Blockchain Economics

Abadi & Brunnermeier (2018)

Cameron Pfiffer

University of Oregon

January 18th, 2019

Introduction

Quick summary

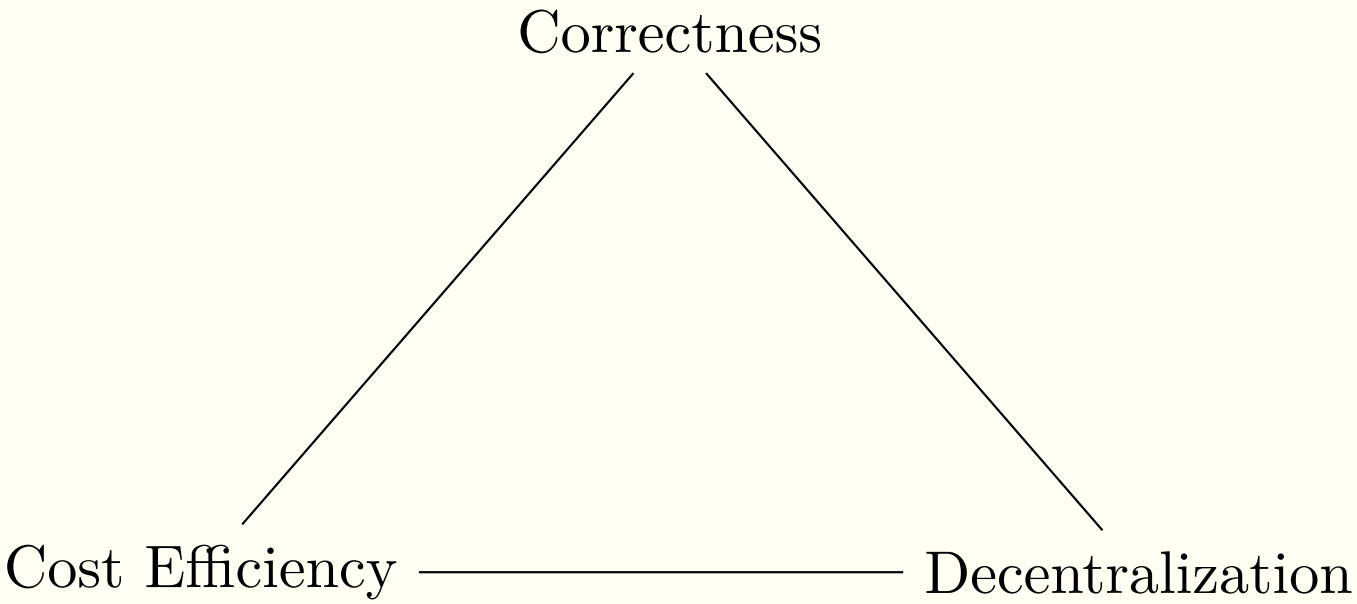
Abadi and Brunnermeier construct a theoretical model to examine general equilibrium in ledger competition under various circumstances.

Key takeaways (shamelessly lifted from the abstract)

1. No ledger perfectly balances correctness, decentralization, and cost efficiency.
2. Centralized ledgers allow the record-keeper to extract rents.
3. Blockchains suppress these rents and reduce or eliminate switching costs[1].
4. Enforcement of ownership is hard on blockchains.

[1] The authors claim sort of hand-wave that switching blockchains incurs no switching costs, but I don't think this is true.

The ledger trilemma



Pick two.

Types of ledgers

Centralized ledgers are things like Amazon, or Google, or clearing and settlement houses. The person who changes the system's rules also holds everyone's information.

Decentralized ledgers are general blockchains, such as the record system for Bitcoin, Ripple, or Ethereum. Record maintainers and people who change the ledger's rules are not necessarily the same.

What is a blockchain

What is a blockchain

A blockchain is a ledger in which agents known as nodes (or miners, or record-keepers) take turns recording information sequentially in data structures known as blocks.

