SMU FinTech Publication

Research – Financial Applications of Blockchain in Banks

Friday, 29 March 2019
By: Yamon Min Ye

Many Uses of Blockchain

It will change how our financial world operates.

Preface[1]: Blockchain is a time-stamped series of immutable record of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) are secured and bound to each other using cryptographic principles (i.e. chain).

Blockchain technology became known to the public in 2008[2] when Satoshi Nakamoto (real identity unknown) released the white paper '*Bitcoin: A Peer to Peer Electronic Cash System*', describing Bitcoin. The main idea behind the blockchain technology was providing digital trust, and a way to record and store data in a publicly accessible place without allowing for unauthorised edits.

Around 2014, the versatility in the usage of blockchain became widely recognised, which led to exploration of applications of the blockchain technology in different kinds of operations.

A Brief Overview on Blockchain Technology

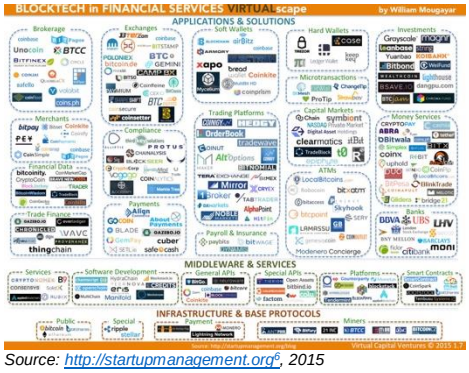
Blockchain is a distributed ledger built from[3]: (i) a private key cryptography, (ii) P2P network, and (iii) a protocol governing incentivisation. One of the ways it operates is on a proof-of-work concept where digital mining is done to create a new block. When a new transaction is initiated, the miners use intensive computing power to solve a difficult mathematical problem, and upon the first successful completion, the miner gets rewarded with a token as an incentive, and the verified transaction gets added on to the blockchain.

What are the Applications of Blockchain?

Blockchain and the distributed ledger technology could be used to establish ownership of assets or account for transactions in a secure manner.

Although cryptocurrency is the main application of blockchain that most people are familiar with, there are many other areas in which the blockchain technology can be used in, such as logistics, digital compliance, trading, insurance, and even healthcare, just to name a few.

An important area in which the application of blockchain is revolutionalising the industry is the finance sector, which will also be the focus of the rest of this paper. It was estimated in 2017[4] that around the highest percentage (30%) of identified blockchain use cases are related to banking and financial services, followed by government (13%), insurance (12%), and healthcare (8%). In fact, IBM estimates[5] that by 2020, around 66% of banks expect to have blockchain in commercial production and at scale. The blockchain technology has many different applications within the financial sector. As more people and businesses recognise the potential of the blockchain technology and its uses in the financial sector, the global landscape is rapidly changing due to many new blockchain-based startups entering this fintech ecosystem, as shown on the right.

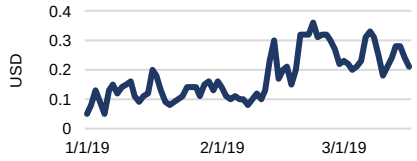


Source: http://startupmanagement.org[6], 2015

Potential Downsides to Blockchain

No new technology is without limitations and weak points, and the blockchain technology is no exception. A key issue faced by blockchain is its slow transaction speed. In 2018, the Bitcoin blockchain can handle only three to seven transactions per second, and the Ethereum blockchain can handle only 15 transactions per second[7]. However, there is a new model being created, called a proof-of-stake system, where miners can only create new blocks if they have a stake in the digital asset. This would increase the speed of transactions for large-scale applications.

The cost of making transactions using blockchain technology may be too high and volatile for scalability. The chart below shows the next block fee of Bitcoin for 2019, which is the cost of having your transaction mined on the next block, within 10 minutes. The average next block fee for 2019 so far (1/1/19 to 16/3/19) is USD 0.179 per transaction, which can be quite costly for applications requiring tens of thousands of daily transactions. The fees also fluctuate daily, making it difficult for financial planning. In addition, most blockchains only allow for storage of data in the range of kilobytes or less. Thus, in order to store large amounts of data, it would need to be broken up into smaller pieces of data per transaction, thus increasing the number of transactions and the cost incurred[8].



