Understanding Blockchain Technology
And What It Means for Your Business

✕ DBS

Understanding Blockchain Technology

And What It Means for Your Business

Antony Lewis	*Principal Author*
Mikkel Larsen	*Contributor and Supervisor*
Chien Yen Goh	*Editor in Chief*
Geraldine Tan	*Editor*
Martin Tacchi	*Art Director*

⊠ DBS

Introduction

Blockchains came to prominence in the popular media recently. Articles ranged from cynicism that blockchains are nothing more than shared databases hyped up by venture capitalists, to amazement and wonder about a new technology that has the potential to create social, societal, and economic change.

So far, the focus of the discussion around this technology has centred on blockchains used as a tool for financial services to improve transparency and efficiency, and reduce cost within the industry. In response, blockchain technology providers are being created all over the world, incubated independently or by innovation labs sponsored by banks and other entities. The start-ups are enthusiastically experimenting on applications of this technology to problems within the financial services domain.

While a lot of the discussion comes from Western Europe and the US, tinted with region-specific issues and perspective, we believe that the potential of blockchains can have the most impact to the Southeast Asian economic community. The major determinant of success in unlocking the potential of this technology will be the ability for entities to collaborate closely, whether the entities are commercial companies, financial institutions, or governments.

With financial technology investment in Asia Pacific rising to US$3.5 billion in the first nine months of 2015 from US$880 million in 2014 according to Accenture[1], we believe that this Asian-focused blockchain primer, the first of our series on blockchains, is timely.

This report aims to give readers a deeper understanding of the technology in hopes that it will aid in investment decisions in start-ups that are exploring and supplying blockchain solutions, or on whether to deploy capital into blockchain experiments for their own businesses. ✖

We believe that the potential of blockchains can have the most impact where it achieves joint implementation of a number of benefitted parties. This is a collaborative challenge rather than a technical one and is not unique to blockchains

1   Accenture. *Fintech Investment in Asia-Pacific set to at least quadruple in 2015*. Retrieved from https://www.accenture.com/sg-en/insight-fintech-innovation-lab-asia-pacific.
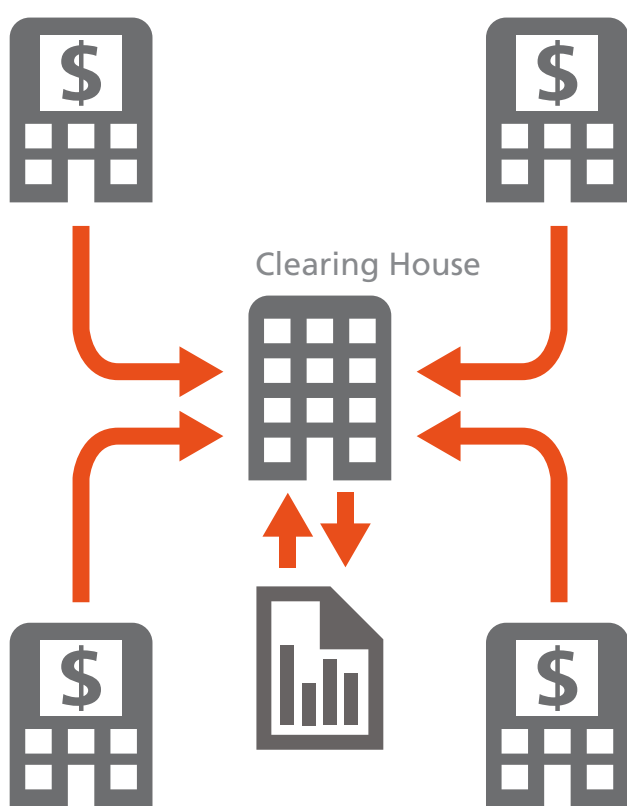
❌DBS

What Are Blockchains?