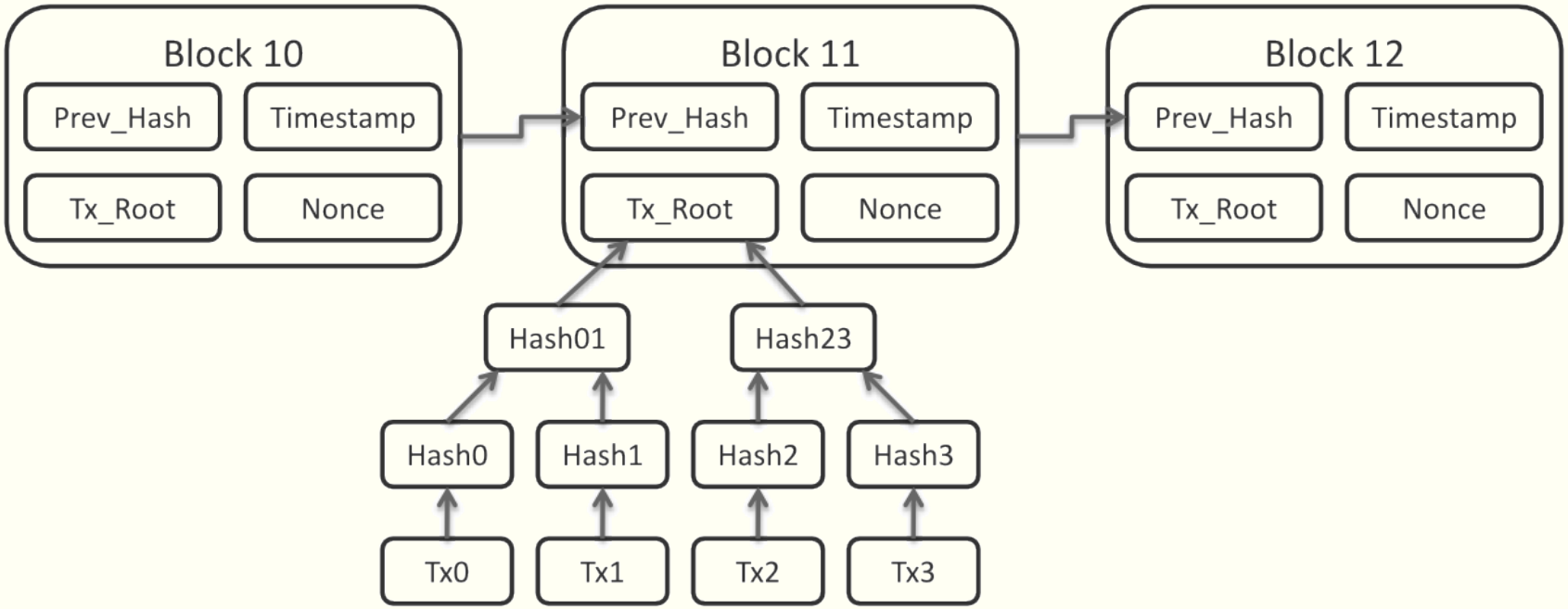
What's in a blockchain?

Data includes

- Payment histories
- Contracts
- Wagers
- Ownership of domain names
- Anywhere information needs to be recorded

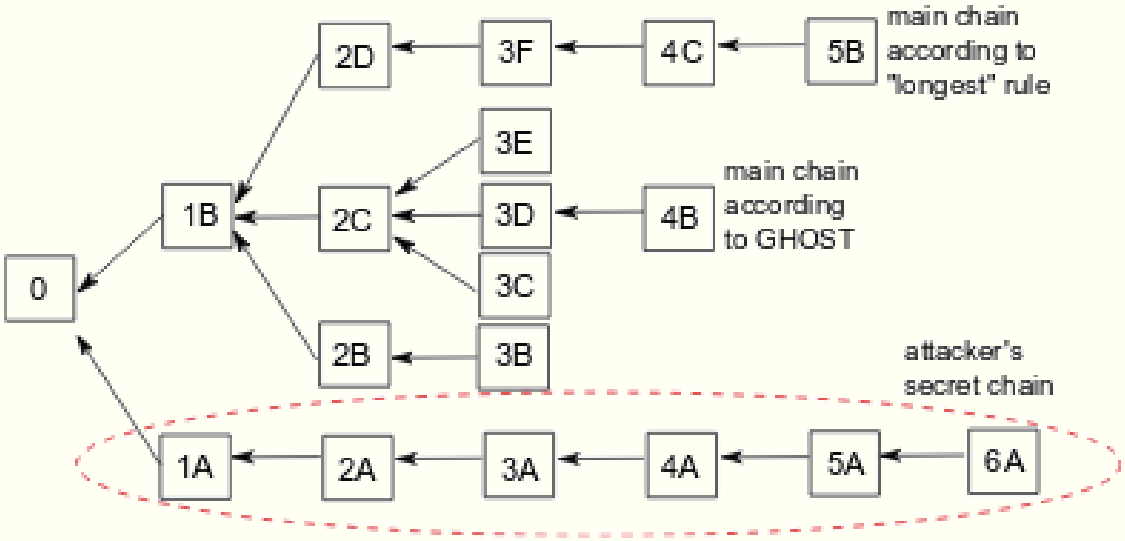
What do they look like?

The blockchain begins with a genesis block, and then blocks are added in sequential order. Record-keepers do math (in most cases[2]) to attach blocks to chains.



[2]See *proof of stake* for more information on when this is not true.

But they are not always linear



What is a blockchain

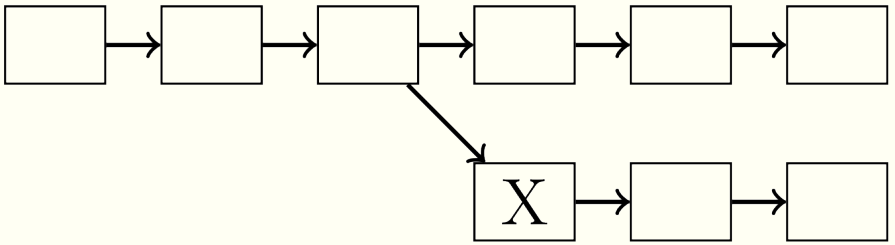
Blockchains have a security dimension — they are not always safe from people trying to cheat, but the authors show that this is a good thing, because of forks.