Source: Bitcoinfees.info[9], 2019

So, why will Banks want to use Blockchain?

Currently, there are many pain points faced by banks when settling payment transactions, especially across international borders. These include long settlement times for international transactions, and a lack of mechanism to track throughout the transfer process. The current method of international money transfer requires about one to four days of settlement time[10], which can take even longer in reality, since transfers cannot happen over weekends and bank holidays when banks are closed. Additionally, there are many fees incurred as well, such as currency exchange costs and lifting fees.

The use of blockchain would solve these problems by allowing for real time settlement and tracking of transactions.

The steps involved in monetary transfers using blockchain technology are[11]:

1. A initiates a money transfer to B.
2. This transaction is stored into a block.
3. The block is broadcast to all computers in the network.
4. These computers approve the transaction as valid.
5. This block can then be added on to the chain, providing an immutable and transparent record of transactions.
6. After the validity is approved and the block is added on to the chain, the ownership of money is transferred from A to B.

The above process can take place at any time, and in a much shorter timespan of within minutes to a few hours. Faster settlement of transactions can provide many benefits[12], such as greater financial inclusion for consumers who are not well-served by current payment options, easier cash flow management for businesses, and greater global competitiveness overall.

Examples of Banks using Blockchain

Barclays bank[13] executed the world's first trade transaction through the use of blockchain, thereby decreasing the settlement time from seven to ten days to less than four hours. This transaction would typically require many complex paper-based documents and up to a month to be completed, and it is vulnerable to document fraud. However, through the use of blockchain, both the importers and exporters could send the shipping, insurance, and other documents cryptographically as well. Although many believe that large scale adoption of blockchain for financial transactions is still five to ten years away, this transaction proves the future potential of a much more efficient payment system and financial sector as a whole.

UBS, Deutsche Bank, and other firms built the Utility Settlement Coin (USC)[14] to provide a convenient way for global institutional financial markets to process many different transactions using asset-backed custom-built blockchain. Since inception, the technology has been moving through different testing phases in order to ensure it allows for a formal transfer of ownership and real-time transaction settlements, which is crucial for this platform to go live. Although the current scope of usage of USC is quite limited, it has the potential to guide how other central banks will operate in the future, and the ultimate goal is large scale adoption of blockchain platforms that interoperate with one another. To quote Hyder Jaffrey, UBS director of strategic investment and fintech innovation, on the potential impact that this project could have in the future:

"It may well inform the way central banks choose to move things forward. We see it as a stepping stone to a future where central banks issue their own [cryptocurrency] at some point."

Opportunities: Smart Contracts for Banks

A smart contract, also called a blockchain contract, is a digital contract that can facilitate, verify, or enforce the negotiation or performance of a contract digitally. They can be changed to computer code, stored and replicated on the system and supervised by the network of computers that run the blockchain. Smart contracts allow for transactions and exchange of assets in a transparent and conflict-free way without the need for third-party services.

Consider the following example on how a smart contract could be used[15]:

(1) Parties A and B enter into a contract.

(2) This contract is written as code into the blockchain system and stored in the public ledger.

(3) The program will run the code and if a certain condition coded into the contract is fulfilled or not met, the contract will execute itself according to the coded terms. (An example of a condition could be: If a certain amount of digital currency is paid by a certain date, a digital key will be passed to the payer.)

This technology provides numerous benefits, such as safety (due to cryptography and encryption), increased speed (due to fewer paperwork), cost-savings (due to no intermediary services), and improved accuracy (due to less manual work). Jeff Garzik, owner of blockchain services Bloq, described smart contracts as:

"Smart contracts … guarantee a very, very specific set of outcomes. There's never any confusion and there's never any need for litigation."

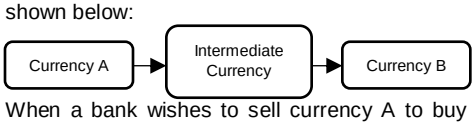
In the banking sector, smart contracts would be useful in the process of clearing and settlements. Currently, most transactions and asset exchanges involve multiple parties and require the banks to ensure that the various terms of the contract have been satisfied before commencing on the actual transfer of money. Due to the various challenges involved with such verification processes, banks need a lot of time and money to process these transactions. Due to the self-executing nature of smart contracts, they can be coded to execute certain transactions only when the coded terms of the contract are satisfied. This will aid in greatly reducing the complexity and operational costs of clearing and settlement for banks. In addition to faster transaction processing speed, there will also be increased accuracy of execution of the contracts since there will be less human error.