When people talk about blockchains, at the broadest level, they mean a network of databases spread across multiple entities that are kept in sync, where there is no single owner or controller of the data. The databases tend to be append-only, that is they can be written to, but historical data can't be altered without broad agreement from the participants of the network. This means that a user or system administrator in one entity can't alter data held on a blockchain without agreement from the other participants.
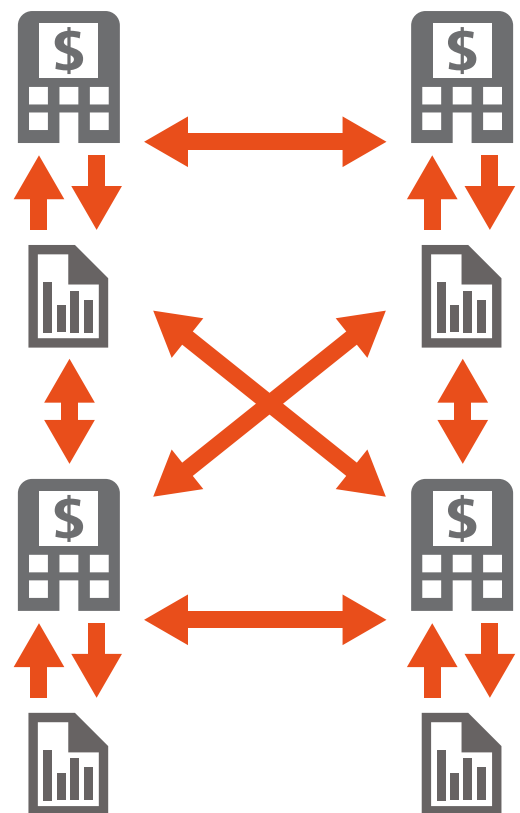
Purer than golden sources of data

Historically, when multiple parties need to rely on the same data, we have used golden sources of data, held and controlled by trusted third parties. A classic example is the use of a clearing house that is the golden source of data about a trade between two entities. Blockchains can empower groups of parties to agree on events without needing the third party, such is the promise of this new technology.

How blockchains, with a distributed database, eliminate the need for third parties among financial entities

Clearing House

Centralised Database

Distributed Database

Benefits of Blockchains

In situations where trust levels are low, due to differences in operational and regulatory landscapes, such as multi party cross border transactions, the transparency offered by blockchain could help by making the lack of trust less of a hurdle in these interactions.

Efficiency

No need to reconcile data externally

Blockchain technology could improve efficiency when financial entities are reconciling trades. Typically a bank will nominate one of its systems as the golden source of trade data for any particular security. That golden source could be an in-house built system or an off-the-shelf solution. Reconciling this against an external party (whether that's the trading counterpart or an industry third party) has drag and inefficiencies due to system incompatibilities and processes. This leads to reconciling using the "best common technology" – typically end-of-day batch files. A blockchain will mean that the agreed trade data is already in-house, removing the need to reconcile externally, as the blockchain has already done that in real time.

Using "smart contracts" to speed up payments

The use of blockchains could also help speed up payments between financial entities. As blockchains can store data, they can also include code snippets that automate messages and one-day payments, using the "if-this-then-that" logic. If parties can agree upfront on the payoffs (usually this is agreed in term sheets written in dry legal language) and can encode the payoff terms into the trade details itself, then there can be efficiencies when trade lifecycle events take place, including error reduction and speed increases. These code snippets saved onto blockchains are called "smart contracts".

Transparency

A real time view of the trades

With trade data published to a common platform, regulators or other interested parties can plug into this and get a real time view of the trades. This gives regulators oversight into one common source, rather than receiving reports in different formats at different times from each institution. The transparency offered by blockchains could help regulators detect systemic risks sooner.

Computer coded "smart" contracts

Traditionally for trade payoffs, entities had to rely on heavy legal documentation, such as International Swaps and Derivatives Association (ISDA) master agreements. But computer code, by its very nature, is far more readable and predictable than legal language. By writing payoff structures onto a common platform in computer code which can be tested against, a smart contract on a blockchain provides for much higher levels of transparency over outcomes.

