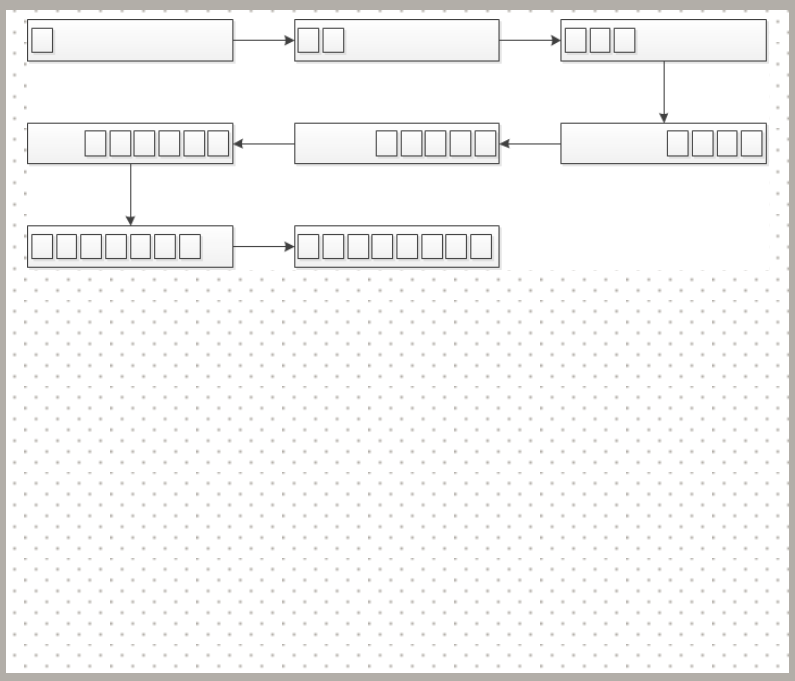
INSIGHT

SEPTEMBER 2015

BLOCKCHAIN TECHNOLOGY

BLOCKCHAIN TECHNOLOGY HAS THE POWER TO LOWER COSTS, PREVENT FRAUD AND REDUCE TIME TO SETTLEMENT. READ ON TO FIND OUT MORE ABOUT THE INNOVATION THAT THE MAJOR BANKS ARE INVESTING IN NOW TO HELP THEM ADHERE TO REGULATION AND PROVIDE A BETTER SERVICE FOR THEIR CLIENTS.



Anju Patwardhan, Chief Innovation Officer at Standard Chartered, has claimed Blockchain Technology could contribute to the "security of banks and integrity of the financial system"[1]. While John Palychata, of BNP Paribas Securities Services, says the "system has the potential to completely upend post-trade infrastructure"[2]. Furthermore, Oliver Bussman, Group Chief Information Officer at UBS, claims the technology has the possiblity "not only to change the way we do payments but it will change the whole trading and settlement topic"[3]. So what is Blockchain technology and what impact could it have in the real economy? In this article we outline how Blockchain technology works, and discuss the benefits and drawbacks of what could be the biggest change to the banking industry since the 16th Century, when central clearing banks were first established.

Technical Overview

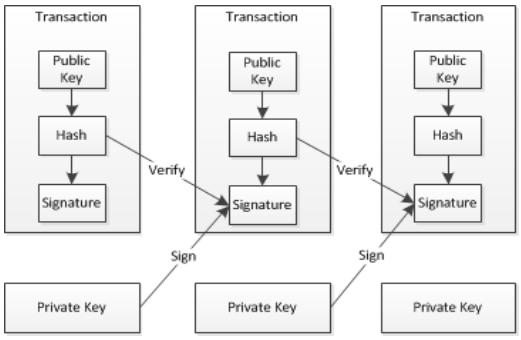
Origins of Blockchain Technology, the real innovation of Bitcoin

Blockchain is the technology behind the much debated Bitcoin currency. Bringing together cryptography, game theory and peer-to-peer networking, the key innovation behind the digital currency is a distributed ledger which allows a payment system to operate in an entirely decentralised way, without any intermediaries. An electronic payment system, such as Bitcoin, must have a reliable method of recording transactions that all participants can agree are accurate. To achieve this there are two main issues: devising a secure and reliable method of updating a public ledger of which there are multiple copies distributed globally, and the second is creating the necessary incentives for users to contribute resources to verify transactions.

