Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world


Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Computer Fraud & Security*

Mention the word 'blockchain' to most people and, assuming that they've heard of it at all, they will most likely associate it with Bitcoin, or perhaps another crypto-currency. As a decentralised, cryptographically authenticated record of transactions, the blockchain is the key concept that makes Bitcoin feasible. Yet, as Patrick Hubbard, technical product marketing director at SolarWinds, explains in this interview, the same concept has applications far beyond the contentious world of alternative currencies – in fact, far beyond finance altogether.

"It's a bit unfortunate that it is so tightly bound with Bitcoin and financial services," says Hubbard. "Once upon a time there was a reason for that. It was still new. But we're years into it at this point and its value really lies outside of financial services."

According to Hubbard: "If you think of it as a mechanism for assuring things such as assets and other things that are valuable, then it applies to just about everything." Financial transactions, say, or credit history are arguably just the most obvious applications. But there are plenty of other activities in which the assurance of authenticity is important because these things have value and these are all candidates for assuring with blockchain.

This was underlined recently at a conference at the MIT Media Lab. The 'Business of Blockchain' event emphasised how the technology has gained respectability and is finding a home in corporate applications.[1] The trading of carbon credits, the securing of health records and the registering of business contracts are just some of the uses that are being trialled.[2]

The fact that blockchain has achieved mainstream acceptance is also underlined by the fact that the technology is now available as part of the Amazon Web Services (AWS) platform, having been announced at the AWS re:Invent 2016 conference.[3] In its launch presentation, Amazon cited healthcare data, confidential information sharing, smart contracts and corporate governance as potential applications, alongside the usual financial solutions.

"It's a bit unfortunate that it is so tightly bound with Bitcoin and financial services. Once upon a time there was a reason for that. But its value really lies outside of financial services"

In April 2017, IBM announced a partnership with Sichuan Hejia to promote the Yijian Blockchain Technology Application System for pharmaceutical procurement applications.[4] According to the firms: "Small and medium-sized pharmaceutical retailers in China often find it difficult to raise funds as a result of an underdeveloped credit system and a lack of established credit evaluation and risk control. For example, it could take pharmaceutical retailers 60~90 days to recover payment after delivering medicines to hospitals. Without sound credit records and collateral to meet financing standards, these retailers often find it difficult to get loans from traditional financial institutions. Working with IBM, Hejia has established a blockchain-based business network among these supply chain participants. By tracking drugs through the supply chain and encrypting trading records, the transparency of the blockchain can help establish the authenticity of the transaction. In turn, this may help lower the credit risk profiled by financing institutions, which should allow the payment period to be shortened, possibly to the first or next trading day. Overall, the platform is designed to help to reduce the turnover time of funds on both sides of the supply chain and allow banks to be more informed and grant access to funding for small and medium pharmaceutical retailers."

Many of these solutions are being built on top of Hyperledger, an open source project hosted by the Linux Foundation.[5] This offers a number of technologies aimed at a diverse range of industries – although currently, financial services and healthcare are the main sectors that have been targeted, with supply chain solutions promised soon.

Chain of trust

To understand why blockchain technology is attracting so much attention,

Patrick Hubbard is 'head geek' and technical product marketing director at SolarWinds. He has over 20 years of IT experience spanning network management, datacentres, storage networks, VoIP, virtualisation and more. Hubbard's initial interest in technology began with writing assembly language on the Apple II, followed by a half-decade of technogenesis in skunkworks IT at American Airlines. Since then, Hubbard's career has involved product management and strategy, technical evangelism, sales engineering and software development. Since joining SolarWinds in 2007, Hubbard has developed SolarWinds' online demo platform and launched the Head Geek programme.

Hubbard gives the example of gems. Identifying and registering gems such as diamonds is a crucial process in the fight against theft and fraud. Several solutions already exist: for example, Gemprint creates a digital fingerprint based on the characteristics of each gemstone and a serial number is laser-etched on to the stone. That makes it possible for dealers to check serial numbers against a central database or to recreate the fingerprint using the same methods and check that.

