In third parties we (mis)trust

Mutual distributed ledgers pose a threat to the trust relationship in financial services, write *Michael Mainelli* and *Vinay Gupta*

Trust leverages a history of relationships to extend credit and benefit-of-the-doubt to someone. Trust is about much more than money; it's about human relationships, obligations, experiences, and about anticipating what other people will do.

In risky environments trust enables cooperation and permits voluntary participation in mutually beneficial transactions which are otherwise costly to enforce or cannot be enforced by third parties. By taking a risk on trust, we increase the amount of cooperation throughout society while simultaneously reducing the costs, unless we are wronged.

Trust is not a simple concept, nor is it necessarily an unmitigated good, but trust is the stock-in-trade of financial services. In reality, financial services trade on mistrust. If people trusted each other on transactions, many financial services might be redundant.

Technology is transforming trust. Never before has there been a time when it's been easier to start a distant geographical relationship. With a credible website and reasonable products or services, people are prepared to learn about companies half a world away and enter into commerce with them. Society is changing radically when people find themselves trusting people with whom they've had no experience, e.g. on eBay or Facebook, more than banks they've dealt with their whole lives.

People use trusted third parties in many roles in finance, for settlement, as custodians, as payment providers, as poolers of risk. Trusted third parties perform three roles:

- **validate** – confirming the existence of something to be traded and membership of the trading community;
- **safeguard** – preventing duplicate transactions, i.e. someone selling the same thing twice or 'double-spending';
- **preserve** – holding the history of transactions to help analysis and oversight, and in the event of disputes.

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. Medieval folk split tally sticks. In the modern era, the implementation of choice for a ledger is a central database, found in all modern accounting systems. In many situations each business keeps their own central database with all their own transactions in it, and these systems are reconciled, often manually and at great expense if something goes wrong.

But in cases where 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.

The latest technological approach to all of this is the distributed ledger (aka blockchain aka distributed consensus ledger aka the Mutual Distributed Ledger – MDL, which we'll stick to here. To understand the concept, it helps to look back over the story of its development

1960/70s:Databases

The current database paradigm began c1970 with the invention of the relational model, and the widespread adoption of magnetic tape for record-keeping. Society runs on these tools to this day, even though some important things are hard to represent using them. Trusted third parties work well on databases, but correctly recording remote transactions can be problematic.

One approach to remote transactions is to connect machines and work out the lumps as you go. But when data leaves one database and crosses an organisational boundary, problems start. For Organisation A, the contents of Database A are operational reality, true until proven otherwise. But for Organisation B, the message from A is a statement of opinion. Orders sit as "maybe" until payment is made, and is cleared past the last possible chargeback: this tentative quality is always attached to data from the outside.

1980/90s: Networks

Ubiquitous computer networking came of age two decades after the database revolution, starting with protocols like email and hitting its full flowering with the invention of the World Wide Web in the early 1990s. The network continues to get smarter, faster, and cheaper, as well as more ubiquitous – and it is starting to show up in devices like our lightbulbs under names like the Internet of Things. While machines can now talk to each other, the systems that help us run our lives do not yet connect in joined up ways.

Although in theory information could just flow from one database to another with your permission, in practice the technical costs of connecting databases are huge. Worse, we go back to paper and metaphors from the age of paper because we cannot get the interconnection software right. All too often, the computer is simply a way to fill out forms: a high-tech paper simulator. It is nearly impossible to get two large entities to share our information between them on our behalf.

Of course, there are attempts to clarify this mess – to introduce standards and code reusability to help streamline business interoperability. You can choose from EDI, XMI-EDI, JSON, SOAP, XML-RPC, JSON-RPC, WSDL and half a dozen more standards to "assist" your integration processes. The reason there are so many standards is because none of them finally solved the problem.

Take the problem of scaling collaboration. Say that two of us have paid the upfront costs of collaboration and have achieved seamless technical harmony, and now a third partner joins our union, then a fourth, and a fifth … by five partners, we have 13 connections to debug: by 10 partners the number is 45. The cost of collaboration keeps going up for each new partner as they join our network, and the result is small pools of collaboration which just will not grow. This isn't an abstract problem – this is banking, this is finance, medicine, electrical grids, food supplies, and the government.

A common approach to this quadratic quandary is to put somebody in charge, a hub-and-spoke solution. We pick an organisation – Visa would be typical – and all agree that we will connect to Visa using their standard interface. Each organisation has to get just a single connector right. Visa takes 1% off the top, making sure that everything clears properly.

