



Transaction Banking by D Sign

Blog

Professor Michael Mainelli
July 2015

The Temple & The Souk – The Future Of Mutual Distributed Ledgers

Boring old accounting ledgers have become one of the most exciting technologies of our time. Growing confidence in ‘mutual distributed ledgers’, such as the Blockchain technology underlying Bitcoin, is transforming people’s views of trusted third parties, and money itself. Bitcoin questions the nature of money, but mutual distributed ledgers question the future of economics and finance.

Boring Old Ledgers

A ledger is a book, file, or other record of financial transactions. People have used various technologies for ledgers over the centuries. The Sumerians used clay cuneiform tablets for recording transactions. Medieval folk used split tally sticks. So much so in England that, when tally sticks were retired in 1834, the destruction of so many tallies got out of control and burned down the Houses of Parliament. In the modern era, the implementation of choice for a ledger is a database, found in all modern accounting systems. So far, so boring.

When many parties interact and need to keep track of complex sets of transactions they have traditionally found that creating a centralised ledger is helpful. A centralised transaction ledger needs a trusted third party who makes the entries (validates), prevents double counting or double spending (safeguards), and holds the transaction histories (preserves). Over the ages centralised ledgers are found in registries (land, shipping, tax), exchanges (stocks, bonds), or libraries (index and borrowing records), just to give a few examples. In the modern era, the implementation of choice for a centralised ledger is a centralised database run by a trusted third party, such as a bank, an insurer, an exchange, or a registry.

Exciting New Ledgers

“Although the monetary aspects of digital currencies have attracted considerable attention, the distributed ledger underlying their payment systems is a significant innovation.” ... “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.”

Bank of England, Quarterly Bulletin (2014, Q3)

Bitcoin relies on a database of all bitcoins ever traded, its Blockchain. The Blockchain is a public ledger of integrity without central authority. Bitcoin ‘mining’ is a ground-breaking way of concurrently validating new transactions with no central authority. Blockchain is a



ground-breaking way of providing a pervasive and persistent ledger. While a work of genius, the Bitcoin and its Blockchain could be equally regarded as just a new assemblage of existing components. The principal components are public-key cryptography (Diffie-Hellman circa 1976) and a proper decentralised peer-to-peer network (Gnutella 2000). The two technical weaknesses are also apparent. If public-key cryptography is cracked, or internet peer-to-peer somehow switches off, then cryptocurrencies would fail, along with much else in modern finance starting with credit cards.

Mutual distributed ledgers allow groups of people to validate, record, and track transactions across a network of decentralised computer systems. The ledger itself is a distributed data structure held in part or in its entirety by each participating computer system. The computer systems follow a common protocol to add new transactions. The protocol is distributed using peer-to-peer application architecture. Peers are equally privileged participants in the protocol. Mutual distributed ledgers are not new – concurrent and distributed databases have been researched and implemented since at least the 1970s. But growing confidence has led numerous firms, particularly in financial services, to announce their interest in using them, Nasdaq, BNY Mellon, UBS, USAA, IBM, Samsung, and many others.

The Blockchain is just one type of public, permissionless, proof-of-work, peer-to-peer distributed ledger. Mutual distributed ledgers can be implemented in a number of ways. Perhaps the most common implementation choices are:

- ◆ public versus private – is reading the ledger open to all or just to defined members of a limited community?
- ◆ permissioned versus permissionless – are only people with permission allowed to add transactions, or can anyone attempt to add a transaction?
- ◆ proof-of-stake, proof-of-work, consensus or identity mechanisms – how are new transactions authorised?
- ◆ true peer-to-peer or merely decentralised – are all nodes equal and performing the same tasks, or do some nodes have more power and additional tasks?

The Temple Or The Souk?

At a conference in Germany in 1997 Eric Steven Raymond described the struggle between top-down and bottom-up software design, [The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary](#). He contrasted “happy networked hordes of programmer/anarchists [the bazaar] outcompeting and overwhelming the hierarchical world of conventional closed software [the cathedral]”.

So what does the future hold for ledgers? I would contrast the Temple of Financial Services against the Souk of the Sharing Economies. In the Temple the high priests of the Blockchain Maximalists and the Banking Traditionalists wage a schismatic war over ‘the One True Coin’. The Banking Traditionalists believe that these mutual distributed ledger fads too soon shall pass, leaving traditional banking intact. The Blockchain Maximalists, and adherents to some of the other blockchain services, believe that everything in financial services can be replaced. Each believes that only one ledger can prevail, or from the film Highlander, “there can be only one!”

Out in the Souk of Sharing Economies there is an explosion of vibrant stalls and frenzied groups of small shopkeepers engage in animated discussions with clients about a myriad of



ways of trading. Shopkeepers and clients are prototyping, experimenting, and finally deploying hundreds to thousands of different distributed ledgers. These ledgers are often in the corners of wholesale finance, insurance linked securities, OTC trading, registries, or small exchanges. These small communities typically use private, permissioned, identity-authorised ledgers. Meanwhile, governments try to make taxing the church or the market less slippery, with some governments, such as the Channel Islands, exploring how to evaluate sensibly the hundreds of ledgers that may be brought to them for regulation.

While my heart is with the Souk of Sharing Economies, my head recognises that there may be room for both. A sensible union would be a few, competing, ‘blockchain-type’ services encircling the globe providing end-of-day validation and recording of transactions, while thousands of mutual distributed ledgers do the busy work of serving thousands of shared economies. In effect, the merchants of the Souk bring their ledgers up to the Temple to be validated and timestamped by whichever priests occupy the Temple of Financial Services. It may not be orthodoxy, but it’s not heresy either.

[1,072 words]

About the author

*Professor Michael Mainelli is Executive Chairman of Z/Yen Group and Principal Advisor to Long Finance. His latest book, **The Price of Fish: A New Approach to Wicked Economics and Better Decisions**, written with Ian Harris, won the 2012 Independent Publisher Book Awards Finance, Investment & Economics Gold Prize.*