Types of bad activity:

- Sybil attacks
- 51% attacks
- Double spending

Forks

Blockchains can undergo a hard fork, where the chain splits into pieces. Users decide which fork is "real".



Forks

Hard forks can occur when

- Someone has a more efficient way for the system to operate
- Someone wants to change the fees that record-keepers earn
- The community wants to undo history

Types of blockchains

Types of blockchains

1. Private
2. Permissioned
3. Public

Private blockchains

- Single record-keeper
- Very computationally efficient
- Record-keeper is disciplined by users
- The Record-keeper can set all the rules

Permissioned blockchains

- Consortium of known entities are record-keepers
- Record-keepers disciplined by both users and other record-keepers
- Not very common

Public blockchains

- The most recognizable blockchain
- Read and write privileges unrestricted
- Requires computationally difficult exertion from record-keepers
- Very cost inefficient[3]

[3] As cited in this paper, Bitcoin's blockchain uses more electricity than Hungary to process transactions.

Differences in blockchains and centralized ledgers

1. Record-keepers are *transient* in blockchains. No trust required.
2. Information is portable.
3. The thread of a *rollback* is always present in the event of fraudulent activity.

Model of Ledger Choice

Agents

- Ledgers A, B.
- Continuum of users $i \in [0, 1]$.
- Record keepers $j \in M$.
- Two proposers P^A and P^B. Sometimes a record keeper can be a proposer.

Features

- Three-step infinite horizon model.
- Users choose $\phi_i = (\phi_i^A, \phi_i^B)$, representing participation intensity. They can only pick one[^switching-costs].
- Users have stakes in each ledger, $s_i = (S_i^A, S_i^B)$.
- Common value ξ, representing the "better" ledger. $\xi > 0$ implies A is better, $\xi < 0$ implies B is better.
- Proposers choose a parameter L^A and L^B for their ledgers. Think of these as fees or revenues to record-keepers.
- Record keepers choose a_j, representing either honest proof-of-work or attempts at fraud.

Equilibrium

Equilibrium with arbitrary ledgers

Users coordinate on the better ledger when their stakes don't fix them to any ledger.

If users have stakes in one ledger, they may coordinate even if the other ledger is better. If the stakes are transferable, users move to the better ledger.

Traditional competition between centralized ledgers

Network effects and initial stakes anchor users to their ledgers. The incumbent ledger has an advantage.

The equilibrium fee charged by an incumbent is monotonically increasing in the collective stake of the users.

Fork competition

Let A be the original chain, and B be a hard fork of A. The stakes for each users are identical in each ledger ($s_i^A = s_i^B$), as information is perfectly replicated between the two.

In this case, the ledgers are in perfect competition, and there's no rent extracted by record-keepers.

Fork competition — model extensions

Proposers incentives are aligned with users.

Record-keepers contribute computational power $c_j \leq 1$ to secure either A or B in each period.

Fork competition — results

Free-entry requires that record-keepers only break even in equilibrium. This is not so for permissioned blockchains.

When there is an opportunity to make a fork, users choose the cheaper fork and proposers choose rules that benefit users.

The competition between record-keepers and the portability of information ensure perfect competition.

Currency competition

Traders trade in decentralized markets during the day, and centralized markets at night.

Agents can adopt currencies on ledgers A or B in the centralized market without cost, or adopt it in the decentralized market at some cost χ^A or χ^B. It is assumed that $\chi^A = 0$, and users only have to choose whether to adopt B.

Currency competition

Value functions for users are given by

$$W(m^A, m^B|A, B) = \psi^A m^A + \psi^B m^B + \frac{\delta}{1-\delta} E[S|A, B]$$

where ψ represents the value of a currency in terms of goods, m represents the units held, δ represents a discount factor, and $E[S|A, B]$ is the expectations about trade surplus in the decentralized market.

$E[S|A, B]$ captures network effects to some extent, which is critical for later results.

Currency competition

In cases where there has been a fork and $m^A = m^B$, users are incentivized to engage in some activity in B even if they don't want to accept the currency. This engagement encourages others to interact as a function of increased network effect.

The endowment effect here can help a less-established currency to gain widespread recognition. Think about Bitcoin and the USD — the dollar is objectively a better currency, but an endowment effect at play in Bitcoin and its forks encourage users to engage.

Future research

Possible topics

1. The idea of how users choose to develop their stakes through investment in differing ledgers is an interesting one, and would expand more on the opportunity cost incurred by switching between ledgers.
2. The model does not address an equilibrium chain. Is there an "optimal blockchain" using some combination of fees and features?
3. When users are endowed after a fork, what kind of financial implications are there? Can we observe some equilibrium or average effect after this endowment?