Blockchain: a solution looking for a problem

While new financial technologies show considerable promise, many proposed applications are either naive or miss the mark outright

The Holy Grail? Bitcoin is highly centralised and predominantly orientated towards the Chinese market

Alexander Lipton

27 September 2016

Alexander Lipton is a Connection Science Fellow at MIT and an Adjunct Professor of Mathematics at NYU.

Fintech in general, and blockchain and distributed ledger technology (DLT) in particular, are currently the toast of the town. Expectations of their impact on the banking industry are nothing short of miraculous; it looks like finance is going through a ‘cold fusion' phase. Potentially, fintech can have numerous applications; as of now, it is not clear which ones.

Although the current obsession with blockchain and DLT is inspired by Satoshi Nakamoto's 2009 tour de force, *Bitcoin: A peer-to-peer electronic cash system*, bitcoin is not the first digital currency and very likely not the last one either.

There are multiple historical examples of blockchains and distributed ledgers. For instance, family trees of ruling dynasties are blockchains. Moreover, since they were independently maintained in several capitals, they also represent distributed ledgers. More recently, we've seen digicash invented by David Chaum in the 1980s, and Bit Gold invented by Nick Szabo in the 1990s.

While all the building blocks of bitcoin have been known for some time, their unique combination captured the public's imagination only recently. In the beginning, bitcoin's appeal was strong, especially given justifiable disenchantment with the banking sector. It was expected to be a viable non-inflationary peer-to-peer currency based on a proof-of-work unpermissioned public ledger.[1]

> **“ Another problem to be addressed is the sheer scale of the global economy, which precludes the use of an unpermissioned public ledger such as bitcoin**

Reality proved to be less glamorous. Bitcoin supports about seven transactions per second, with real transaction costs of approximately 1.5%. This is down from 2012, when costs were a whopping 8%.[2]

Anecdotally, bitcoin consumes as much electricity as eBay, Facebook and Google combined, making mining a cost-of-electricity game. The environmental costs of bitcoin, which are frequently ignored, are obviously huge. Additionally, bitcoin uses an archaic single-entry accounting rather than a double-entry one.

Bitcoin miners coalesce in gigantic pools, with the three largest pools responsible for about two-thirds of all the work; thus, collusion among these pools makes a 51% attack possible, with the aggressor being able to revise a transaction history, or prevent new transactions from confirming.

Currently, rather than a worldwide distributed system, bitcoin is highly centralised and predominantly orientated towards the Chinese market. In the words of a Russian ex-prime minister Viktor Chernomyrdin, "we wanted the best, but it turned out as always".

Another problem to be addressed is the sheer scale of the global economy, which precludes the use of an unpermissioned public ledger such as bitcoin. This has led to permissioned public ledgers such as Ripple, and private ledgers such as those run by R3, IBM and Digital Asset Holdings, being proposed as alternatives.

That is not to say it is impossible to use DLT to good effect. Inspiration for its use comes from the Estonian experience of switching to a digital government, which was accomplished by connecting all important databases via an adaptor called the X-road.

A similar concept can be used to connect financial institutions via DLT. The financial X-road has to be a permissioned ledger, controlled by trusted notaries paid for their services. Two financial institutions use their respective adaptors to agree on a transaction, execute it via a smart contract, then secure it by hashing.

Afterwards, a quorum of notaries digitally signs the hash and posts it in the common layer, creating an immutable public record – ‘laminating' the transaction, in other words. It is imperative that both securities and cash are treated on a par.

One of the juicier targets is the Holy Trinity of capitalism – trading, clearance and settlement. DLT is clearly unsuitable for high-frequency trading, since distributed clocks are not truly synchronised. However, permissioned private ledgers can certainly cut costs, increase speed of clearing and settlement, and reduce the burden of reconciliation and failures. Yet, the instantaneous settlement – or T+15 minutes as it is occasionally called – should not be implemented, because it obliterates pillars of the current system such as netting, stock borrowing and anonymity.

There are several other areas where DLT can be useful. Trade finance, syndicated loans and other similar high-friction areas are additional attractive candidates for DLT. In global payments, the potential to use DLT is also relatively high. However, despite statements to the contrary, the existing payment system is expensive but not broken, so competition will be tough.

So although the idea of a blockchain and DLT is not novel, modern technology gives it a new life. It remains to be seen where its applications will be best served, however.

[1] The total number of bitcoins in circulation is now 21 million, 16 million of which have been mined and 3-5 million potentially irretrievably lost.

[2] Claims that bitcoin can solve the issue of half the world's population being unbanked are simply ludicrous.