Non-financial parties could also stand to benefit from the transparency offered by

blockchain applications as they allow multiple parties to have access to the same data, where traditionally, data held by third parties can be obfuscated or withheld.

Resilience

The more the merrier

Storing data over a large number of nodes benefits the resilience of the data – the larger the number of blockchain participants, the more robust the data, with longer life. In this respect, a blockchain system is similar to a massively replicated database.

Governance and Trust

Crowd-sourced honesty

In a blockchain system, a majority of participants need to agree on data being added before it becomes part of the definitive blockchain. This is very different to central, often secretive ledgers held and controlled centrally. When multiple parties have a say over what data is written, the ability to alter data, or remove dubious data, it creates a more honest system.

An example would be land registry systems. When held centrally, a database administrator can easily make a change to records and cover their tracks without others knowing. If a land registry were held on a blockchain system with multiple participants (for example local government, regional government, perhaps other government branches and even NGOs), then the other parties would need to agree to make a change to a record, and any questionable changes would immediately be detected and not added without a majority consensus.

Should Banks Be Excited?

Getting on the blockchain bandwagon

If you buy in to the media narrative, it's easy to see why there is so much interest in this space – the promise that for the first time in IT history, you can easily set up a write-only system that creates agreement between disparate entities about events, proven to be tamper-proof, and does not require a third party to host the data.

Contrary to the perception that banks are conservative and big banks even more so, blockchain technology has been latched on to by the largest global banks. Financial institutions are driving this new technology and pioneering experiments.

More and more applications

Initially, blockchains were thought of as a new way to gain efficiency and reduce risk and cost across the entire industry by offering a self-reconciling database for clearing trades. Since then, more applications are under exploration, from asset registration to shared storage of digital documents.

In financial services, multiple entities currently keep track of events in independent in-house ledgers. The ledgers are then reconciled through end-of-day and intra-day processes, with backoffice manpower doing much of the heavy lifting.

A 21st century central clearing house

The idea is that these processes could be replaced by systems that automatically share and reconcile events in real-time, resulting in all entities working from the same data, reducing cost and risk for the participants, much like using central clearing houses, but replacing the trusted third party with a technological solution where participants remain in control of their own data.

How blockchains can benefit financial services

Take for example a centrally cleared, over the counter trade like an interest rate swap. For the entire lifecycle of a trade, which could last many years, the two parties to the trade and the clearing house keep track of events, including:

- Initial booking of the trade
- Calculation of the premium paid
- Payment of the premium
- Calculations of accrued interest for the fixed and floating legs of the trade on each coupon date
- Payment of interest on each coupon date
- Foreign exchange revaluation entries during the course of the trade
- Termination of the trade

Current methods are prone to data corruption

Each of these events are calculated multiple times in multiple systems and recorded in multiple ledgers. The current methods of reconciling separate ledgers are prone to breaks, missing information, and calculation differences. This leads to different versions of the events in different bank systems, increasing risk and associated time wasted investigating the source of these discrepancies.

How blockchains, with a common database, streamline reconciliation of trades between financial entities

Entities reconciling own databases

Entities using a blockchain

⊠DBS

One event, one version

In a blockchain system, each event exists as one single version of the event stored onto a database and distributed to relevant parties. The blockchain consensus mechanism aligns all the entities to have the same view of the event. This happens without a third party, and it is enabled by protocols that ensure that each entity independently checks that data conforms to the technical and business rules that they originally agreed upon.

Improves current trading-floor and control practices

What this means for the front office is that it now has the ability to trade with other entities, with the same trade details being guaranteed for both entities. This is an improvement to current trading-floor practices where shorthand, typos, and misunderstandings can lead to trades being booked the wrong way around or with wrong details.

In the backoffice, employees are kept busy creating and monitoring control processes, reconciling data between fragile legacy systems internally, and then reconciling the same data externally. For example, maintaining reference data, especially sensitive customer data, is a significant cost and risk to banks. The response to date has been to create industry utilities to manage this. In October 2015, Goldman Sachs, JPMorgan Chase, Morgan Stanley, and SmartStream announced the creation a reference data utility called Securities Product Reference Data or SPReD that will normalise and validate data across asset classes.