But while a third party may be trusted, it doesn't mean they are trustworthy. There are a few problems with this approach, but they can be summarised as 'natural monopolies'. Being a hub for others is a license to print money for anybody that achieves incumbent status. Visa gets 1% or more of a very sizeable fraction of the world's transactions with this game; Swift likewise. If you ever wonder what the economic upside of this MDL business might be, just have

THE SHIP REGISTRY SKIT

Act I: Validating.
Shady Shipper: "I'd like to register my vessel. Here's a photo I took on the island this morning of my supertanker berthed at the port terminal".
Scrupulous Registrar: "We need a bit more than that to go on, your purchase certificate, IMO ship registration number, tonnage certificate, load line certificate …"
Shady Shipper: "Here's $10,000"
Scrupulous Registrar: "That will do nicely, Sir".

Act II: Transacting.
Shady Shipper: "I'd like to sell my vessel once to Otto and once to Maria".
Sanctimonious Registrar: "But that's not possible."
Shady Shipper: "Here's $10,000".
Sanctimonious Registrar: "That will do nicely, Sir".

Act III: Recording.
Shady Shipper: "I have to go to court and need you to change your historical records for me such that only Maria is shown to own the ship".
Shady Registrar: "That could cost you…"
Shady Shipper: "Here's $10,000".
Shady Registrar: "That will do nicely, Sir".

a think about how big that number is across all forms of trusted third parties.

2000/10s: Mutual Distributed Ledgers

MDL technology securely stores transaction records in multiple locations with no central ownership. MDLs allow groups of people to validate, record, and track transactions across a network of decentralised computer systems with varying degrees of control of the ledger. Everyone shares the ledger. 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. MDLs are not technically new – concurrent and distributed databases have been a research area since at least the 1970s. Z/Yen built its first one in 1995.

Historically, distributed ledgers have suffered from two perceived disadvantages; insecurity and complexity. These two perceptions are changing rapidly due to the growing use of blockchain technology, the MDL of choice for cryptocurrencies. Cryptocurrencies need to:

- **validate** – have a trust model for timestamping new transactions by members of the community;
- **safeguard** – have a set of rules for sharing data of guaranteed accuracy;
- **preserve** – have a common history of transactions.

If faith in the technology's integrity continues to grow, then MDLs might substitute for two roles of a trusted third party, preventing duplicate transactions and providing a verifiable public record of all transactions. Trust moves from the third-party to the technology. Emerging techniques, such as, smart contracts and decentralised autonomous organisations, might in future also permit MDLs to act as automated agents.

A cryptocurrency like bitcoin is an MDL with 'mining on top'. The mining substitutes for trust: 'proof of work' is simply proof that you have a warehouse of expensive computers working, and the proof is the output of their calculations! Cryptocurrency blockchains do not require a central authority or trusted third party to coordinate interactions, validate transactions or oversee behaviour.

However, when the virtual currency is going to be exchanged for real world assets, we come back to needing trusted third parties to trade ships or houses or automobiles for virtual currency. A big consequence may be that the first role of a trusted third party, validating an asset and identifying community members, becomes the most important. This is why MDLs may challenge the structure of financial services, but financial services are here to stay.

Boring ledgers meet smart contracts

MDLs and blockchain architecture are essentially protocols which can work as well as hub-and-spoke for getting things done, but without the liability of a trusted third party in the centre which might choose to exploit the natural monopoly. Even with smaller trusted third parties, MDLs have some magic properties, the same agreed data on all nodes, 'distributed consensus', rather than passing data around through messages.

In the future, smart contracts can store promises to pay and promises to deliver without having a middleman or exposing people to the risk of fraud. The same logic which secured 'currency' in bitcoin can be used to secure little pieces of detached business logic. Smart contracts may automatically move funds in accordance with instructions given long ago, like a will or a futures contract. For pure digital assets there is no 'counterparty risk' because the value to be transferred can be locked into the contract when it is created, and released automatically when the conditions and terms are met: if the contract is clear, then fraud is impossible, because the program actually has real control of the assets involved rather than requiring trustworthy middle-men like ATM machines or car rental agents. Of course, such structures challenge some of our current thinking on liquidity.

Long Finance has a Zen-style *koan*, "if you have trust I shall give you trust; if you have no trust I shall take it away". Cryptocurrencies and MDLs are gaining more and more trust. Trust in contractual relationships mediated by machines sounds like science fiction, but the financial sector has profitably adapted to the ATM machine, VISA, SWIFT, Big Bang, HFT and many other innovations. New ledger technology will enable new kinds of businesses, as reducing the cost of trust and fixing problems allows new kinds of enterprises to be profitable. The speed of adoption of new technology sorts winners from losers. But make no mistake: the core generation of value has not changed, banks are trusted third parties. The implication though is that much more will be spent on identity, such as Anti-Money-Laundering/Know-Your-Customer backed by indemnity, and asset validation, than transaction fees.

A US political T-shirt about terrorists and religion inspires a closing thought: "It's not that all cheats are trusted third parties; it's that all trusted third parties are tempted to cheat." MDLs move some of that trust into technology. And as costs and barriers to trusted third parties fall, expect demand and supply to increase. ***BT***

About the authors

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.

Vinay Gupta is an architect with Consensys Systems and the Ethereum Foundation.