"But that's also an example of the classic challenge of assuring assets, which is that the long chain of custody is typically done with online systems," says Hubbard. These online systems need to record data that tracks the whole history of each gem going back to the first time it was registered. The assurance that people are seeking is provided only if those records are complete and trustworthy.

"It means that the system has to have records that go way, way back and every time you want to validate and reassure yourself that an asset is what it purports to be, you have to run queries against all the data you have and make a probable guess. This is based on a lot of information and an overlay trust-based security system that you are looking at coherent records," says Hubbard.

Ultimately, however, few people are going to care about that long history. The only thing they actually want to know is, is this gemstone what it purports to be? Every entry in a blockchain is, in effect, authenticated by the one before it because of the reliable chain of cryptographic signing. And so all previous events in the chain can be taken for granted.

"I don't need access to all of that information, to the deep history," says Hubbard, "so the cost of providing assurance using a ledger is a lot lower than if you had to have all these online systems available for every potential transaction somebody might want to complete, against all of the assets that you have in your database."

Ledger in the sky

One of the problems of a centralised database, as in the gemstone example, is that someone has to be in charge of it, acting as a trusted authority.

"The trust of that database is only as good as the trust of its custodians," explains Hubbard. "They may, in certain circumstances – such as financial services – implement something like chain signing, where they use cryptography to show the history elements as a part of the records. But it's not standardised – it's particular to that database. And again I have to trust that the owner of the database is actually maintaining that system."

With blockchain, you have a ledger that's shared by all and is accessible to all. Hubbard points to the way that the likes of Microsoft and IBM are now offering blockchain as a cloud-based service.

What is a blockchain?

In essence, a blockchain is a text file acting as a public ledger recording events such as transactions. Anyone can hold a copy and anyone can read the blockchain and write to it.

While it sounds like this should be a situation ripe for fraud, with people simply inventing or deleting events, in practice this is prevented through the use of cryptographic signatures. These make it impossible – or at least overwhelmingly difficult – to alter or forge events recorded in the blockchain, thus providing assurance that what is presented in the ledger is genuine. Each recorded block includes data about the previous block, which is then cryptographically hashed along with information about the current transaction. This creates a linked chain where the authenticity of every item depends on and is verified by those that preceded it.

The blockchain file is shared among all those who want to use it and one of the arguments of blockchain is that it is open to scrutiny. However, this also means that – in the case of Bitcoin, for example – the file itself becomes ever larger. The task of carrying out the work to sign transactions and synchronise them with the public ledger also introduces delays. Currently, it can take up to an hour for a Bitcoin transaction to be registered.

There have been attacks on the technology as implemented in crypto-currencies such as Bitcoin. However, commercial implementations of blockchain technology claim to have addressed most of the security issues.

For more information, go to: https://en.wikipedia.org/wiki/Blockchain.

"I don't have to worry about it – it's just available to me," he says. The task of managing a large application stack is abstracted away, he says: "As a business, it lets me really focus on how I am assuring assets."

Assurance as a service

There's a nice distinction here in terms of who really benefits most from the blockchain approach.

"The cost of providing assurance using a ledger is a lot lower than it is if you have to have all these online systems available for every potential transaction that somebody might want to complete"

"It is most valuable for businesses that focus on providing assurance as a service, rather than producing things that are assured," says Hubbard. To clarify that point, he gives the example of pharmaceutical companies that spend billions of dollars getting candidate drugs to market.