No need for third parties

Blockchain technologies can negate the need for third parties to be involved in this kind of data management. This can be used for something as trivial as agreeing foreign exchange (FX) settlement holidays (the days on which specific currencies don't settle) through to having an industry view of counterparty data, which can be selectively revealed to trading counterparties.

Tracking virtual currencies is just one use of a distributed database, where the database is used as a transaction ledger. However, the enabling technology - the blockchain system - can be used for more. Just as Microsoft Excel (the enabling technology) can be used for building an income statement, creating charts of sales revenues or solving Sudoku problems; just as a database (the enabling technology) can be used as a trade repository or an address book; just as the internet (the enabling technology) can be used for building Facebook or Twitter or news websites, so too can a blockchain system be used for more than tracking the movement of virtual currencies.

Withering of trusted third parties in financial sector?

Third party risks

In finance, trusted third parties are relied upon extensively. Entities such as clearing houses, central counterparties, exchanges for equities and futures all exist to reduce risk between financial institutions that may not trust one another fully but need to work together. However, while the problem of "golden source of truth" is solved, adding a third party creates new problems.

× DBS

Technical failure

The third party becomes a single point of potential failure. Technical failures occur and effects can be significant. For example, in October 2014, the Real Time Gross Settlement payment system in the UK, which is responsible for clearing hundreds of thousands of payment transactions worth £275 billion per day, went offline for ten hours. This led to delayed crucial payments and sparked the need for an independent review. Exchanges, which are centralised entities where buyers and sellers meet, are prone to similar outages. This leaves customers at risk, temporarily unsure about the state of orders left with the exchange. A recent example of this was in July 2015 when the New York Stock Exchange went down for over three hours due to a software glitch.

Data concentration attracts attacks

The third party is at risk, both from external hackers and internal employees. The concentration of valuable data makes the third party an attractive target, both for reselling the data and for causing damage to the systems. Internal employees enjoy privileged access to data and systems. This increases and concentrates risk.

Disrupting third parties' monopolies

Often, industry third parties have a monopoly and industry participants often don't have alternatives. As such, the incumbent industry utilities have no real incentive to offer competitive prices, no real incentive to produce superior customer experience, and no real incentive to innovate. For example SWIFT, an interbank messaging network and standardisation scheme used for sending messages about payments (and more), has such a grip on the banking sector that there is no real competition. Similarly, CLS (a specialist US financial institution) is the de-facto clearing mechanism for FX trades. Many countries use clearing houses for equity transactions. Each of these trusted third parties act as quasi-monopolies for their function.

Cross border legal complications

International third parties add an additional element of legal risk, as they are in a specific jurisdiction that may be different to the jurisdictions where each party to a transaction is located. The government of the third party can subpoena data belonging to the trading counterparts, who are not in a position to keep their data private.

There are many reasons why giving up trust, power, and control to third parties is undesirable. The potential of consensus distributed ledgers lies in the ability to remove the third party, yet still have participants agree on what the golden source of truth is.

