BLOCKCHAIN'S BIG DEAL

The technology behind Bitcoin is gearing up to build a new set of foundations for business.
By **Danny Bradbury**

OVER THE SUMMER four of the world's biggest banks decided they wanted to harness a technology that was developed to go around not just themselves but also the central banks that control the money supply. Bitcoin distributed the business of creating money around the internet, using computer algorithms to ensure that payments make their way securely from buyer to seller. UBS and its partners aim to use similar technology to the blockchain routines that underpin Bitcoin to speed up the settlement systems used to trade stocks and other financial instruments.

Digital money is only the start. As blockchain technology provides a way for multiple participants to keep track of who spent money without having to trust each other directly, a number of organisations see it as a way of supporting other systems where trust is key but difficult to enforce.

The distributed design of the blockchain ensures no single point of failure and/or control. The blockchain cannot be controlled or subverted by a single party. It acts like a vast distributed ledger, with thousands of people able to check each other's numbers to avoid fraud.

That is a pretty powerful concept. It was only a matter of time before people saw an opportunity to use those underlying qualities and use them for other applications. One of the biggest breakthroughs was the idea that instead of just recording value, a distributed ledger could begin running programs, too. The first result outside digital money is the smart contract.

Get smart

Smart contracts are executable programs, but instead of running on one computer, they run on multiple computers in a blockchain. They enable all participants to run the same code and verify each other's results. If the blockchain was a distributed ledger, smart contracts turn it into a distributed computer.

GETTY IMAGES. THINKSTOCK. IMAGE SOURCE

Running on a blockchain gives it some unique properties, says Vitalik Buterin, founder of Ethereum. "It's a piece of code that can autonomously receive payments, transfer property and resolve conflicts between signing parties."

Ethereum is the most popular example so far of a smart contract-enabled blockchain. Launched in early 2014, it put smart contracts at its core. Think of a smart contract as a computerised agreement between multiple parties that doesn't need a lawyer to oversee it.

"Smart contracts buy you the chance to figure out what you want and get it done at a low cost," says Vinay Gupta, a software developer who was closely involved with Ethereum and now runs a venture capital fund focusing on decentralised startups.

Gupta uses the example of multiple owners of a company, one of whom wants to slowly divest their shares by 0.5 per cent every year. Perhaps they want to sell that equity using the average of the share price in the preceding year.

"Something like that is pretty easy to describe in code. It's five or ten lines. If you took it to a lawyer, it would cost you perhaps 25 grand," he says. The contract could also make the calculations, execute the yearly transfer and keep the ownership records automatically.

Sectors ranging from finance to supply-chain management are looking at smart contracts and distributed ledgers as a means of making transactions more resilient. Eris Industries offers a software platform that lets financial services companies create their own blockchains, complete with smart contracts. CEO Casey Kuhlman sees smart contract-enabled blockchains as the third generation of business-automation software.

The first generation saw large, expensive software packages from the likes of Oracle and SAP that would handle business processes in a heavy, complex way, he argues. In the second generation, we saw software-as-a-service (SaaS) companies offer similar capabilities online, for smaller companies who could not afford the heavy stuff.

"Neither of those generations of process automation tooling focused on the relationships part," Kuhlman argues. Companies deal independently and directly with each other all the time, and it makes sense to have a distributed technology that lets them form those relationships directly rather than paying – and trusting – an intermediary to handle the transactions.

Streamlined business

There are few business applications that cannot be handled in the traditional way. But blockchains enable companies to streamline direct transactions with each other. The more complex these interactions become, the better the blockchain is at handling them. The finance community has become interested in wider applications of the >

Manufacturers could keep lines running efficiently by using blockhain-supported contracts to switch between distributors automatically based on price and availability

< blockchain. Their whole business revolves around the exchange of value. The idea of a digital currency for settling stock trades is just the beginning. Historically, banks have exchanged messages informing each other of financial trades, but have had to maintain details of them in their own ledgers.

One historical problem is that banks cannot all be sure that they have the same understanding of a deal, and one bank can't be sure that the other will pay up as agreed. So they have to work with clearing houses to reconcile those deals, confirming that the trades went through. This clearing and settlements process typically takes days to complete.

One proposed option is for all banks to agree on the same shared database. There are problems with that though, points out Tim Swanson, author of several books on cryptocurrencies and also director of market research at R3, a firm that works with dozens of banks to develop distributed ledger technology specifically for finance.

"Who would control that database would become a very touchy thing," he says. "There is no vendor that provides a database that all our members would use to build applications that they would like, as of right now. One way to solve it is through a shared-ledger system."

His use of the term 'shared ledger' is significant. Financial companies often avoid the term 'blockchain', because financial institutions have different requirements of these shared, distributed ledgers from those of bitcoin traders.

Bitcoin survives on complete transparency in which everyone participates, and where everyone can see information about all of the transactions. Conversely, financial institutions typically do not want this kind of information circulating on a public blockchain and may be required by regulators not to share it. Instead, they use distributed ledgers in which only qualified parties are able to transact. This is often called a 'permissioned' distributed ledger.

> 'There is no vendor providing a database that all our members would use to build applications that they would like, as of right now.'
> **Tim Swanson, R3**

These ledgers are often different from public blockchains in other ways. They frequently don't use vast amounts of computing power for their proof of work, because they do not have to deal with tens of thousands of participants that do not trust one another.

Financial shared ledgers often also control who gets to participate, and who sees which information according to rules set by the community and the regulator. "What is not tenable for regulated financial institutions is the ability for anyone beyond those participating in a transaction to be able to also see that transaction," Swanson says. "They call that controlled transparency."