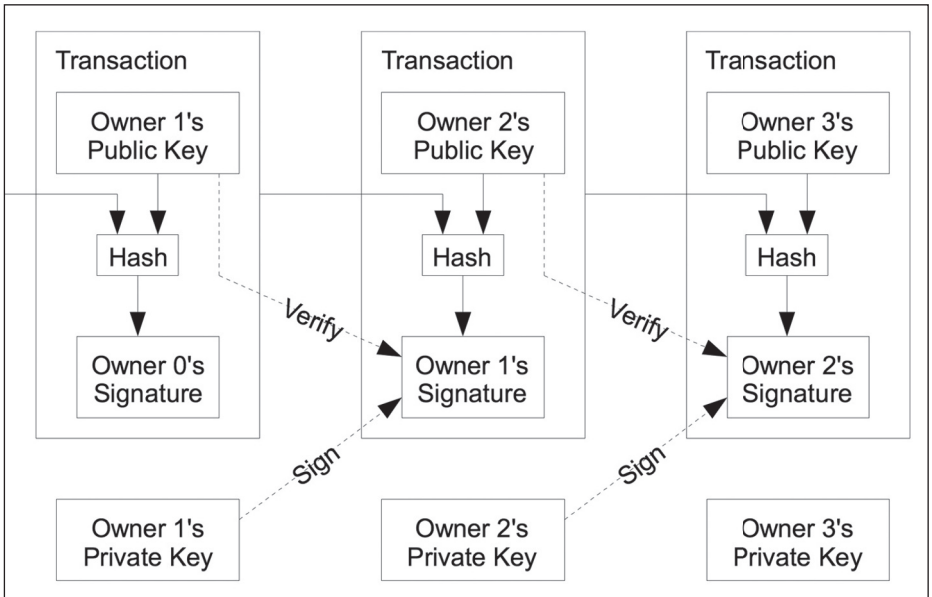
"A big part of that is the field trial," he explains. "They have healthcare providers that distribute candidate medications in the field, but there's a lot of variation in the quality of both the facilities where it's being delivered and, of course, time and the candidates that are a part of the pool."

This leads to large amounts of data being collected and it's important to show that this data hasn't been compromised and is coherent. This is in a context where the trials may take place in geographically dispersed locations and under widely varying circumstances, including emergency medical procedures. Chronology and context become very important and these are the added dimensions that blockchain easily and efficiently provides – over and above what you might achieve, for example, with document signing using public key encryption.

Hubbard underlines this with another example, this time revolving around patent law. A key issue here is when an idea was first expressed and recorded. If someone else comes along years later and claims to have had the idea first, you need a means by which you can establish a strict timeline. Depending on timestamps on individual documents doesn't achieve that because the clocks on the various systems used to create and store those documents may not be synchronised and timestamps are prone to fakery.

"If you have publicly available mechanisms to sign anything, then chronology doesn't exactly go away as a concern, but something that is normally very expensive becomes a lot easier," says Hubbard. "Think of songwriters – you have these artists that are now publishing their music directly to their listeners over the Internet. They're not using the traditional mechanisms of recording companies. It's nice to be able to sign a piece of art as your own."

One of the reasons for working with a traditional music company was the intellectual property protection it provided, he adds. Now, with 'blockchain as a service' offerings, musicians can explore a wider range of publishing routes, needing only to pay a small transactional fee to benefit from IP protection.



The chain of transactions as described by 'Satoshi Nakamoto' in his original paper on Bitcoin.

In the air

One sector that Hubbard believes could really benefit from the application of blockchain technology is the aviation industry, where Hubbard himself worked for many years.

"When you have enterprises, governments and other entities that look at blockchain as an enabling technology, they apply the standards of application performance measurement, the understanding of the delivery stack – all of the other things that we in business expect and rely on to be able to deliver end services to people"

"Airlines have, in some cases, billions of parts that they have to track and pretty much everything on the aircraft has a chain of custody," he explains. "There's a lot of government regulation. And then, of course, they really do care about their passengers and they like to make sure that they're safe."

These parts can be in a variety of places – on the aircraft, in a bin in a warehouse or in a workshop being

overhauled. And many of them will stay with the airlines for decades, during which time they must be carefully tracked. Typically, that involves large databases and huge amounts of paperwork.

"To assure that a part was not only what it purported to be, but that it had never left the certifiable custody of the airline, or had maybe gone to a third party and come back and it's still the same part, you had to look at the entire history of that part, look at the part itself and then somebody would vouch for it," he says. "So, again, you get back into that trust relationship, that trust authority."

