BLOCKCHAIN AND ITS USE IN FINANCIAL SETTLEMENTS AND TRANSACTIONS

Daniel Broby, Chartered FCSI, director, Centre for Financial Regulation and Innovation, University of Strathclyde
daniel.broby@strath.ac.uk

Greg Paul, doctoral researcher, Strathclyde University Electrical and Electronic Engineering Department
greig.paul@strath.ac.uk

ABSTRACT

Blockchain is the technology at the core of what could become the 'fintech' transformation of capital markets. It can potentially facilitate cheaper, more efficient and secure operations. The mechanism behind it is introduced in this paper, as are its uses and suggested areas for future academic research. The paper critically reviews the promise that blockchain and distributed ledgers will speed up financial settlements and transactions. In it we recommend financial institutions evaluate the adoption of blockchain and/or adapt their existing legacy systems to allow for digital clearing over the internet.

Have you ever wondered why it takes three days to clear a cheque, why it takes a ten-minute telephone call, long account numbers and a punitive fee to transfer money abroad? None of these issues need happen, thanks to blockchain technology. This is at the core of the fintech revolution which promises a vision of seamless financial transactions over the internet. The concept is already in beta testing and billions of pounds are being invested in related applications. Some people believe it will transform financial services.

Blockchain was first described by Nakamoto (2008). It is based on a distributed computer architecture and facilitates the sending of digital instructions over the internet. In technical terms, it has what are called network nodes that execute and record digital transactions. These transactions are batched together into blocks before they are processed, hence its name. The blocks are effectively a series of written digital instructions linked together in a chain. This ensures that the contents and order of transactions can be verified. Such an instruction, for example, could contain written code to send money from Bob to Alice.

CONFUSION WITH BITCOIN

The programmed messages in blockchain are used to facilitate financial market infrastructure, payments, and settlements. There is a great deal of discussion in the media, banking circles and academia about the impact this technology will have on financial settlement and operations. A lot of this is misinformed. The concept is often confused with bitcoin, a digital currency that utilises blockchain technology. At the same time, the terminology has a habit of alienating informed discussion by practitioners. This is because financial and technical jargon do not mix well. Academics tend to focus on the engineering and cryptographic challenges. They overlook the complexities of introducing such technology alongside the legacy payment systems that dominate modern banking. This lack of clarity is hindering informed debate and has led to a slow uptake of the new technology despite its advantages

The concept of blockchain is not as complex as its execution. As explained, it consists of a series of sequenced transactions, grouped into blocks, which are then processed by a network of computers that are digitally connected. In the case of the financial transactions it handles, the transactions may be of the sort normally kept on a bank ledger. In this instance, with a double-ledger entry for each transaction. This method highlights the origin and beneficiary of a payment.

The blocks, meanwhile, are chronologically connected by a series of cryptographic hashes (Damgard, 1990). These are unique secure identifying numbers, which act as fingerprints of the data contained within the blocks. Each block contains the fingerprint of the previous block, meaning that the data in each block can be used to ensure the previous block has not been altered. This fingerprint element is what joins the blocks together, creating a chain.

These chronological blocks can hold multiple transaction records. They are distributed through the nodes of the blockchain network which are carrying out the processing (Decker & Wattenhofer, 2013). In a public blockchain network, anyone may run their own node to process and validate transactions. The blocks are verified by the cryptographic hash which cannot be easily changed or falsified (Peters et al, 2015). If there is a change to any part of the data, the hash will appear to be totally different. The sequence is illustrated in Figure 1 below.

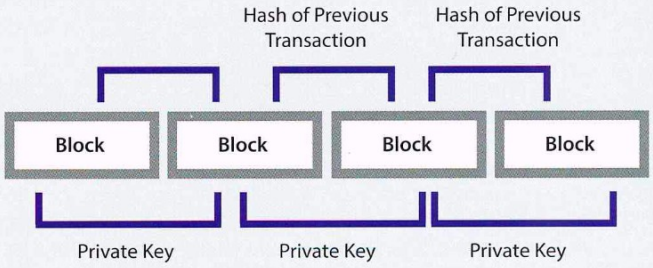

Figure 1: The mechanism of securing transactions on blockchain

The inclusion of the cryptographic hash makes fraud difficult. It is the key innovation that makes a blockchain secure. It solves the problem of the order of previous digital transactions being manipulated by a malicious party seeking to defraud others. Were someone able to alter the order of previous transactions, they could insert a transaction before a payment to another individual, draining their funds. This would result in the latter payment failing, leaving the recipient unpaid. Blockchain eliminates this so called "double spending problem", according to Hoepman (2007).

