APPLICATION OF BLOCKCHAIN IN FINANCE
区块链的金融应用

Engineering Authority

The economics of blockchain application design

Steve Randy Waldman || swaldman@mchange.com || http://www.interfluidity.com/

What is a blockchain?

Why would we want one?

When would we want one?

When *wouldn't* we want one?

What kind of blockchain application?

…open, or "permissionless"

…closed, or "permissioned"

…hybrid blockchain/traditional designs

What is a blockchain?

The term “blockchain” refers to a family of networked application architectures that serve to automate an existing costly labor-intensive process.

What is a blockchain?

The term “blockchain” refers to a family of networked application architectures that serve to automate an existing costly labor-intensive process.

What costly labor-intensive process???

What costly labor-intensive process???

…the production of AUTHORITY

What is authority?

…authority is a **characteristic of information** that causes a wide variety of individuals, institutions, and firms who may have **divergent interests** and perspectives to **behave as if** the information is true

…regardless of whether or not the content of the information **serves a party's interests or even is actively harmful to those interests**

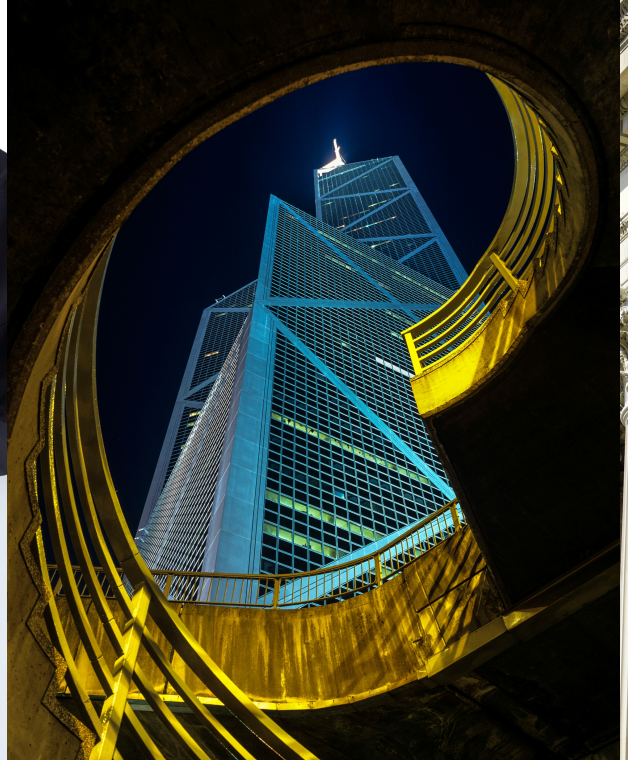
…**regardless of whether a party actually agrees that the information is true!**

Authority lies in the **relationship between information and human behavior**

Information is authoritative not because of what it “says”,
but **by virtue of how humans respond to it**

Authority is **essential to social, economic, and political coordination**

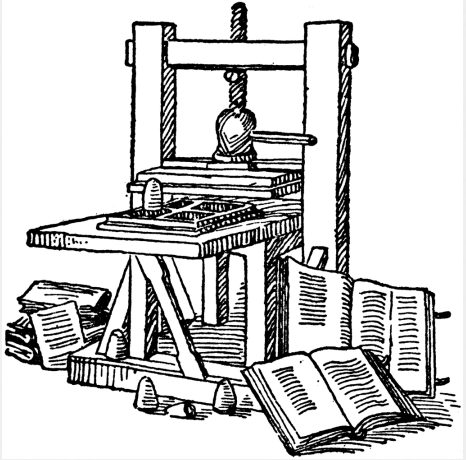
Authority is an old, solved problem.




Authority is an old, solved problem.
But traditional technologies of production for authority are labor-intensive and costly.

Are blockchains a “revolution”?



…maybe!

…but in the way that the Gutenberg Press was a “revolution”.