Why You Should Be Excited Too

What we now have is the ability to build networks of data storage (and computational processing, in the case of smart contracts), where participants can know that the data conforms to the rules of the particular blockchain, both on technical and business levels, and that the stored data is trustworthy, without prejudice to the trust levels of the individual participants.
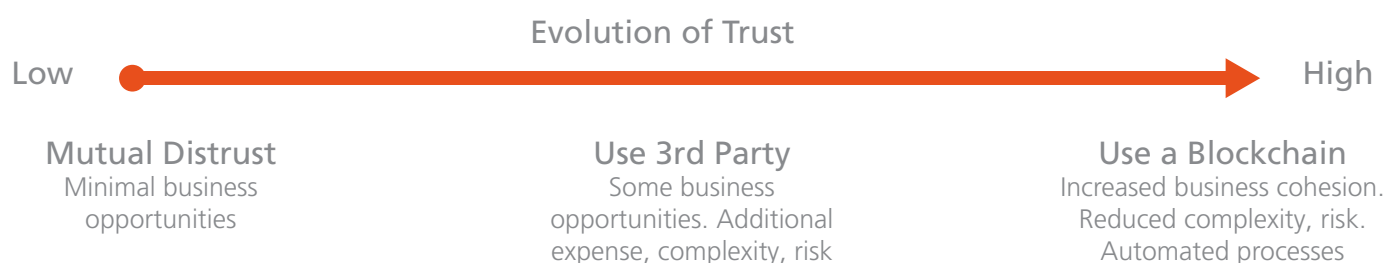
It is always difficult to predict what technology will eventually be used for. In the medium term, we currently believe that blockchains can make a positive impact where you have any of the following situations:

- Separate entities need to rely on the same version of events (use a blockchain where each entity can write and validate the data)
- Trust in a centralised entity or authority is low (use a blockchain where the validation is spread between multiple separate, unrelated entities)
- Logging of events needs to be shown to be tamper-proof (use a blockchain where external entities are connected and validating data in real time)

Bridging trust gaps

We believe that there are several environments where blockchains could solve problems, or at least reduce risk or increase efficiency. Blockchains are the ideal solution for mulitple entities that do not fully trust each other and need to agree on a single version of events, or require a data source that is tamper-proof. Blockchains could also add value where third parties are used either due to a low trust environment (such as escrow services) or as a golden source of truth.

How implementation of a blockchain can improve trust between stakeholders

Evolution of Trust

Low ●━━━━━━━━━━━━━━━━━━━━━━━▶ High

Mutual Distrust
Minimal business
opportunities

Use 3rd Party
Some business
opportunities. Additional
expense, complexity, risk

Use a Blockchain
Increased business cohesion.
Reduced complexity, risk.
Automated processes

Doing away with paper

Another place to look is where paper documentation is prevalent. Paper documents have historically been used in place of trust – instead of trusting the word of the merchant, you trust the paper certificate of authenticity. However, the world has evolved and paper

certificates are easy to replicate or forge – easier than digitally signed digital documents. Blockchains can provide for digital records with guaranteed authenticity and uneditable audit records.

Technology trumps trust

Where digital records are held centrally by a single entity, there may be a place for blockchains – if trust in the entity is low or if the entity needs to demonstrate that the data is tamper-proof. This is because having the data on a blockchain demonstrates mathematically and systemically what an auditor had to accept on trust previously.

The promise of the technology is to replace the need to trust third parties with live, append-only databases with some level of compute logic, self-reconciled, and independently validated across multiple data centres and owners, containing uneditable, time-stamped records of the network-agreed truth.

Transaction ledgers

Exist only in ether impedes adoption

Bitcoin is a digital token whose ownership can be passed from user to user. This token has no real-life tangible representation, and as such is referred to as an 'on-chain' asset. That means, it exists on its blockchain, and owning the token reflects nothing else except that you own the token. The role of on-chain assets in traditional financial services is currently uncertain, and remains so unless or until on-chain assets can legally represent sovereign currencies, shares, or other dematerialised assets.

Opportunities in digitizing real assets

'Off-chain' assets, by contrast, are real-world items (such as gold, shares, currency) that are digitally represented on a ledger by a token or tokens issued by an issuer. The issuer will safe-keep the real-world item and issue tokens on a ledger against them. The token represents a title deed for that asset and can be passed from user to user. Ultimately a user will return the digital token to the issuer and make a claim on the real-world asset. One current idea for blockchains-as-asset-ledgers is to facilitate faster and more efficient settlement of off-chain assets.