The number of Bitcoins at any address is derived from the output of earlier transactions that are all publically available on the Blockchain. Bitcoin transactions may have a number of inputs or outputs; for instance, any 'change' from a transaction is paid as an output and any credit included in the input which is not accounted for in the output is accepted as a transaction fee. Digital signatures are used to provide proof that the transaction message was created by the person who wants to make the payment. This is a form of public-key cryptography – it works by creating 'public' keys which can be used to decrypt messages encoded by a corresponding 'private' key. To create a digital signature, the sender encrypts the message they wish to sign with their private key. This message can then only be decoded with the corresponding public key, which is also broadcast so the transaction can be verified. 'Miners' is the term given to those who compete to decrypt blocks on the Bitcoin network; these miners are arranged in a peer-to-peer configuration, with no centralised point. Although miners are under no obligation to do so, the Bitcoin protocol calls for all messages to be transmitted across the network on a 'best efforts' basis, sharing the message with one's immediate peers. This means the transaction is not broadcast to the entire network at once, but instead goes to a subset of the peers first, then to their peers and so on. Bitcoin users are under no formal requirement to pay transaction fees and if they do offer one, the size of that fee is at their discretion. However, Bitcoin miners are able to choose which transactions they process, so a higher fee offered gives them a greater incentive to validate transactions.

Verification of a transaction block has two elements: validation and achieving consensus. Validating a transaction, which includes checking the digital signatures, takes a very short amount of

WORKFLOW OF A SIMPLE BLOCKCHAIN



Source: Bitcoin : Peer-to-Peer Electronic Cash System, Nakamoto

time – less than 10 seconds in 99% of cases. By design, establishing consensus is more difficult and requires each miner to demonstrate the investment of computing resources known as 'proof of work'. Digital currencies make use of a fundamental principle in game theory: 'cheap talk'. That is, any proposed change to the ledger, since it is effectively free to issue, should receive very little weight. In order for a proposed change to the ledger to be accepted by others as true, those

proposing the change must demonstrate that is was costly for them to initially issue the proposal. This allows the incentivisation of the system to be balanced in favour of transaction verification by making it very easy to spot a fraudulent transaction. The only method of attacking the system is by assembling sufficient computing power on a network to 'verify' fraudulent transactions. This would undermine trust in the ledger as a whole and the value of any Bitcoins the attacker could steal. Therefore, it is logical for anyone capable of assembling the necessary computing power to contribute to the continuation of the system, rather than attacking it. The proof of work scheme means that the time taken for a miner to successfully verify a block of transactions is largely random. As new miners join the network or as exiting miners invest in faster computers, the time taken for a successful verification can fall. To allow time for each verification to pass across the entire network, the difficulty of the proof of work problem is periodically adjusted so that the average time between block remains broadly constant at ten minutes for Bitcoin, meaning that payments are not instantaneous.

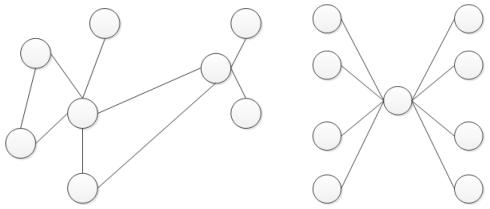
The nature of a distributed system means that it is feasible for two miners to successfully verify two different candidates for the next block at essentially the same time. When this happens, both copies are initially retained by the network as branches of the main chain, but miners will proceed to work on the candidate block that follow on from whichever one they receive first. The chain of blocks representing the longest sum of work done is accepted as truth within the Bitcoin network. Whichever branch is received by the majority of the network will initially be selected. However, the branch with the most computation resources should ultimately take the lead. This branch will be the most likely to have a subsequent block built on top of it and is therefore more likely to eventually 'win' the race. Miners that are working from alternate branches then have a significant incentive to switch to the longer branch, as any work they contribute to the shorter branch will never be accepted by the majority of the network.

