

Blockchain manoeuvres: applying Bitcoin's technology to banking

By [Dan Barnes](#) | Published: 14 May, 2015 |

<http://www.thebanker.com/Tech-Trading/Technology/Blockchain-manoevres-applying-Bitcoin-s-technology-to-banking>

Bitcoin's blockchain is being hailed as revolutionary. But will the likes of UBS, ING and Nasdaq, who are exploring the potential of the technology, be able to overcome the challenges that remain, not least security and regulatory issues?

Bitcoin may never fly as a currency but the blockchain – the technology behind Bitcoin – has revolutionary potential. It could transform almost every aspect of commerce and make standard internet transactions seem old fashioned.

Already there are ideas for using the blockchain to make payments faster and cheaper, to make it easier for small businesses to obtain finance and for banks to assess mortgage portfolios at the click of a mouse. Smart trade finance contracts are being worked on that are so watertight, they will never be argued over in court. Securities transactions could be settled in minutes rather than days. Audits and compliance could be done with a fraction of the resources previously used. Many aspects of business, such as wage payment, could be done instantly.

Nasdaq announced in May plans to use a blockchain system for stock issuance on its private market, citing the system's integrity, auditability, governance and transfer of ownership capabilities.

If only half these ideas come to fruition, Bitcoin's blockchain would be a catalyst for technologies that would make web 2.0 or 3.0 seem like something from the Stone Age. "[Smart contracts] are the foundation for a new generation of applications on the internet," says one tech innovator.

Best brains

Obviously there are huge challenges, security and regulatory issues among them. But many banks are putting their best brains to work on research to come up with solutions. UBS, for example, has a team based at Level 39, the tech start-up incubator in London, looking at multiple-use cases and determining how resilient blockchain constructions are. The bank is in good company – the Bank of England reportedly also has people at Level 39 working on blockchain.

INNOVALUE Management Advisors Ltd.

3 More London Riverside
London SE1 2RE, UK
www.innovalue.com

PHONE +44 203 283 43 25
E-MAIL contact@innovalue.com

DIRECTORS
Kai-Christian Claus
Andreas Habersetzer

HSBC BANK PLC HBEU
BIC: MIDLGB2105E
IBAN: GB68 MIDL 4001 0491 8146 13
SORT CODE 400104, ACCOUNT 91814313

VAT REG NO.: GB181 1212 49
REGISTERED IN ENGLAND

“Blockchain could have the potential to change the way we do business in various asset classes. It could have the potential to change identity management in personal and institutional banking,” says Oliver Bussmann, group chief information officer at UBS.

Mark Buitenhok, global head of transaction services at ING, says: “The usage is much broader than just a currency. We are focusing on everything else around it. We are taking this extremely seriously. When you talk about disruption in the banking industry, starting with payments, this is one of the most far-reaching technologies that is around.”

Model for the future

Ironically for a technology with such revolutionary potential, the Bitcoin/blockchain operating principle is best explained in terms of ancient forms of exchange. For 500 years or more, stone coins called rai, up to 3.6 metres in diameter, have been used on the Pacific island of Yap. The apparent impracticality of the currency is misleading. Ownership of a coin does not require a physical transfer of the rai stone; the owner passes ownership to a new person by word of mouth, along with the historical record of ownership. Transactions are public, as is ownership. The location of the coin, whether at the top of a mountain or the bottom of the sea, is immaterial. However, reciting the correct record of ownership will soon reveal whether the current owner is in legitimate ownership of the coin.

Bitcoin operates in just the same way. Transfer from one account to another involves no coin, simply a continuous record of transactions. This record is encoded in a block, in such a way that it can never be interfered with. The technology that underpins this model of transaction is called the blockchain, an immutable, distributed ledger system that records the transfer between accounts.

A blockchain model consists of three things: the database or ledger; the meaning given to the number of units, for example, one Bitcoin; and the transaction function that confirms a viable transfer from – in the case of Bitcoin – address A to address B.

Using Bitcoin requires the download of software to connect to the network. Likewise, if users want to mine Bitcoins – effectively process settlements – then they need to download Bitcoin mining software. This results in payment by Bitcoin and an encrypted record added to the block, which forms the ledger. Key to the success of technologies based on the blockchain is the information record the ledger creates – using this supply of information has the potential to make arduous processes much simpler.

Security issues

But is it safe? High profile thefts of Bitcoins have caused concerns about its security, but these are not related to the ledger model any more than a theft from an online bank account is related to a centralised ledger system, says Francesco Burelli, partner in the payments practice at strategic management advisory firm InnoValue.

“Similar types of breaches happen to custodians within centralised and distributed ledger ecosystems,” he says. “While the distributed ledger is very robust and cannot be tampered with, the anonymity of its transactions and the practical lack of [know your customer verification] and compliance [in Bitcoin], make it more vulnerable at custodian level.”

It is the nature of Bitcoin's anonymity, the ability of users to mask IP addresses and the ability to keep the stolen Bitcoin values in peer-to-peer transactions within the Bitcoin ecosystem for an indefinite number of transactions that makes it more vulnerable than institutional payment systems. "That makes investigations and the prosecution of criminals within the Bitcoin ecosystem way more complex than in the incumbent financial services industry," says Mr Burelli.