Event recording

Beyond ledgers any event can be "blockchained"

Moving away from the term 'ledger', with its financial connotations, events can also be recorded. An event could take the form of any sort of data and can be recorded in plain view or encrypted. Events in financial services could be anything from messages between entities to documents, meeting minutes to shareholder votes, counterparty data (e.g. mapping of legal entities to nostro accounts) to industry-agreed FX settlement holidays. The protection gained from using a blockchain is that the data can not be edited once written, and has a trusted timestamp, without relying on an independent trusted third party. ❎

Understanding the Technology

This technology and space are new, and as such there are many different ways to understand blockchain systems and terminology has yet to be standardised. In its simplest form, a blockchain acts like a shared, replicated, append-only database where write access is shared among participants, but validation is performed by all participants. Taking the elements common to most blockchain systems, there is:

- A data store, usually containing financial transactions, but could contain any type of data
- Data replication across a number of systems in real-time
- Peer-to-peer network topology instead of hierarchical client-server models
- Usage of cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights
- Mechanisms that make it hard to change historical records, and make it easy to detect when someone attempts to do so

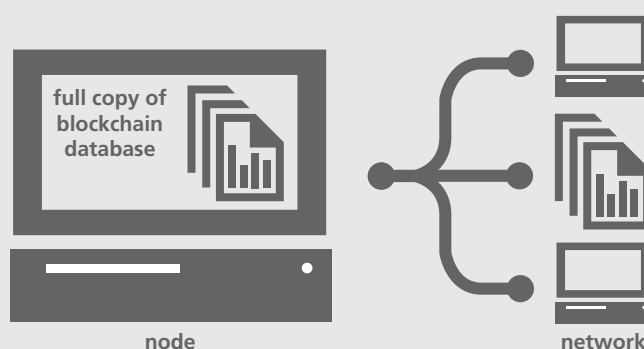*a blockchain acts like a shared, replicated, append-only database*

Where blockchains differ widely in set-up and functionality are whether they are public or private; like any network that is open to the public, defences are needed that are different to a private network. Blockchain systems have different mechanisms or protocols depending on if they need anyone to be able to write to them (public or permissionless blockchains) or if the participant pool is limited (private or permissioned blockchains). The purpose of the blockchain affects the engineering of the system. In general, public-write blockchains are much more constrained than private ones.
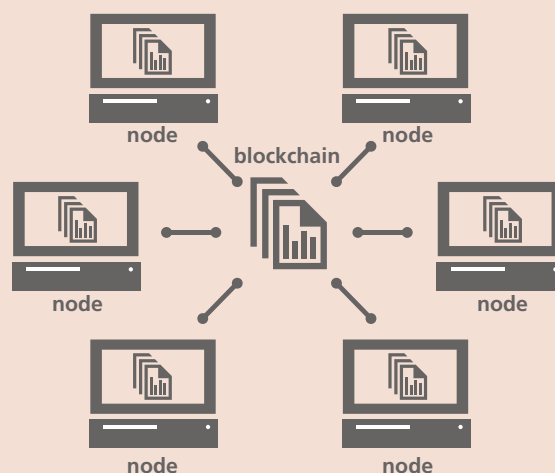
How It Works

Be part of the blockchain system network

To be a part of a blockchain system, participating entities will each install and run some software that connects their computer or server to other participants in the network. By running this software, the participants act as individual validators, called network nodes.

When a node connects to the network for the first time, it will download a full copy of the blockchain database onto its computer or server.

full copy of blockchain database

node

network

×DBS

The network of nodes manages the database, also known as the blockchain. The nodes are entry points for new data, as well as the validation and propagation of new data that have been submitted to the blockchain.

But in a distributed system with no golden source of truth, how does the network come to consensus, or agree on what data to write on the blockchain? How do you resolve a situation where equivalent people can say conflicting things, but there is no boss to arbitrate?