Post-settlement trade is just one use case that banks are exploring for distributed ledgers. Others include managing complex financial instruments like derivatives, or syndicated loans. Last year, Nasdaq launched Linq, a blockchain-based service to issue and manage pre-IPO shares in companies. This year, it launched a broader blockchain-based service to more than a hundred market operator clients.

As companies awaken to the possibilities of distributed ledgers, other use cases are emerging. One of them lies in insurance, Kuhlman says. Companies can use smart contracts to manage the premiums they pay more effectively.

Moving targets

Inventory within logistics companies changes constantly, which creates problems with insurance contracts, he warns. "Sometimes you're overinsured, and other times you're underinsured for what you have in stock at any point in time."

A smart contract may link to an RFID tagging system that automatically registers stock in a warehouse, giving it constantly updated inventory information for that logistics company. "Once you have that, insurance companies can participate in that blockchain ecosystem and offer insurance services that reflect what you have in stock at any one time along with a calculation of the premium," Kuhlman says.

Clients win because they could adjust their policy payments to save money without >

Blockchain-based insurance can reflect changing inventory – whether in the factory or in transit – in real time

< having to give the insurance company intrusive access to their back-end computers. The insurance company wins because it gets to verify its clients' inventory levels without having to build and maintain its own back-end system.

Deloitte is one of several companies experimenting with the technology and has various proof of concepts. Its global financial services blockchain leader Eric Piscini says that supply-chain management represents low-hanging fruit: "Any time you have a supply chain, you can apply [the technology] to track assets."

One proof of concept Deloitte is working on serves a client that hires out highly specialised, very expensive tools to customers internationally. Instead of arranging for the transport and tracking of those tools itself, it can have customers send the tools to each other, and use the blockchain application to track their whereabouts, he explains.

"Do I, the owner of the tool, want to be part of the process of moving the tool, or do I want to let them do that peer-to-peer and then just know where the tool is?" he asks.

Obstacles

Although the efficiencies sound attractive there are speed bumps to navigate. The industry hit one in June, in the form of the hack on the Decentralised Autonomous Organisation (DAO). Built on top of the Ethererum blockchain, DAO was a company with ambitious plans for decentralised technology that was supposed to be governed entirely using smart contracts.

The DAO was originally conceived to support Slock.it, a start-up which came up with the idea of physical locks, 'Slocks', that could be unlocked by Ethereum smart contracts. A Slock owner might use the lock to secure a bike that they owned. Someone could rent the bike from them by making a payment to a smart contract online. The smart contract would authenticate that renter.

All of this would be done directly between the renter and the owner on the Ethereum blockchain. There would be no middle man – a large company like AirBnB or Uber – to control the deals and take a cut. Instead, Slock.it's profit would come from a payment made to it by the DAO.

Slock.it proposed the DAO as an online virtual company in which people could take a stake by purchasing online digital tokens. These stakeholders could use their tokens to interact with smart contracts, electronically voting on how the DAO spent its money. Slock.it hoped that the DAO would vote to take it on as a contractor, using some of the money from the token sale to fund its project.

DAO participants paid for their tokens in Ether, which is the cryptocurrency supporting the Ethereum blockchain, and which has a variable conversion rate to the dollar. In a process that drove up the price of Ethereum's cryptocurrency, the DAO accumulated $150m of Ether. Then, an attacker spotted a bug in a smart contract governing the DAO, and used it to extract tens of millions of dollars-worth of Ether into their own DAO.

The DAO's loosely-coupled group of volunteer organisers rushed to fix the problem, patching the code, but the money had already been taken. To stop the attacker using it, they worked with Ethereum to fork its blockchain. A fork effectively rewrites history by getting users of a blockchain to start using a new version of the ledger rather than the old one, thus enabling them to reclaim the lost Ether. Some users ignored that fork, meaning that there are now two Ethereum blockchains – the new one, and 'Ethereum Classic'. In short, it was a disaster. What lessons did we learn?

"It taught us that making complex applications with absolutely zero bugs is hard! And in my opinion it also taught us that security will inherently be an incremental process," says Buterin. "Right now, I think we are going to see developers build things that are as simple as possible, and only get comfortable creeping up the complexity."

Blockchain tools and the techniques need work, says Sergio Demian Lerner. He is chief scientist at RSK Labs, which is building Rootstock, an open-source smart contract platform designed to run atop the bitcoin blockchain.

"Some elements in the smart-contract ecosystem are immature. Training, education, tools, compilers and standards need to improve," Lerner says. "But more importantly, a complex system cannot be centrally created, deployed untested and then become instantly decentralised. These type of systems require progressive decentralisation."

As the nascent industry thrashes out all of these issues, there are others looming. Interoperability is becoming a discussion topic, both for blockchains and smart contracts. The Linux Foundation has taken code donated by IBM and others to form Hyperledger, an open-source blockchain implementation that it hopes will serve as a kind of vanilla implementation that others can then build on, much as it does with the Linux Kernel.

On the smart contract side, the Chamber of Digital Commerce, which is a trade association for the blockchain industry, has formed the Smart Contracts Alliance. It hopes to work on interoperability standards for this distributed code. Microsoft, too, has formed a working group, codenamed 'Kinakuta', to exchange best practices on smart contracts and to work on improving security.

But before it gets too far down that road, the blockchain community has to get people using the technology in anger. That will initially happen in the rarefied circles of the financial community, and then in areas of the supply chain.

When it has proved its mettle there, it may begin spreading to other sectors that require distributed resilience, peer-to-peer relationships, and the transfer of value – assuming there are no more DAO disasters. •