The unique hash identifiers in a blockchain will show as being different if any of the transactions within a block are modified or tampered with. Figure 2 illustrates how the hash of a block is used within the header of the next block to verify the history of events. The process of checking that transactions have not been modified is called validation. Buyya et al (2008) illustrate this works within decentralised networks, in other words over the internet. In this way, financial payments can be carried out, with transactions sent and stored on the internet using multiple online validation nodes and participants in the network. Blockchains are therefore sent to and stored on distributed ledgers. There are multiple copies of it kept by multiple parties, and any may verify the records at any time.

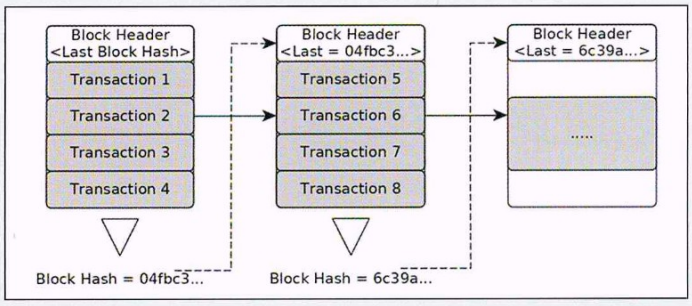

Figure 2: Illustration of the chaining of blocks, through the incorporation of the previous block hash in the next block header. This prevents alteration of previous blocks' contents, and preserves the order of blocks, and therefore transactions

The reason for the attention afforded to blockchain is that it has the potential to evolve into the next generation of the internet for financial processes. This is because it can facilitate the exchange of assets or information between various parties without the need for a trusted intermediary. Several features of blockchain technology make it particularly attractive. These include the immutability of digital records, and the resulting traceability and proof of ownership. The security and privacy of blockchains have captured the attention of financial market participants. With controlled access to distributed ledgers, financial transactions can be stored on the internet rather than simply on the server of individual banks. This makes them less dependent on legacy systems.

CRYPTOGRAPHY AT THE CORE

Security is at the core of blockchain, and as such can also be used to create digital currency. This is because the cryptographic hashes can not only be used for connecting the blocks but also for confirming the validity of blocks containing transactions. Cryptocurrencies such as bitcoin, litecoin and peercoin use this process, referred to as mining, as the basis of their security. The process of mining is used to ensure that blocks added to the ledger require a predictable amount of work to be carried out. This prevents any one party from dominating the blockchain by having a monopoly over the creation of new blocks. To reward miners, the successful creation of a new block results in the award of some new bitcoins to the miner. The limited supply and proof of work add to the 'attraction' of the use of such digitally based currencies. There are a few hundred such cryptocurrencies, called altcoins. Whether any of these will become a global success is debatable, but clearly there is potential for the world to move to a digital currency in the future, now that the technology is available.

Bitcoin was the first blockchain use in currency transactions (Nakamoto, 2008). Bitcoin, as a digital cryptocurrency, is secured by cryptography, rather than legislation, and is therefore operated independent from national or international regulation by governments or authorities, although parties participating in the network may be regulated within their own jurisdictions.

As said, cryptography is one of the core features of blockchain. The other is peer-to-peer networking, explained by Koshy et al (2014). They point out it solves the communication protocol known as the Byzantine Generals' Problem that was identified by Lamport et al (1982). This is what is termed a logical agreement problem and is based around how multiple parties can reach a consensus without any party being able to mislead the others. In the context of blockchain, the agreement relates to the transactions. Feldman and Micali (1997) demonstrated that by using this protocol, no network user can 'betray' others unless more than half of network participants take a control of the network. This is what is termed a '51% attack'. This risk is reduced through the distributed nature of the blockchain network, allowing everyone to participate.