The costs of doing this are bad enough, Hubbard says, but when you add in the risk of massive fines if and when it fails, the financial implications are huge. And it's only getting more complicated as many airlines move their maintenance operations offshore to cut costs. You can see why: Hubbard explains that the brake packs on an Airbus A320 cost around half-a-million euros each to maintain. A team of mechanics is required to remove the brake which is then sent to a repair shop. Thousands of parts are involved, each with a unique ID. When it's reassembled, it's sent back to the airline to be installed on another aircraft.

"Think about how many signatures are involved in that," says Hubbard. Then there's the certification of all the engineers and mechanics involved – another set of records. "Blockchain gets particularly interesting when you look at multiple assets that are interacting, each of which needs to be assured. If you think about the complexity of not just maintaining a part but a whole series of parts for an aircraft … well, that is ripe for blockchain technology."

Aviation is a heavily regulated industry. Is this the kind of environment where the blockchain could really show its worth by providing records whose authenticity can be highly trusted?

"Any time there's regulation, there's a lot of cost associated with that, or at least risk to the business," says Hubbard. "I think enterprises are always looking for tools and technology that can help diminish that risk. Properly applied, blockchain can be one of those enabling technologies."

But it's really a lot bigger than that, he says, because there are so many things that need to be assured and there is so much cost with maintaining digital records. "When you look at huge digital transformation projects that a lot of companies are going through, in many ways it's to get visibility to their data," he says. "And when you look at big data, at machine learning, at a lot of BI [business intelligence] – all of these technologies are trying to make sense out of the data that enterprises have. If you look at what's driving that, there are many things that are transactional, that they'd like to be able to innovate around. If you can simplify the process of guaranteeing assurance about things, that a thing is what it purports to be and do it without the need to go back and look at all the details that have ever been recorded about that object, it means a lower cost of service and the ability to quickly deliver great user experiences."

Getting it to work

Getting a blockchain solution to work for your organisation isn't necessarily a simple matter, however.

"You have to make sure that the quality of experience, all the way down to the service delivery, is good, or else you won't get the result you want, especially with consumer-focused or mobile users"

"You have to make sure that you're not dramatically increasing complexity," says Hubbard. "If you have the expertise to either build your own distributed ledger blockchain service in-house, or you're going to use one that's provided by a cloud provider and you're not worried about it, then you can focus on the business advantage of it. But if you're worried about the application itself, or about the containers it runs on, the abstraction layer inside of physical servers that it's operating on and storage and all of the other considerations of actually delivering the service to the end user, then well maybe it's not for you."

The end user performance is a critical issue and this is something that is sometimes overlooked.

It's okay if the query for a fat client comes back in half a second, says Hubbard. But because of the shared nature of the blockchain, where it's often distributed to where users are carrying out transactions, it's crucial to maintain performance in terms of recording the transactions, because those records provide the assurances you're seeking. "You have to make sure that the quality of experience, all the way down to the service delivery, is good, or else you won't get the result you want, especially with consumer-focused or mobile users," he says.

Securing the solution

While the blockchain offers assurances about the authenticity of transactions, it's not a security solution. That's something that tends to be overlooked and there have been warnings about the sudden popularity of the blockchain approach blinding developers to the need to secure the applications and infrastructure that surround the blockchain.[6] But Hubbard believes the technology could offer some benefits there, too.

"In some ways blockchain is a little easier to secure," he says. "One, it's easy to identify that it's been manipulated; and two, because you have multiple copies it's easier to reconcile a change. So if

you discover that one of the ledgers has been compromised, you have multiple copies to actually roll it back to."

Why now?

The blockchain has been around for some time. The paper by the pseudonymous 'Satoshi Nakamoto' that detailed the Bitcoin concept dates back to 2008.[7] And even that built on previous concepts, notably work by Stuart Haber and W Scott Stornetta in 1991 and further developments in 1996 by Ross Anderson and 1998 by Bruce Schneier and John Kelsey. So why the sudden rush of interest now?