Application in the real economy

Despite the application of new technology, the basic structure of centralised payment systems has remained unchanged since the early banks set up a central 'clearing' bank so their clients could transfer money to the clients of other banks. In the traditional banking system, there is a central ledger, with settlement taking place across the books of a central authority, acting as a clearing bank. This is traditionally undertaken by the central bank of the given country. Each participant holds a balance at the central bank, recorded in the ledger, which is reflected in the participant bank's internal ledger. However with the application of the blockchain, financial organisations or even individuals could directly exchange funds without the need for any intermediaries. Banking is already almost entirely digital, so technology innovation is likely to be the most influential source of disruption. This should lead to reduced transaction transfer times, at a lower cost.

A key problem of any electronic payment system is how to ensure that money cannot be 'double-spent'. A payment system that relies on digital records must have a way of preventing double spending because it is simple to copy and edit digital records. An alternate approach to the historic central ledger approach is to implement a fully decentralised payment system, in which copies of the ledger are shared between all participants and a process is established by which users agree on changes to the ledger. Since

DISTRIBUTED VS CENTRALISED LEDGER NETWORK



anybody can check any proposed transaction against the ledger, this approach removes the need for a central authority and thus for participants to have confidence in the integrity of any single entity.

Legal implications

Combat Money Laundering

With Blockchain technology creating the visibility to view the full transaction history of every event throughout the chain, vendors have already shown how anti-money laundering (AML) services can be developed. By giving greater transparency

and enhancing compliance to regulations, the technology can aid in the identification of any activity that is suspicious or non-compliant. Blockchain technologies can aid industry participants to adhere to a number of regulations including AML and T+2 Settlement.

A Private Network

The traditional banking system has a level of privacy by limiting access to information to the parties involved and the trusted third party. In a distributed system it is necessary to announce all transactions publicly, however privacy can be maintained by recording events in a different way. By keeping public keys anonymous everyone can see that an individual is sending an amount to someone else, but without information linking the transaction to that person. This is analogous to the level of information released by stock exchanges, where the time and size of individual trades is made public, without revealing who the parties involved were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. However if regular multi-input transactions occur there is a risk of the transactions being linked to the owner.

Risk

In an intermediated banking set up there are three main types of risk: credit, liquidity and operational risk. The modern banking system evolved in response to the need to make payments more efficiently, and when payment systems were computerised this need remained. However, because there is a centralised point in the network which all transactions must pass through, there is a single target for attackers. Current distributed payment systems remove the credit and liquidity risks by eliminating intermediaries: payments are made directly between the payer and the payee. To confirm this, users need to have confidence that for any distributed system they use, the cryptography employed has been implemented correctly.

Distributed systems should also be more resilient to systematic operational risk because the system as a whole is not dependent on a centralised third party. A distributed system effectively has as many redundant backups as there are contributors to the network. The ledger exists in multiple copies which essentially makes it more resilient than a centralised database. Historic transactions are unalterable and permanently accessible to all participants, ensuring that if an attack does occur each participant's balance is recoverable.

Fraud

The nature of fraud risk is also significantly different between a centralised and decentralised payments system. In a decentralised system there is no need for users to disclose their complete payment details when making a payment, thus removing the risk of payment details being stolen in the transaction process. However, the risk of direct loss of currencies is higher than that for deposits held with commercial banks: if a user's private key is lost then their digital currency will not be recoverable. The problem of keeping private keys secure means that investors could entrust an authority to look after them, opening up a new market for companies offering this service.

Distributed systems are also subject to a danger of system wide fraud if the process of achieving consensus is compromised. Cryptocurrencies are currently designed so that a would-be attacker would require sustained control of a majority of the total computer power across the entire network of miners. The rule that the chain with the greatest sum of work done wins is the vital element in combating fraud in the Bitcoin network. Any attacker attempting to modify earlier blocks would have to control enough computing power for them to both catch up with and overtake the genuine blockchain as the longest. To be assured of success, the would-be attacker would need to obtain and retain the majority of all computing resources on the network. This is known as the 50%+1 rule.