One of the advantages of blockchain is that it enables what have become called 'Smart contracts' to be encoded within blocks, and executed automatically and impartially by software (Kosba, A. et al., 2016). Train commuters may be familiar with the basic building blocks of a smart contract, as this is similar to how their journey is recorded, or their season ticket validated, when they touch their card on the entrance sensors, as illustrated by Poon & Chau (2001). In effect, a smart contract instructs, verifies and enforces a set of contractual instructions. Koshy et al (2014) meanwhile showed that emerging smart contract systems can now allow mutually distrustful counterparties to safely transact financial settlements without a trusted intermediary.

Another advantage of blockchain usage is that it can potentially reduce operational expenses for the processing of large volumes of transactions, by bringing into effect newer and more modern processes, thereby hopefully reducing fraud. It can have a dramatic effect in reducing operational costs in financial incumbents. Traditional financial incumbents are testing and evaluating blockchain for this rather than its attraction as a decentralised structure. Either way, the technology is becoming more widespread.

In 2015 the earliest adopters of blockchain launched a consortium for blockchain technology named R3 CEV. This consortium has gained momentum and has the goal of applying such distributed ledger technologies in financial organisations. It has focused on daily transactions and the sharing of a common distributed ledger system.

The other key intiative is Ethereum. This was first described in 2013 and was officially launched on 30 July 2015. Ethereum is a platform designed to run smart contracts over a decentralised network of peers. A smart contract in the context of Ethereum is described as "an application that runs exactly as programmed without downtimes, censorship, fraud or third party interference". The Ethereum project's mission is to fully decentralise the internet. It provides a platform on top of which anyone can create a decentralised internet service secured by the blockchain. Ethereum makes it easy to launch blockchain-based applications without needing to create a new blockchain protocol.

Blockchain technology allows for a new model of consensus and validation of records/events, ensuring that all participants can reach a compatible and congruent view of previous transactions. The ability to validate transfers or transactions cryptographically provides opportunities for enhancing the security of current trading and settlement platforms. In certain circumstances, such as for high value or priority transfers or settlements, the ability to prove cryptographically that an attempt was made to initiate a transfer at a given time would assist in ensuring the correct relative ordering of settlements, or allow a party to prove the existence of a signed transaction at a certain time, such as to comply with contractual obligations or similar.

THE ROLE OF TIME-STAMPING

The legacy international settlement system is called the SWIFT network. This is not without its security and authentication issues and is becoming very dated. By moving to a model of a blockchain, where transactions are broadcast and validated by others, a more robust security model can be adopted. In that way transfers can be cryptographically verified against the bank of origin. In the event of the transaction being improperly signed, the cryptographic validation will fail, and the other banks will detect this conflict, refusing to honour the transaction, and alerting the issuing bank as to the potential for a compromise of their systems.

One of the challenges of blockchain for banks and financial institutions is that it does not inherently provide accurate time-stamps of transactions. While the blockchain construct gives an immutable history, and verifiable order of events, individual events themselves can only be validated as existing at or after a given point; inclusion within blocks is not guaranteed, and if two rival blocks were produced at the same time, this will result in a clash causing one block to appear before the other. The transactions from the second block will still be included in the network, but may appear at a time later than would otherwise be indicated from their position within the chain.

More generally, within a blockchain, the content need not only be financial transactions of a currency-derived commodity; assets or other property could have verifiable and accountable ownership transfers

carried out within a blockchain. For example, house sales could be carried out on a form of blockchain, allowing government to ensure that all transfers are properly registered and thus that taxes are correctly paid. In addition, such a construct could facilitate interesting future opportunities to make doing business online easier. With such a registry, a user could, in theory, cryptographically prove ownership of their own home within seconds, allowing a lender to offer them a secured loan immediately. Tenancies could be agreed digitally, with a blockchain used to identify 'rogue' unregistered landlords, since tenants would lodge their contract and deposit via the blockchain. Unauthorised subletting could be similarly detected.