…it’s not that they let us do anything new

…they let us do old things **so much more cheaply that novel applications become radically more accessible!**

What is a blockchain?

The term “blockchain” refers to a family of networked application architectures that serve to **automate the production of authority.***

* largely, not entirely

Why would we want one?

We might want a blockchain application because we wish the information our application produces **to be authoritative** among a wide variety of individuals, institutions, and firms **who may have divergent interests and perspectives**.

When would we want a blockchain application?

…when the computations of your application need to be authoritative **outside the boundaries of your own organization** (defined not by legal form but by unitary IT).

…when the **incremental cost** of accessing traditional sources of authority would be high.

…or, when the **incremental savings** of accessing the traditional sources of authority would be large.

When would we ***not*** want a blockchain application?

…**most of the time**, for existing business applications**.**

…beware **chainwashing** (Tim Swanson)
http://www.ofnumbers.com/2017/02/13/chainwashing/

…there's no need for a blockchain when the computations of your application need not be authoritative **outside the boundaries of your own organization**.

- because the information will only used internally
- because external users will **never have either the desire or the capacity to meaningfully dissent** from the information your application produces

…when **regulatory fixed-costs** mean the incremental cost of accessing traditional authority is low.

…when privacy considerations rule out a blockchain application, for now (perhaps **changing soon**)

Comparative cost of executing and managing computation

High Cost	Medium Cost	Low Cost
Independent, discretionary access of labor-intensive traditional infrastructure *e.g. clearing bureaucracies with audited accounts defined and governed only by legal arrangements*	Industry-amortized private blockchain Deployment on existing, widely-used public blockchain platform Access of traditional infrastructure adjacent to nondiscretionary regulatory use	Purely internal business application

Authoritative — Non-authoritative

What kind of blockchain application do we want?

…open, or “permissionless”

…closed, or “permissioned”

…hybrid blockchain/traditional designs

Authority, community, and consensus

We said…

"authority is a **characteristic of information** that causes a wide variety of individuals, institutions, and firms who may have **divergent interests** and perspectives to **behave as if** the information is true"

Authority, community, and consensus

But more accurately, we should have said…

"authority is a **characteristic of information** **in the context of some community** that causes a wide variety of individuals, institutions, and firms **within that community** who may have **divergent interests** and perspectives to **behave as if** the information is true"

Authority is engendered by **enforced consensus** within the **particular community** over which the authority will prevail

…which might range from a **small, particular group of people**

…to an **industry consortium**

…to a **national community**

…to potentially **everyone in the world**

Authority, community, and consensus

…blockchain systems require **near-unanimity within the community** to enforce consensus

…blockchain systems rely on **participatory verification and norms of representation** to generate the consent that underlies consensus

…blockchain systems depend upon **ordinary indifference**

— authority can fail if large fractions (or factions) of blockchain participants have shared, divergent, incentives with respect to potential outcomes. Most nodes should be indifferent to most potential actions

…both to maximize ordinary indifference and uphold norms of participation and representation, blockchain systems should be designed to **include, or at least offer an option of inclusion, to all members of the community** over which its information is intended to be authoritative

Authority, community, and consensus

Note: This is very different from traditional modes of authority, where *in extremis* a state can coercively enforce authority despite severe, organized disagreement with the community the state superintends.

Should my blockchain application be open or closed?

Applications face tradeoffs

…open, permissionless, blockchain systems **maximize participation, representation, and the principle of ordinary indifference**

…existing open blockchain platforms can be **inexpensively used**, while closed blockchains usually require bespoke development and deployment of blockchain infrastructure

…open blockchain systems are, at least for now, **computationally less performant than closed, permissioned systems**

…open blockchain systems are complex and typically out of the application users' control, arguably increasing **operating risk**

…open blockchain systems, at least for now, may be **unsuitable for many applications due to privacy and regulatory concerns**

When might private, “permissioned” blockchains be best?

