1 Finance and blockchain

Stephen G. Cecchetti and **Kermit L. Schoenholtz**[1]
Brandeis International Business School and CEPR; NYU Stern School of Busines

> "Only 1% of 3,138 chief information officers at companies surveyed by Gartner last year said they had 'any kind of blockchain adoption'…."
> *The Wall Street Journal*, 7 May 2018.

Blockchain is all the rage. We are constantly bombarded by reports of how it will change the world. While it may alter many aspects of our lives, our suspicion is that they will be in areas that we experience only indirectly. That is, blockchain technology mostly will change the implementation of invisible processes – what businesses think of as their *back-office* functions.

In this chapter, we briefly describe blockchain technology, the problem it is designed to solve, and the impact it might have on finance.

Blockchain basics

Blockchain is a record-keeping mechanism; a 21st century version of the recording systems that have been around since people started chiselling marks on cave walls. Over the millennia we have moved from ledgers that are carved into clay and stone to ones that are digital.

To be more specific, consider the problem of tracking the ownership of a share of equity. Imagine that there is a sequential list of all owners, with the name of each

[1] We thank Morten Bech, Ethan Cecchetti, and Hanna Halaburda for patiently explaining many aspects of how the blockchain works and how its applications to economics and finance. An earlier version of this chapter appeared on www.moneyandbanking.com.

crossed out, except for that of the current owner. The key question is the following: who has the right to cross out a name and write in a new one?

Put another way, the challenge we face is to create a tamper-proof and universally accepted way of recording things like ownership of assets, obligations of one person to provide a product or service to another, levels of inventories, personal identities, and the like. What we require is that the system be a reliable, secure, and trusted mechanism for accessing and updating essential records that cannot be hijacked by someone with ill intent.

The four types of ledgers

In thinking about the challenge of maintaining records – a ledger – consider differences along two dimensions: the structure of the database in which the records are stored, and how we establish that any changes are legitimate. Along the first dimension – *ledger structure and ownership* – the database and its ownership can be either *centralised* or *distributed*. And, on the second dimension – *access rights* – the system can have *limited access* in which a restricted number of people (or entities) can make alterations, or *open and public access* (also called 'permissionless') so that anyone can participate. In either case, following a legitimate modification, all versions are immediately updated, guaranteeing agreement on the current state.

This two-by-two classification system leads to four ledger frameworks. To understand this taxonomy, Tables 1 and 2 provide a set of nonfinancial and financial examples.[2]

The upper-left cell of each table is the case of a centralised database with limited, proprietary access rights. This case captures the ledger practices of human civilisation until now. There is one central ledger containing the authoritative record of ownership or obligations that can only be changed by the organisation or person maintaining it. While there may be copies, there is only one definitive version. Examples are everywhere – hospital records and records of securities ownership are just two.

[2] For a more detailed discussion with examples, see Haeringer and Halaburda (2018) and Dwyer (2016).

Table 1 Ledger structure and ownership, and access rights: Nonfinancial examples

		Access rights	
		Limited/Propietary	Open/Public
Ledger structure and ownership	Centralised	Hospital records (current systems)	Customer ratings (user review websites)
	Distributed	Supply chain inventory* (closed, trusted networks)	Property title* (proof of work/stake systems)

Note: *Potential implementations.

Table 2 Ledger structure and ownership, and access rights: Financial examples

		Access rights	
		Limited/Propietary	Open/Public
Ledger structure and ownership	Centralised	Securities ownership records (current systems)	CFPB Consumer Complaint Database (user review websites)
	Distributed	CLSnet (closed, trusted networks)	Bitcoin (proof of work)

Note: CFPB is the Consumer Financial Protection Bureau.

Turning to the top-right cell, this is the case of an open-access, but centralised recording system that allows anyone to write and read. Lacking security, this mechanism is of limited use. Nevertheless, examples exist. In the nonfinancial realm, these include the customer rating systems employed by Amazon, eBay, TripAdvisor and the like. Wikipedia uses this protocol for creating and updating entries. Given the security concerns, financial examples are more difficult to find. One instance is the Consumer Complaint Database of the Consumer Financial Protection Bureau (CFPB).

