The requirement of a unitary avatar **influences and constrains** how individuals can behave.

[8] G. Goodell, T. Aste. **"A Decentralised Digital Identity Architecture."** To appear, Frontiers in Blockchain.

The Future of Identity

(1) If a link between two attributes can be proven, then it can be **forcibly discovered**.

(2) The requirement of a unitary avatar **influences and constrains** how individuals can behave.

(3) More assurance is **not always better**: the greater the assurance needed, the more narrow and limited the use case must be.

[8] G. Goodell, T. Aste. **"A Decentralised Digital Identity Architecture."** To appear, Frontiers in Blockchain.

The Future of Identity

(1) If a link between two attributes can be proven, then it can be **forcibly discovered**.

(2) The requirement of a unitary avatar **influences and constrains** how individuals can behave.

(3) More assurance is **not always better**: the greater the assurance needed, the more narrow and limited the use case must be.

(4) Might multiple unlinkable identities be a **human right**?

[8] G. Goodell, T. Aste. **"A Decentralised Digital Identity Architecture."** To appear, Frontiers in Blockchain.

The Future of Identity

(1) If a link between two attributes can be proven, then it can be **forcibly discovered**.

(2) The requirement of a unitary avatar **influences and constrains** how individuals can behave.

(3) More assurance is **not always better**: the greater the assurance needed, the more narrow and limited the use case must be.

(4) Might multiple unlinkable identities be a **human right**?

(5) Virtually unlinkable identities might be achievable with DLT.[8]

[8] G. Goodell, T. Aste. **"A Decentralised Digital Identity Architecture."** To appear, Frontiers in Blockchain.

Challenges for Building a DLT Community

Governance: what are the rules and who should have a say?

Challenges for Building a DLT Community

Governance: what are the rules and who should have a say?

Education: the system requires technology and procedures; how do we ensure that users are competent?

Challenges for Building a DLT Community

Governance: what are the rules and who should have a say?

Education: the system requires technology and procedures; how do we ensure that users are competent?

Growing the community requires **long-term stewardship** and a **light touch**.

Challenges for Building a DLT Community

Governance: what are the rules and who should have a say?

Education: the system requires technology and procedures; how do we ensure that users are competent?

Growing the community requires **long-term stewardship** and a **light touch**.

System integrators and consultants must be able to focus on **guidance**, **support**, and **advocacy**, rather than operating the infrastructure or choosing specific platforms.

Challenges for Building a DLT Community

Governance: what are the rules and who should have a say?

Education: the system requires technology and procedures; how do we ensure that users are competent?

Growing the community requires **long-term stewardship** and a **light touch**.

System integrators and consultants must be able to focus on **guidance**, **support**, and **advocacy**, rather than operating the infrastructure or choosing specific platforms.

Co-regulation may be an option: consider the example of best execution (e.g. NMS in the US, MiFID in the EU).

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Whether it is constructive or destructive depends upon the specific **application** and **implementation**.

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Whether it is constructive or destructive depends upon the specific **application** and **implementation**.

For every new proposed DLT-related policy or initiative, always ask:

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Whether it is constructive or destructive depends upon the specific **application** and **implementation**.

For every new proposed DLT-related policy or initiative, always ask:

- How will it work as a **system**? (technology and policy together)

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Whether it is constructive or destructive depends upon the specific **application** and **implementation**.

For every new proposed DLT-related policy or initiative, always ask:

- How will it work as a **system**? (technology and policy together)
- Does it assume **decentralisation**? (that never lasts...)

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Whether it is constructive or destructive depends upon the specific **application** and **implementation**.

For every new proposed DLT-related policy or initiative, always ask:

- How will it work as a **system**? (technology and policy together)
- Does it assume **decentralisation**? (that never lasts...)
- Whose **interests** are behind it?

Conclusions

Blockchain (and DLT in general) offers real value for business and human society alike.

Whether it is constructive or destructive depends upon the specific **application** and **implementation**.

For every new proposed DLT-related policy or initiative, always ask:

- How will it work as a **system**? (technology and policy together)
- Does it assume **decentralisation**? (that never lasts...)
- Whose **interests** are behind it?
- **Cui bono?** (Who benefits?)

Thank You

Photo Credit: https://www.pinterest.co.uk/pin/736268239051855079/