Closed blockchain applications are ideal **when the community over which the blockchain is to be authoritative is itself restricted** to a moderate number of actors **who can share the cost** of designing, building, and maintaining the system.

- …since the community itself is finite, a closed blockchain can in this case be **fully representative and participatory** while still enjoying the performance and privacy benefits that come with a permissioned system.
- …consortia of **efficiency-seeking incumbents in well-defined industries** (e.g. finance) are already in the process of replacing low-efficiency authority production with closed, permissioned blockchains.
- …**small communities and organizations** might eventually define bespoke permissioned blockchains, but for now they are too novel and expensive to develop

When might open blockchains be best?

Open blockchain applications are ideal **when the community over which the blockchain is to be authoritative is unrestricted**, enabling a large and indefinite community of users to participate.

Preexisting open blockchains are **ideal for small-business and entrepreneurial use-cases**, because development for public, open platforms is inexpensive and representation or participation in the authority-generating process is available to all potential customers.

…liquid, tradable tokens for local investment and small-business finance

Bespoke open blockchains are ideal for **large-scale internet applications and protocols in which the broad public are invited to participate**.

…so far mostly cryptocurrencies

…but perhaps soon digital infrastructure, decentralized ride-sharing or social networks, etc.

Hybrid permissioned blockchain + regulatory blessing

Likely model for large financials
…clearing and settlement
…escrow and collateral management
…auditing of mutualized central counterparty exposure

In hybrid model, closed, permissioned blockchains generate authority *within the community defined by industry consortia* while the imprimatur of the traditional state will extend authority to the rest of us.

Promising for a variety of inefficiently performed highly regulated or direct state functions for
…notary and digital signature management
…documentation of identity
…real estate, land, and cadastral registries

Competitive Privatization!

Conclusion

Blockchains are an **ordinary technological breakthrough**. They automate and make cheaper a previously expensive labor-intensive production processes.

The process blockchains automate is **the production of authority** and authoritative information in human communities

For large financial organizations that currently make extensive use of traditional, expensive means of producing authority, **blockchains will create efficiency gains**

The radical cheapness of blockchain-based authority production will make possible **new kinds of business arrangements, network protocols, and institutions** that are exciting but difficult to foresee.

Engineering blockchains is a social problem as much as it is technical. An understanding of **how you are producing authority and for whom** must guide technical choices.

Global Fintech Summit

Appendix: Three levels of consensus

1… Metaconsenus

2… Procedural consensus

3… Enforced consensus

Appendix: Three levels of consensus

1… Metaconsenus

Agreement as to the laws or rules that will usually govern what information comes to be viewed as authoritative, usually determined by legislatures and professional organizations in traditional production of authority, negotiated informally among stakeholders for blockchain systems so far (although systems like Dfinity and Tezos may soon formalize)

2… Procedural consensus

3… Enforced consensus

Appendix: Three levels of consensus

1… Metaconsenus

2… Procedural consensus

Consensus generated by following the laws or rules that specify the production of authoritative information under ordinary circumstances. In traditional production of authority, generating procedural consensus is the day-to-day work of auditors, regulators, lawyers, banks, and courts. In a blockchain system, this is “automatic consensus” (Gavin York’s term), what comes of the system generating and incorporating new blocks according to its protocol.

3… Enforced consensus

Appendix: Three levels of consensus

1… Metaconsenus

2… Procedural consensus

3… Enforced consensus

Usually the enforced consensus is simply the procedural consensus.

But nearly all systems of authority have the capacity to recognize exceptions, and create a divergence between procedural and enforced consensus. Governments can pardon individuals, or pass special laws to alter prior outcomes. Stakeholders in blockchain systems can arrange hard forks, and newer systems define special procedures for overriding automatic consensus. In both kinds of system, experience of exceptions are sometimes fed back into modifications of the rules (and so alter the metaconsensus), or sometimes are treated as one-offs.