Currently, Citigroup[16] has started to employ the London-based blockchain payments and settlements platform offered by the startup SETL. The goal is to improve the efficiency of matching transactions and payments, and to reduce the resources required for transaction settlements.

However, despite the myriad opportunities offered by smart contracts for the banking and financial sector, there could be limitations as to the scalability of this application. As most banks process a large number of transactions daily, it could be difficult and time-consuming to switch to adopting the use of smart contracts fully, and it could take years before the wide scale adoption of smart contracts by banks takes place.

Opportunities: Central Bank-issued Intermediate Cryptocurrency

For a faster cross-border settlement system in the future, the model of an intermediate cryptocurrency being issued by the central banks of different countries is being explored and considered[17]. This digital asset would only be circulated in the interbank market, and not actively traded like the public cryptocurrencies such as Bitcoin. Simply put, this model works as shown below:



When a bank wishes to sell currency A to buy currency B, currency A is first exchanged for the intermediate currency, which is then exchanged for currency B, at the quoted price.

When any two banks wish to perform this exchange and transaction, it can be facilitated through the dealer network or exchange, which will provide a price quote on the exchange. This will allow the two banks to directly exchange currencies using the intermediate cryptocurrency. This would increase the speed and improve the efficiency of cross-border payments, since the intermediate currency can be directly transferred from the sender's account to the receiver's account.

However, a current limitation of this proposed model is that such central bank-issued intermediate cryptocurrencies have to be distributed on an interoperable, common ledger. This will reduce the complexity involved in the transactions and increase the efficiency of the overall cross-border settlement system, since there will be no need for interledger operations, and conversion of the intermediate cryptocurrency to off-ledger assets.

How can Interoperability be Achieved?

There are two categories of interoperability[18]: (1) exchange of digital assets, and (2) exchange of arbitrary data. Firstly, the exchange of digital assets can be thought of as the transfer of assets from different blockchains without the involvement of third parties. The second category of the exchange of arbitrary data is more complex and can be considered as the ability to use the data stored on one blockchain to alter another blockchain. This exchange of arbitrary data can be used for wider applications outside of value transfer as well, although that will be the main focus of this section, although it can be harder to achieve this category of interoperability.

The methods to achieve interoperability[19] in terms of exchange of arbitrary data are (1) notary schemes, and (2) relays. The method of hashed timelocks can be used to achieve interoperability in terms of exchange of digital assets.

To explain these three methods briefly, firstly, notary schemes require the services of a trusted federation to verify to the first chain a certain event about the second chain. After verification, the federation will issue a signature to proceed with the payments on the first chain, which requires this verification.

Relays allows verification by the chains themselves, thus eliminating the need for a notary federation, by allowing the first chain to understand event changes on the second chain. Currently, there are some projects underway to allow for two-way interoperability between chains, through a central hub called a relay chain.

Hashed timelocks require the payee to either acknowledge receipt before the deadline expires or give up on claiming payment, upon which, the amount to be transferred will be returned to the payer. The most famous use of a hashed timelock contract is in the Lightning Network, which allows for micropayments without third party services.

In terms of functionality, the use of hashed timelocks is the most limited method, whereas notary schemes can achieve full cross-chain interoperability. However, the drawback is that notary schemes require the most amount of trust since a notary federation needs to be employed in the verification process. Relays can offer similar levels of interoperability to notary schemes without the need for as high a level of trust, but there will be difficulties in achieving compatibility with current blockchain networks. On the other hand, the use of hashed timelocks is the most practical approach, requiring the least amount of trust, but it can only be used to achieve interoperability in exchange of digital assets, but not exchange of arbitrary data.

So, where are we headed from here?

Here is a quote by Fred Ehrsam, the co-founder of the digital currency exchange company Coinbase, which summarises our future and the blockchain's place in it[20]:

"Everything will be tokenised and connected by a blockchain one day."

Despite the current limitations of blockchains in financial applications in banks, this technology is here to stay, and we would do well to employ it early to improve the overall performance of the global banking and financial sector. Its applications are numerous and far wider than just the field of cryptocurrency alone. With current projects in place to improve upon the issues of scalability and interoperability, the importance and various applications of blockchain technology will only continue to grow from here on, until it permeates all aspects of our daily lives.