One fallacy about blockchain comes from the perception that exposing transaction data over the internet is insecure. Blockchains need not be fully exposed to the public. An entirely private blockchain is possible. It could be held between a group of mutually trusting entities such as banks. Alternatively, a hybrid blockchain is possible, whereby anyone may read the blockchain, but only authorised members may append to it, perhaps for transfers of restricted assets. The other fallacy is that it is insecure because unknown and faceless programmers are developing it. This overlooks the power of group software development, which historically has proved superior to single code production, and the ability for anyone to inspect open source code for quality and correctness.

Critically, one should also point to both the large data demands of blockchain, as well as the amount of processing power required to create cryptographic hashes and validate the transactions. These two areas, blockchains biggest weaknesses, require further academic and practical investigation.

In conclusion, the security, reliability and effectiveness of blockchain will result in more efficient and cheaper financial transactions. We recommend that financial institutions evaluate its adoption. If this happens, blockchain has the potential to significantly transform banking through new models for the processing of transactions in a distributed manner, rather than the current more centralised approach.

BIBLIOGRAPHY

Buyya, R., Yeo, C. & Venugopal, S., 2008. *Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities*. In High Performance Computing and Communications. s.l., HPCC'08.

Damgard, I., 1990. A design principle for hash functions. *Advances in Cryptology*, Volume CRYPTO89 Proceedings. Springer, pp. 416–427.

Decker, C. & Wattenhofer, R., 2013. *Information propagation in the bitcoin network*. s.l., IIEEE P2P 2013 Proceedings (pp. 1-10).

Feldman, P. and Micali, S., 1997. 'An optimal probabilistic protocol for synchronous Byzantine agreement'. *SIAM Journal on Computing*, 26(4), pp.873-933.

Hoepman, J., 2007. *Distributed double spending prevention*. In International Workshop on Security Protocols, April ed. (pp. 152-165): Springer Berlin Heidelberg.

Kosba, A. et al., 2016. The blockchain model of cryptography and privacy-preserving smart contracts. *Security and Privacy (SP)*, IEEE.(May), pp. IEEE Symposium on (pp. 839-858).

Koshy, P., Koshy, D. & McDaniel, P., 2014. *An analysis of anonymity in bitcoin using p2p network traffic*. In International Conference on Financial Cryptography and Data Security. March ed. Berlin Heidelberg: Springer.

Lamport, L., Shostak, R. & Pease, M., 1982. *The Byzantine Generals' Problem*. ACM, s.n.

Nakamoto, S., 2008. *Bitcoin: a peer-to-peer electronic cash system*, s.l.: Private distribution.

Peters, G., Panayi, Y. and Chapelle, A., 2015. *Trends in crypto-currencies and blockchain technologies: a monetary theory and regulation perspective*. Working paper.

Poon, S. & Chau, P., 2001. Octopus: the growing e-payment system in Hong Kong. *Electronic markets*.

DANIEL BROBY, CHARTERED FCSI

Daniel Broby, Chartered FCSI has enjoyed a successful career in both academia and practice, and is one of the Institute's longest-standing members. His research into financial benchmarks and markets has had important practical applications. Prior to his academic career, he worked in a number of senior executive positions in the fund management industry. These include chief executive, chief investment officer, and chief portfolio manager. Daniel's practical skill set includes financial modelling, accounting analytics, investment, index and portfolio construction.

He is now director of the Centre for Financial Regulation and Innovation at the University of Strathclyde, which in November was named Business School of the Year at the Times Higher Education awards. He is a regular host to CISI events.

GREG PAUL

Greg Paul is a doctoral researcher at Strathclyde University Electrical and Electronic Engineering Department . He is a recipient of the EPSRC Doctoral Training grant and has written numerous peer reviewed papers on blockchain and mobile/cyber security protocols. He is a regular speaker at Blockchain events and international conferences. His experience covers a broad range from building early secure smart contracts around blockchain, to security issues of fingerprint authentication, to finding security problems in software.