"Blockchain gets particularly interesting when you look at multiple assets that are interacting, each of which need to be assured. If you think about the complexity of not just maintaining a part but a whole series of parts for an aircraft … well, that is ripe for blockchain technology"

"I think the biggest barrier is that it has been sort of do-it-yourself up until this point," says Hubbard. Given that much of the focus with blockchain was on crypto-currencies, it didn't attract the kind of effort and support that more widely applicable open-source projects have enjoyed. As more projects have appeared, including frameworks that make it easier to deploy, things have started to snowball.

"Now that people are thinking of it as something that can be consumed as a service, says Hubbard, "it's much easier for enterprises to think of it as a facility to allow innovation as opposed to a headache and one more complex thing that they would have to manage with IT."

We might have got to this point sooner if it hadn't been for the Bitcoin connection. When asked if the radical, counter-culture image of Bitcoin had tainted the image of blockchain technology, Hubbard admits: "A little bit."

He adds: "At AWS re:Invent last year, I sat in on a couple of sessions on blockchain and the audience was really interesting. Half of the audience were in khakis or really nice jeans and a decent dress shirt, mostly financial services and enterprise technology managers who were trying to figure out how they could actually use blockchain in their environments. And then the other half of the room were late twenties to early thirties guys, with a bit of a tattoo sticking out from under the shirt and a baseball cap with a sticker on it. There is still a bit of association that somehow blockchain is this amazing stone and if you do something great to it, it will generate cash. But I think the enterprise is beginning to get past that as they see examples of how blockchain can actually be applied in the real world. That makes them realise that it's a technology just like anything else. When they think about it as a utility – and it's essentially a special type of assurance database – that helps demystify it a bit."

The technology is also overcoming a reputation for technical difficulties. As Bitcoin is based on a single ledger file that is now gigabytes long and getting ever-longer, it's hitting performance issues. But Hubbard explains that these technical challenges are easily solved.

"When you look at what Microsoft is doing with Azure and IBM with Bluemix, that is the way we can move past a lot of the limitations that we see with Bitcoin," he says. "There are many things about Bitcoin that are not exactly enterprise-class. And when you have enterprises, governments and other entities that look at blockchain as an enabling technology, they apply the standards of application performance measurement, the understanding of the delivery stack, service level agreements – all of the other things that we in business expect and rely on to be able to deliver end services to people."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Computer Fraud & Security *and its sister publication* Network Security. *He also blogs and podcasts on infosecurity issues at Contrarisk.com.*

References

1. 'Business of Blockchain'. Technology Review. Accessed April 2017. http://events.technologyreview.com/presents/business-of-blockchain/2017/.
2. Knight, Will. 'The technology behind Bitcoin is shaking up much more than money'. Technology Review, 18 Apr 2017. Accessed Apr 2017. www.technologyreview.com/s/604148/the-technology-behind-bitcoin-is-shaking-up-much-more-than-money/.
3. 'AWS re:Invent 2016: Blockchain on AWS: Disrupting the Norm (GPST301)'. AWS, via SlideShare, 19 Dec 2016. Accessed Apr 2017. www.slideshare.net/AmazonWebServices/aws-reinvent-2016-blockchain-on-aws-disrupting-the-norm-gpst301.
4. 'IBM and Hejia launch blockchain-based supply chain financial services platform for pharmaceutical procurement'. IBM, 11 Apr 2017. Accessed Apr 2017. https://www-03.ibm.com/press/us/en/pressrelease/52055.wss.
5. Hyperledger, home page. Accessed Apr 2017. www.hyperledger.org.
6. Kuchler, Hannah. 'Cyber-attacks raise questions about blockchain security'. FT, 12 Sep 2016. Accessed Apr 2017. www.ft.com/content/05b5efa4-7382-11e6-bf48-b372cdb1043a.
7. Nakamoto, Satoshi. 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Bitcoin.org. Accessed Apr 2017. https://bitcoin.org/bitcoin.pdf.