The bottom rows cover the range of distributed (or decentralised) databases. The distinction here is that there are now many copies of the ledger, all with equal standing. So long as they follow an agreed set of rules, anyone who has a copy can make a change. Put another way, participants directly interact with each other. And, as with the centralised systems, there are two cases: limited access and permissionless.

Blockchain technology seeks to implement distributed systems, providing automatic mechanisms that create trust, ensuring there are no conflicting changes, and preventing malicious actors from making unauthorised or improper changes. It has the potential to record transactions between two parties, maintaining an agreed sequence, without reliance on potentially costly third-party verification.

To prevent people from arbitrarily attacking the system, violating trust, and making illegitimate modifications, the ability to alter the ledger is based on a scarce resource. In the limited-access model, the scarce resource is identity – only specific people or institutions can make modifications. The idea of an open system is to make identity irrelevant – anyone can join, leave, and re-join as often as desired. Here the scarce resource that allows alterations to the ledger can be something like computational power or a stake (possibly financial) in the system.

In the open system, participants can make changes so long as they follow the rules. Importantly, the rules must prevent a bad actor from capturing the system. The original Bitcoin protocol, where the scarce resource is computational power, is immune from takeover so long as no one controls more than half of the computing power. But, as has been pointed out repeatedly, the system is incredibly expensive, generating substantial deadweight loss. Electricity costs alone exceed $3 billion per year.

The uncertain future of blockchain

Both financial and nonfinancial uses of blockchains remain limited, with the obvious exceptions of cryptocurrencies. In Table 1, we list two possible nonfinancial applications – supply chain inventory management and property title records – but so far as we know, neither has yet been implemented on a broad scale.

Where is this all heading? Without a further theoretical breakthrough, open distributed systems appear both costly and slow. Estimates for the Bitcoin protocol, for example, are that speeds cannot exceed seven transactions per second. In contrast, there may be some promise in distributed systems that are proprietary. We suspect that most of the corporate developers working on such projects have this kind of architecture in mind, perhaps in the hopes of creating a profitable monopoly. Unfortunately, a monopolist would be unlikely to lower transactions costs in the way that the advocates of open distributed systems hope.

Conceivably, a blockchain system could securely track the ownership of every financial instrument and exposure in the global economy. While this is a very tall order, it would be truly revolutionary. Financial market participants could overcome information asymmetries, improving risk pricing and capital allocation. Authorities could monitor position concentrations and other risks to the financial system. And, money laundering and terrorist finance would be easier to police.

In practice, we are still a long way off. Before we can map the entirety of the financial system, we need to be able to identify both entities and instruments globally.[3] But even if such identifiers are in place, we question whether people would be happy with the result. It would create a *world without privacy* in which everyone's balance sheet and transactions are public. Even if a much less invasive version were to become possible, it would be deeply ironic if blockchain, a technology initially championed by libertarians disenchanted by government and fiat money, ended up by narrowing the range of individual freedoms.

Today, blockchain faces a major problem of *scalability*. The fastest proprietary blockchain systems currently can handle no more than several thousand transactions per second.[4] To put this into perspective, at its peak the Depository Trust & Clearing Corporation (DTCC) processes 25,000 equity transactions per second (roughly the same as VISA's payments processing capacity). DTCC (2018) points out that any new technology would have to have a maximum capacity of 2 to 3 times this peak – more

[3] For a discussion of global legal entity identifiers (LEIs) and global financial instrument identifiers (FIIs), see Cecchetti and Schoenholtz (2017b).