There are two areas of weakness in the 50%+1 rule: the position of the attacker in the network and the strategic timing of when an attacker chooses to release messages to the rest of the network. An attacker's position in a network is significant because the longer it takes for messages to propagate across a digital currency's network, the greater the probability that a fork in the chain will emerge. A potential attacker which is centrally located will be able to communicate to most of the network quickly, and so may not strictly require a majority if other users are relatively distant. Furthermore, an incentive exists for miners to strategically choose when they broadcast their success at verifying transaction blocks. Miners can

delay announcing their success so that other miners waste time trying to verify the old block, while the user starts to work on the new block. As mining is a zero-sum game, it is possible that when one miner receives outsized returns, this creates an incentive for other miners to either drop out or to join in the first pool, eventually leading to the pool controlling a majority of the network's computing resources. However, in principle this could be resolved by existing completion rules, assuming that Regulators have visibility of the proof-of-work of each pool.

Moreover, it is possible to impose conditions on the payment, so they the receiver cannot spend the proceeds unless they are met. Therefore, the rules could be set so that any user would have to announce the block to the whole network fully before they could start work on the next block. More complex transactions may require multiple conditions to be met before any funds are released. This capability allows the technology to be expanded to support more complex transactions.

Economic implications

Impact on intermediaries

Through better visibility between supply and demand, settlement processes will be more easily streamlined leading to reduced overheads in settlement costs including personnel to run settlement desks, reduced/non-existent buy-ins, reduction in failed trades and associated costs, to name a few. Overall the transparency allows the whole supply chain to work a lot more efficiently, reducing overall costs, through direct personal and indirect costs (buy-in, fails etc) and lead times to settlement. As the adoption of blockchain continues, we expect to see rationalisation in intermediaries, in addition to new blockchain-only entrants offering a more efficient service to clients who wish to trade directly.

The cost

One major concern about blockchain technology's application to banking is how all these transaction blocks would be stored, as a distributed ledger is far less efficient than a centralised database. A block header with no transactions is roughly 80 bytes in size. In cryptocurrencies so far, a new block is generated approximately every ten minutes. This equates to: 80 bytes x 6 x 2 4 x 365 = 4.2MB per year. Moore's Law predicts that at the current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory. Consequently, there is the question of how much computing power would be required to operate at the volume and frequency of modern payments. In order to be able to break the keys quickly, significant computing power is required; the amount of heat this would generate could be significant, causing unexpected server shutdown. This amount of server power is expensive to maintain efficiently and is damaging to the environment – something which financial services organisations are increasingly considering when making investments.

Blockchain in practice

Incentivisation

One of the biggest questions about how to put a distributed system into practice, is how to incentivise people to actually join the network. Bitcoin rewards users with new coins each time they map the transaction keys – this also serves to grow the supply of the currency within the network. However, this is not sustainable in the real economy. An alternate method of incentivisation can also by funded with transaction fees. If the output of a transaction is less that its input values, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Similarly there could be a fixed transaction fee, like with Paypal, that the public would be willing to pay over and above traditional banking rates for an improved service.

The incentive may also help to encourage miners to stay honest. If a potential attacker is able to assemble more CPU power that all the other nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate more money. He ought to find it more profitable to play by the rules than to undermine the system and the validity of his own wealth.

Infrastructure challenge

Adopting this technology would require the industry to completely change the way they think about IT architecture. This will require significant investment and modification of internal, as well as external, processes. However, when financial institutions are faced with such challenges – as has recently been the case with KYC – they can collaborate and find cost effective solutions if there is a common goal. We are seeing nearly all global banks setting-up research departments into this area or buying-up fintechs who are specialized in distributed technology to stay competitive.

WHEN IS IT RECOMMENDED TO HAVE WHICH TYPE OF NETWORK

Distributed Ledger	Centralised Ledger
Multiple entries and exists in the market	Stable market
Low value transactions	High frequency transactions
Irreversible transactions	Long/short transactions
Trust is an issue	Participant verification required
Multiple assets in a transaction	Unsophisticated participants
Susceptible to money laundering	Trades cannot be pre-funded

Conclusion

This could be one confirmed success story where banks, regulators and tech companies work together to reduce costs, increase transparency and restore consumer trust. Distributed ledgers work best where transactions can be pre-funded, participants are knowledgeable and where money-laundering is an issue. The largest potential markets are cross-border payments and clearing securities. These are obvious opportunities as blockchain technology thrives where new parties regularly enter and leave the market, and where transactions involve multiple entities and assets.