The answer – using protocols. In a blockchain system there will be protocol, i.e. pre-agreed rules for technical and business validity of data to be written, and a rule to determine how consensus is achieved.
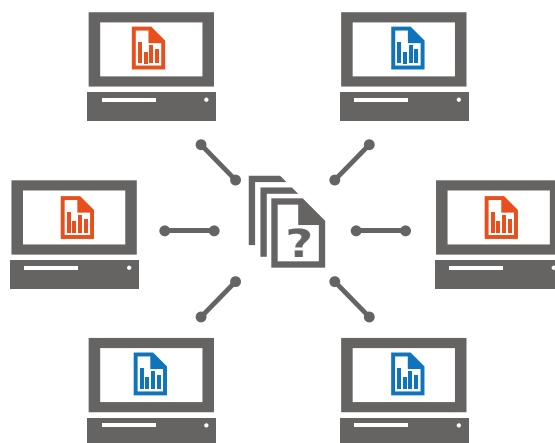
A block is created by grouping similar transactions together. These blocks are added in chronological order, in a way that resembles a chain, hence the name blockchain. The nodes then store these new blocks on the local blockchain database on their computer or server.

What about conflicting data entries?

One node may receive two pieces of mutually conflicting data. For example A is, "I sell all my shares to Alice," and B is, "I sell all my shares to Bob." Each node will have to keep one and reject one as they cannot both logically coexist.
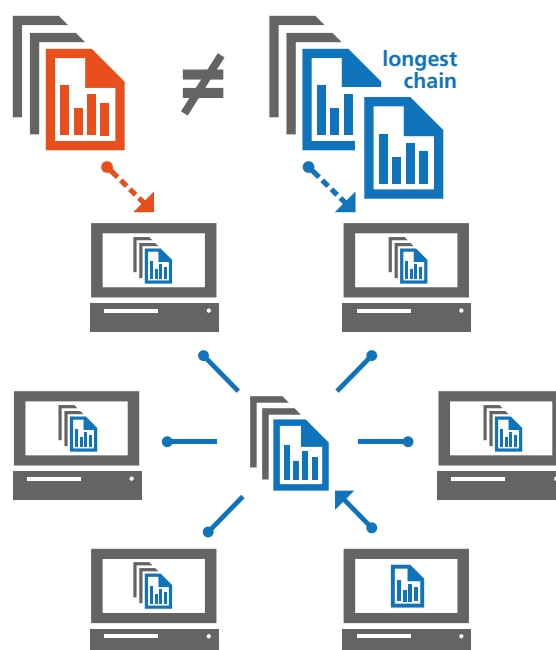
An intuitive solution is for nodes to act on time priority, keeping the first and rejecting the second. However different nodes may hear the messages in different orders. The messages will propagate and some proportion of the network will believe A has happened (and B hasn't) and the rest of the network will believe B has happened (and A hasn't). The network is in an unstable state. ▶

▶ How is this resolved? Each node is working on its own version of the truth. Whichever node gets to add the next block will propagate its version of events, and all nodes will read this and act on the new 'truth'.

What about conflicting blocks?

Across a network, there is a possibility that two different blocks are added at the same time by different nodes, creating a fork in the chain. In this case, there is a 'consensus rule' that helps nodes figure out which is the block they should believe. In bitcoin, the rule is called the 'longest chain rule' – each node acknowledges the legitimacy of both contender blocks and the situation resolves when the next block is built on one of the contenders. The longer chain becomes part of the de-facto blockchain.

Public Versus Private Blockchains

Bitcoin blockchain is the grandfather of public blockchains

One of the breakthroughs of bitcoin was the ability to maintain a consensus view of transactions in a system, where anyone can create and send transactions, and anyone can write blocks of transactions to the ledger – all without needing the permission of higher authority. The bitcoin blockchain is the grandfather of public, or 'permissionless' blockchains – anyone can write data to it just by running some free software, and without signing up.

Conversely, private blockchains limit the participants using traditional methods, such as private networks with firewalls and IP whitelisting. A private blockchain can be set up so that known entities can add data to the blockchain, without letting external entities read or write access.

In finance and trade, in general, we have a set of known entities who are trying to legitimately do business with each other and who don't have a problem with revealing their identity. The issue before blockchains is that they may struggle to reach a common understanding of events. To solve that, they have always used third parties, such as banks and escrow services, which then involve a high amount of risk, or avoid the situation altogether.