Contact: Yamon Min Ye
ymminye.2018@business.smu.edu.sg

Sources:

---

[1] Blockgeeks. (2016). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved from https://blockgeeks.com/guides/what-is-blockchain-technology/

[2] Bernard Marr. (2018). A Very Brief History Of Blockchain Technology Everyone Should Read. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#67fa2f767bc4

[3] Nolan Bauerle. (n.a.). What is Blockchain Technology? Retrieved from https://www.coindesk.com/information/what-is-blockchain-technology

[4] Hileman, Garrick and Rauchs, Michel. (2017). Global Blockchain Benchmarking Study. Retrieved from https://poseidon01.ssrn.com/delivery.php?ID=854006004112117119067021023072110069053032069011093069025100067025001117086104069006030110036003123013013081103088002115117106028051002032011065094084028066000083068040012032017067068125101073097113119089024090119025075107114028120082011024084075084067&EXT=pdf

[5] Lucinda Shen. (2016). Blockchain Will Be Used By 15% of Big Banks By 2017. Retrieved from http://fortune.com/2016/09/28/blockchain-banks-2017/

[6] William Mougayar. (2015). The Global Landscape of Blockchain Companies in Financial Services. Retrieved from http://startupmanagement.org/2015/10/22/the-global-landscape-of-blockchain-companies-in-financial-services/

[7] Ryan Browne. (2018). Five things that must happen for blockchain to see widespread adoption, according to Deloitte. Retrieved from https://www.cnbc.com/2018/10/01/five-crucial-challenges-for-blockchain-to-overcome-deloitte.html

[8] Lukas Marx. (2018). Storing Data on the Blockchain: The Developers Guide. Retrieved from https://malcoded.com/posts/storing-data-blockchain/

[9] Bitcoinfees. (2019). Bitcoin Transaction Fees. Retrieved from https://bitcoinfees.info

[10] Fexco. (2017). How long do international bank transfers take? Retrieved from https://fexco.com/fexco/news/how-long-international-bank-transfers-take/#

[11] Shah, Tejal & Jani, Shailak. (2018). Applications of Blockchain Technology in Banking & Finance. Retrieved from https://www.researchgate.net/publication/327230927_Applications_of_Blockchain_Technology_in_Banking_Finance

[12] Faster Payments Task Force. (n.a.). Benefits of Faster Payments. Retrieved from https://fasterpaymentstaskforce.org/payment-landscape/benefits-of-faster-payments/

[13] Jemima Kelly. (2016). Barclays says conducts first blockchain-based trade-finance deal. Retrieved from https://www.reuters.com/article/us-banks-barclays-blockchain/barclays-says-conducts-first-blockchain-based-trade-finance-deal-idUSKCN11D23B

[14] Michael del Castillo. (2017). Barclays, HSBC Join Settlement Coin as Bank Blockchain Test Enters New Phase. Retrieved from https://www.coindesk.com/hsbc-barclays-join-utility-settlement-coin-as-bank-blockchain-test-enters-final-phase

[15] Blockgeeks. (2017). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Retrieved from https://blockgeeks.com/guides/smart-contracts/

[16] Cyberius. (n.a.). Smart Contracts in the Banking Sector. Retrieved from https://www.cyberius.com/smart-contracts-in-the-banking-sector/

[17] Xiaohang Zhao, Haici Zhang, Kevin Rutter, Clark Thompson & Clemens Wan. (2018). Cross-Border Settlement Systems: Blockchain Models Involving Central Bank Money. Retrieved from https://www.r3.com/wp-content/uploads/2018/05/CrossBorder_Settlement_Central_Bank_Money_R3-1.pdf

[18] Aleks Larsen. (2018). A Primer on Blockchain Interoperability. Retrieved from https://medium.com/blockchain-capital-blog/a-primer-on-blockchain-interoperability-e132bab805b

[19] Vitalik Buterin. (2016). Chain Interoperability. Retrieved from https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf

[20] Fred Ehrsam. (n.a.). Blockchain Quotes. Retrieved from https://www.brainyquote.com/quotes/fred_ehrsam_850313?src=t_blockchain