[4] Since all copies of a distributed ledger must be revised before anyone can record the next transaction, the speed of light materially limits the rate at which these systems can operate. If, for example, there a ledger is in both New York and London, at a minimum, it will take between 20 to 40 milliseconds for a transaction in one location to be recorded in the other. This means that fully distributed systems cannot process more than 50 transactions per second. Some degree of centralisation, combined with geographic proximity, lowers this latency and increases the maximum throughput.

than 50,000 equity transactions per second. For the foreseeable future, given physical constraints on the speed of transmission for such a large volume of information, we see no way that the financial system can escape its reliance on centralised clearing and settlement systems.[5]

Conclusion

All that said, we really have little idea where this will lead. A decade since the appearance of Nakamoto's (2008) paper that launched Bitcoin, we have more than 1,000 crypto-clones. But where are the broader applications of the blockchain technology? We expect that it will find increased use in the clearing, payments, and settlement system (Cecchetti and Schoenholtz 2017a). Perhaps it also will be applied across a range of other activities, such as recording property titles or managing the supply chain both within and across firms or for a variety of accounting and audit functions. Such applications would likely focus on cases with limited numbers of transactions and where speed is less important. But, for now, we anticipate the development and implementation of proprietary systems, not those with open access.

References

Bank for International Settlements (BIS) (2018), "Cryptocurrencies: looking beyond the hype", Annual Economic Report, June.

Budish, E (2018), "The Economic Limits of Bitcoin and the Blockchain",NBER Working Paper No. 24717.

Cecchetti, S G and K L Schoenholtz (2017a), "Modernizing the U.S. Payments System: Faster, Cheaper, and More Secure", www.moneyandbanking.com, 31 July.

[5] Permissionless distributed systems of the type use for Bitcoin also face a severe incentive problem. As Chapter V of the most recent BIS Annual Economic Report (BIS 2018) describes in detail, the possibility that the system will be taken over means that it is impossible to guarantee finality. Budish (2018) derives the condition under which Bitcoin-style systems will be attacked and captured by a malicious actor.

Cecchetti, S G and K L Schoenholtz (2017b), “Managing Risk and Complexity: Legal Entity Identifier“, www.moneyandbanking.com, 30 October.

Depository Trust and Clearing Corporation (DTCC) (2018), “Modernizing the U.S. Equity Markets Post-Trade Infrastructure“, January.

Dwyer, G P (2016), “Blockchain: A Primer“, MPRA Paper 76562, University Library of Munich.

Haeringer, G and H Halaburda (2018), “Bitcoin: A Revolution?”, Baruch College Zicklin School of Business Research Paper No. 2018-05-01.

Nakamoto, S (2018), “Bitcoin: A Peer-to-Peer Electronic Cash System”.

About the authors

Stephen G. Cecchetti is the Rosen Family Chair in International Finance at the Brandeis International Business School. Before rejoining Brandeis in 2014, he completed a five-year term as Economic Adviser and Head of the Monetary and Economic Department at the Bank for International Settlements. During his time at the BIS, Cecchetti participated in the numerous post-crisis global regulatory reform initiatives. In addition to his other appointments, Cecchetti served as Director of Research at the Federal Reserve Bank of New York; Editor of the J*ournal of Money, Credit, and Banking*; and is currently Research Associate of National Bureau of Economic Research and Research Fellow of the Centre for Economic Policy Research since 2008. Cecchetti has published widely in academic and policy journals, and is the author of a leading textbook in money and banking. Together with Kim Schoenholtz, he blogs at www.moneyandbanking.com.

Kim Schoenholtz is the Henry Kaufman Professor of the History of Financial Institutions and Markets in the Economics Department of NYU Stern School of Business. He also directs the Stern Center for Global Economy and Business. Previously, Schoenholtz was Citigroup’s Global Chief Economist from 1997 until 2005. Schoenholtz currently serves on the Financial Research Advisory Committee of the U.S. Treasury’s Office of Financial Research. He also is a panel member of the U.S. Monetary Policy Forum and a member of the Council on Foreign Relations. Previously, he served on the CEPR

Executive Committee.Schoenholtz is co-author of a popular textbook on money, banking and financial markets and of a blog on the same topic at www.moneyandbanking.com. Schoenholtz was a Visiting Scholar at the Bank of Japan's Institute for Monetary and Economic Studies from 1983 to 1985. He holds an M.Phil. in economics from Yale University and an undergraduate degree from Brown University.