

Blockchain Finance

Robert Sams

March 2015

clearmatics

The Big Idea

If we can transfer digital currency on a blockchain, why not transfer stocks, bonds and other assets on a blockchain?

Thesis: if it works for **on-chain** assets, it can work for **off-chain** assets.

What are the bankers saying?

Oliver Bussmann, CIO of UBS

I believe—and this is my personal view—that **blockchain technology** will not only change the way we do payments but it will change the whole trading and settlement topic.

Bank of England, *Quarterly Bulletin*

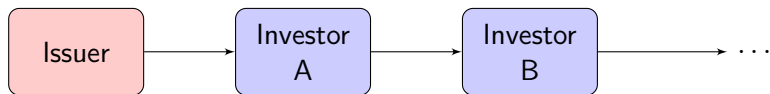
In a similar way, the potential impact of the **distributed ledger** may be much broader than on payment systems alone. The majority of financial assets—such as loans, bonds, stocks and derivatives—now exist only in electronic form, meaning that the financial system itself is already simply a set of digital records. These records are currently held in a tiered structure. . . but it may be possible in the future—in theory, at least—for the existing infrastructure of the financial system to be gradually replaced by a variety of distributed systems.

Let's replace this. . .



Source: Richard Gendal Brown <http://gendal.me>

... with this!



No intermediaries! P2P finance!

The 3 Sins of a Centralised Ledger

Sin of Commission **forgery** of transaction

Sin of Omission **censorship** of transaction

Sin of Deletion **reversal** of transaction

My thesis

You cannot eliminate all three. You must choose to minimise either **censorship** or **reversal**, but not both.

The 3 Sins of a Centralised Ledger

Sin of Commission **forgery** of transaction

Sin of Omission **censorship** of transaction

Sin of Deletion **reversal** of transaction

My thesis

You cannot eliminate all three. You must choose to minimise either **censorship** or **reversal**, but not both.

Code-as-Property-Law?

Nick Szabo

Fiduciary code will often execute some of the functions traditionally thought of as the role of commercial law or security, but with software that securely and reliably spans the globe regardless of traditional jurisdiction. Thus: Property titles (registered assets), where the on-chain registry is either the **legally official registry for off-chain assets** or controls on-chain ones, thus providing reliable and secure custody of them.

Wrong!

Not if the blockchain is based on *permissionless validation*.
Much of "Blockchain Finance" is really a **political programme** to bring back *bearer assets* in cryptographic form.

Code-as-Property-Law?

Nick Szabo

Fiduciary code will often execute some of the functions traditionally thought of as the role of commercial law or security, but with software that securely and reliably spans the globe regardless of traditional jurisdiction. Thus: Property titles (registered assets), where the on-chain registry is either the **legally official registry for off-chain assets** or controls on-chain ones, thus providing reliable and secure custody of them.

Wrong!

Not if the blockchain is based on ***permissionless validation***.
Much of "Blockchain Finance" is really a **political programme** to bring back *bearer assets* in cryptographic form.

Take your pick

Permissionless blockchain (e.g. Bitcoin)

- censorship resistant
- reversals possible
- only suitable for **on-chain** assets

Permissioned blockchain (e.g. Distributed Ledger)

- legally accountable validators
- no reversals – settlement finality
- suitable for **off-chain** assets like securities, fiat currency, . . .

Take your pick

Permissionless blockchain (e.g. Bitcoin)

- censorship resistant
- reversals possible
- only suitable for **on-chain** assets

Permissioned blockchain (e.g. Distributed Ledger)

- legally accountable validators
- no reversals – settlement finality
- suitable for **off-chain** assets like securities, fiat currency, . . .

Take your pick

Permissionless blockchain (e.g. Bitcoin)

- censorship resistant
- reversals possible
- only suitable for **on-chain** assets

Permissioned blockchain (e.g. Distributed Ledger)

- legally accountable validators
- no reversals – settlement finality
- suitable for **off-chain** assets like securities, fiat currency, . . .

What Really Works

Distributed Ledger

- Blockchain (Permissioned)
- Distributed Virtual Machine (Turing-complete)
- Smart contracts govern **off-chain** assets
- Network achieves **settlement finality**

What Really Works

Distributed Ledger

- Blockchain (Permissioned)
- Distributed Virtual Machine (Turing-complete)
- Smart contracts govern **off-chain** assets
- Network achieves **settlement finality**

What Really Works

Distributed Ledger

- Blockchain (Permissioned)
- Distributed Virtual Machine (Turing-complete)
- Smart contracts govern **off-chain** assets
- Network achieves **settlement finality**

What Really Works

Distributed Ledger

- Blockchain (Permissioned)
- Distributed Virtual Machine (Turing-complete)
- Smart contracts govern **off-chain** assets
- Network achieves **settlement finality**

What Really Works

Distributed Ledger

- Blockchain (Permissioned)
- Distributed Virtual Machine (Turing-complete)
- Smart contracts govern **off-chain** assets
- Network achieves **settlement finality**

Implication: Eliminate the Clearing House

Smart contracts replace **intermediation** between buyer and seller.

- Simultaneous exchange of assets peer-to-peer
- Payment-versus-Payment (FX)
- Delivery-versus-Payment (Securities Settlement)

Implication: Eliminate the Clearing House

Smart contracts replace **intermediation** between buyer and seller.

- Simultaneous exchange of assets peer-to-peer
- Payment-versus-Payment (FX)
- Delivery-versus-Payment (Securities Settlement)

Implication: Eliminate the Clearing House

Smart contracts replace **intermediation** between buyer and seller.

- Simultaneous exchange of assets peer-to-peer
- Payment-versus-Payment (FX)
- Delivery-versus-Payment (Securities Settlement)

Implication: Eliminate the Clearing House

Smart contracts replace **intermediation** between buyer and seller.

- Simultaneous exchange of assets peer-to-peer
- Payment-versus-Payment (FX)
- Delivery-versus-Payment (Securities Settlement)

Implication: Eliminate ISDA Derivatives

Smart contracts replace **ISDA** Master Agreement.

- Independent valuation
- High-frequency variation margining
- Enforcement by **collateral** rather than **law** (legal recourse)

Implication: Eliminate ISDA Derivatives

Smart contracts replace **ISDA** Master Agreement.

- Independent valuation
- High-frequency variation margining
- Enforcement by **collateral** rather than **law** (legal recourse)

Implication: Eliminate ISDA Derivatives

Smart contracts replace **ISDA** Master Agreement.

- Independent valuation
- High-frequency variation margining
- Enforcement by **collateral** rather than **law** (legal recourse)

Implication: Eliminate ISDA Derivatives

Smart contracts replace **ISDA** Master Agreement.

- Independent valuation
- High-frequency variation margining
- Enforcement by **collateral** rather than **law** (legal recourse)

Which Moral Imperative?

Choose the right technology for the objective.

- Censorship resistant finance → **Permissionless** blockchain
- Reform financial markets → **Permissioned** blockchain

Follow me

Robert Sams

Twitter: @codedlogic, @clearmatics