These challenges are not deterring tech firms and banks from exploring blockchain's possibilities. A number of firms are developing technologies that use the same mathematical cryptographic model as blockchain to work outside of Bitcoin, using custom networks to exchange everything from currency to property contracts, or in some cases even contracts that instruct further actions. The range of possible applications is enormous.

No limits

As blockchain is open source, there are no limits as to who can develop it. More than 100 firms are looking at creating blockchain models for practical business purposes. For Mr Bussmann of UBS, the next stage is the collective adoption of particular systems that are trusted enough to be used by several financial institutions.

"The potential is great, the idea of a distributed ledger that removes complexity is good; the question is how will that work from a workflow perspective, from a scalability perspective and, most importantly, can I trust the involved parties?" he says. "If the industry agrees on a certain standard, then we will see scale and volume exploding. If parties agree this is the most safe, reliable model and regulators are comfortable with it, then volume will come through."

Key to the start-ups is the concept of the contract that is exchanged. Bitcoin is really a tamperproof contract of exchange and the development of increasingly complex contracts offers a wealth of functionality to a blockchain.

Smart contracts

Fintech start-up Diacle is positioning itself to develop the first smart contract so that lawyers are able to make it more binding and link it directly with payment, which would provide a more useful service than a page of a document that could be argued over in a courtroom, which is itself an expensive process.

"With that in mind, the role of a lawyer in a commercial environment is relatively inadequate irrespective of their drafting of an agreement," says Adam Vaziri, director of Diacle. "What we are doing is using blockchain technology, software that both parties to the transaction can run. So when the person delivers the goods, the digital currency is automatically sent to the seller, so what you are creating now is an escrow service without the trust of a third party and the lawyer that is involved in not only providing you with a bit of paper but providing you with enforceability in software."

Another tech start-up Factom offers a permanent, time-stamped record of data in the blockchain to reduce the cost and complexity of conducting audits, managing records and complying with government regulations.

Paul Snow, CEO and lead developer at Factom, says: “Such technology can vastly reduce the amount of reporting that has to be done and this is the real cost savings that could occur. If you can use mathematics to replace regulation, you can vastly decrease the cost of financial transactions and greatly increase their efficiency and speed.”

Factom notes that buying mortgage businesses without being able to accurately analyse the acquired contracts has cost banks billions of dollars in fines, which could potentially have been saved if those mortgage records were easily auditable via a ledger model.

Next-generation apps

The breadth of the systems being developed is considerable. At the very open end, Ethereum is developing a system that will allow complex contracts to be exchanged that, depending upon the interaction between them, can trigger further actions via other contracts with the model secured via a distributed ledger model.

Mihai Alisie, one of Ethereum’s founders, says: “We have a blockchain that is featureless in a sense and it has embedded within it a programming language that allows people to create all sorts of things that run on top of the blockchain architecture. The building block for Ethereum is a smart contract; it is like a virtual machine or autonomous programme that is maintained by everyone in the network. Inside the contract you can specify what its purpose is. The contracts are the foundations for a new generation of applications on the internet.”

Mr Alisie sees the potential for such a system to create a decentralised, autonomous organisation, with actions such as wage payment simply requiring validation in the network.

At the narrower end, Ripple is specifically targeting payments within financial services firms. Chief executive Chris Larsen says: “The protocol really exists at the bottom of that existing payment stack. We are trying to provide a connecting tissue to all of these essentially closed-value exchange systems.”

The level of adoption for these platforms has been low so far, however, there are live cases. Germany’s Fidor Bank is already using Ripple to underpin one of its payments platforms. Fidor, which has developed its own operating system to facilitate the development of services for customers, is keen to exploit new technologies to create customer choice.

Fidor chief executive Matthias Kröner says: “Each partner has advantages and disadvantages and we want to come up with a payment configurator so the customer can send \$50 from the US to the Philippines and preselect a super traditional payment with low risk but paying approximately \$10 in commission and taking five days or a newer route that takes five seconds.”

Jerry Norton, managing director of financial services at technology provider CGI says that his firm has built a proof of concept within a bank environment between an account and a mobile wallet. “We built an adapter for the bank that talks [universal financial industry standard] ISO20022 one way and talks into the Ripple network at the other. It works, it is running transactions and we have some ideas about how to make it industrial strength.”

Many other banks, including ING, are in talks with Ripple to explore the potential of the system as an alternative to the complex and costly model for setting up a payments platform.

ING's Mr Buitenhek says: "Can we use this to replace existing technology, whether for transfers or payments or in the security space? Banks are making the choice to move to a 24/7 real-time payment service: instant payments but also instant business. Discussions of what kind of technology to use is an interesting dilemma: do you go for the brand new, not completely tested but very promising blockchain type of technology with everything in it or proven technology with databases? As the outages have shown in the UK and other countries, people don't accept downtime."

Money has memory

Nasdaq is using a blockchain-based system to enhance its ability to keep track of clients' private issuance of stock. Chief executive Robert Greifeld says: "Our initial application of Nasdaq's blockchain technology-enabled offering will modernise, streamline and secure typically cumbersome administrative functions, and will simplify the overwhelming challenges private companies face with manual ledger record-keeping."

Future applications have exciting potential, including the ability to challenge the concept that 'money has no memory', says Mr Kröner. "We have thought about the memory of money via a blockchain. That's an idea we would love to drill down into, but a little bit further down the road."

CONTACT DETAILS

Francesco Burelli: francesco.burelli@innovalue.com