Not only does Blockchain technology have the potential to completely revolutionise the traditional banking industry, it has the capacity to bring banking services to completely new markets. According to the IMF, around 50% of the World's adult population do not access formal banking services in any form. This may be due to geographic location, lack of trust in the banking system or being 'unbanked' because they lack the credit worthiness financial institutions require. However, with blockchain, as long as you have an internet connection and the appropriate software you can make a transaction; furthermore, as described above, a distributed ledger removes the need for preceding trust in the participants as money cannot be double spent.

It remains to be seen whether banks will successfully adopt this new technology or be completely surpassed by it. While it is likely that there will continue to be demand for transitional banking services, this is another threat to profits that banks will have to carefully navigate. This challenge is so apparent that China has banned Bitcoin because of the threat it poses to the traditional banking system. On the other hand, blockchain technology could, according to Santander, "reduce banks' infrastructure costs related to cross-border payments, securities trading and regulatory compliance by $20bn a year up to 2022"[4].

1 https://www.linkedin.com/pulse/blockchain-disruptive-force-good-anju-patwardhan

2http://securities.bnpparibas.com/quintessence/hot-topics/beyond/bitcoin-and-blockchain-what-you.html#.VfWED_lVikp

3 http://www.efinancialnews.com/story/2014-10-28/fintech-news-2-oliver-bussman-ubs?ea9c8a2de0ee111045601ab04d673622ea9c8a2de0ee111045601ab04d673622&ea9c8a2de0ee111045601ab04d673622ea9c8a2de0ee111045601ab04d673622

4 http://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/

YOUR CONTACTS

DEAN BEDGGOOD

Manager - CIB and Regulatory
+44 7584 450 988
dean.bedggood@sia-partners.com

DAVID QUIRIN

Manager - CIB and Regulatory
+65 927 102 01
david.quirin@sia-partners.com

CHESCA VEAL

Junior Consultant
+ 44 7825 083 266
chesca.veal@sia-partners.com

ABOUT SIA PARTNERS

Founded in 1999, Sia Partners is an independent global management consulting firm with over 600 consultants and an annual turnover of USD 120 million. The Group has 16 offices in 13 countries, including the U.S., its second biggest market. Sia Partners is renowned for its sharp expertise in the Energy, Banking, Insurance, Telecoms and Transportation sectors.

For more information visit : www.sia-partners.com . Follow us on Twitter @SiaPartners

Asia

Hong Kong
701, 77 Wing Lok St,
Sheung Wan, HK
T.+852 3975 5611

Singapore
3 Pickering street
#02-38
048660 Singapore
T.+ 65 6635 3433

Tokyo
Level 20 Marunouchi
Trust Tower-Main
1-8-3 Marunouchi,
Chiyoda-ku
Tokyo 100-0005
Japan

Europe

Amsterdam
Barbara Strozzilaan
101
1083 HN Amsterdam
- Netherlands
T. +31 20 240 22 05

Brussels
Av Henri Jasparlaan,
128
1060 Brussels -
Belgium
+32 2 213 82 85

London
Princess House,
4th Floor, 27 Bush
Lane,
London, EC4R 0AA –
United Kingdom
T. +44 20 7933 9333

Lyon
Tour Oxygène,
10-12 bd Vivier
Merle
69003 Lyon - France

Milan
Via Medici 15
20123 Milano - Italy
T. +39 02 89 09 39
45

Paris
18 bd Montmartre
75009 Paris - France
T.+33 1 42 77 76 17

Rome
Via Quattro Fontane
116
00184 Roma - Italy
T. +39 06 48 28 506

Middle East & Africa

Dubai, Riyadh, Abu Dhabi
PO Box 502665
Shatha Tower office
2115
Dubai Media City
Dubai, U.A.E.
T. +971 4 443 1613

Casablanca
14, avenue Mers
Sultan
20500 Casablanca -
Morocco
T. +212 522 49 24 80

North America

New York
115 Broadway 12th
Floor
New York, NY10006 -
USA
T. +1 646 496 0160

Montréal
600 de Maisonneuve
Boulevard West,
Suite 2200
Montreal, QC H3A
3J2 - Canada