Difference between public and private blockchains

Public blockchain, e.g. Bitcoin	Private blockchain
Anyone can write	Limited set of known entities can write
Anyone can read	Read-access is configurable

Smoother information flows

So what is the difference between a private blockchain and existing third party systems? Blockchains can replace the need for data to flow from institutions to the third party and back. Instead, data flows between known institutions and comes to a consensus within a short period of time. This means that all parties can work from a single, known state of events. Encryption keeps private data private and digital signatures ensure authenticity, data integrity, and non-repudiation. Blockchains can solve the problem of needing to trust third parties.

From Bitcoin to Blockchains: A Brief History

Bitcoin

The first widely known and discussed blockchain was The Bitcoin Blockchain, and it serves as the de-facto example of how blockchain systems can work. The Bitcoin Blockchain is a database file that sits on thousands of computers worldwide, where the individual copies are kept aligned through the rules of the Bitcoin protocol. The Bitcoin Blockchain file (actually it is a series of files, because large files are difficult to manage) contains a list of every single bitcoin transaction that has ever happened: it is the ledger of record for Bitcoin and has been growing since January 2009.

The Bitcoin Blockchain is an open or 'permissionless' database. That is, should you wish to write entries to the database you may do so without signing up, logging in or asking permission from anyone in charge. In practice, this is done by downloading some open-source software and running it. By doing so, your computer will connect over the Internet to other computers running similar software. The software lets you start sending and receiving bitcoin transaction data with neighbours, and allow you to add data to the bitcoin blockchain, by playing a computationally intensive lottery known as 'mining'.

By studying The Bitcoin Blockchain file it is easy to see which bitcoin account has how many bitcoins and which accounts are sending bitcoins to whom. This transparency is needed so that the validators of the transactions determine whether a transaction is legitimate or not. For example, a bitcoin transaction that pays someone using bitcoins that don't exist would not be considered valid.

Other Blockchains

There are currently thousands of public and private blockchains running at the moment, however many of them have no significant uptake. Public systems built with blockchain technology that have gained prominence include Ripple, NXT, and Ethereum, which we highlight to explain the differences between the types of platforms that currently exist. There are many more under construction as the industry takes shape.

Ripple

Aims to dematerialise currencies and assets

Ripple sits somewhere between the public and private platforms and has a heavy reliance on validating nodes controlled by Ripple Inc. It aims to dematerialise currencies and assets by having customers park real-world assets with guardians called 'Ripple Gateways' who would issue tokens against the assets, just as goldsmiths issued receipts against gold deposits. The tokens can be sent between anyone with a Ripple account, traded for other tokens, and finally redeemed by sending them back to the guardian in return for the real-world item.

NXT

Uses 'proof-of-stake' as a
block-adding mechanism

NXT is a public platform whose genesis block was created in November 2013. It works with a slightly different block-adding mechanism to bitcoin called 'proof-of-stake' instead of bitcoin's energy-intensive 'proof-of-work'. 'Proof-of-stake' distributes mining rewards in proportion to the balance of your account, as opposed to in proportion to how much electric power you are expending. The NXT platform includes more functionality than just sending tokens around (to date it has messaging, new token creation, new asset creation, a decentralised exchange, and a marketplace).

Ethereum

Its network acts as
one giant consensus
computing machine

Ethereum is a public platform and takes distributed computing one step further. The Ethereum network acts as one giant consensus computing machine instead of just a giant consensus database. The computations it is capable of are 'Turing-complete' meaning that it can calculate anything that any other computer can calculate, just a lot more slowly.

Ethereum's genesis block launched in July 2015 and the platform is currently one of the leading platforms for permissionless smart contracts. ✖

'*The Bitcoin Blockchain file contains a list of every single bitcoin transaction that has ever happened since January 2009*'

✖ DBS

When Blockchains Can be Used

Blockchains have yet to find their niche for single entities where data governance is under one structure as general databases perform adequately. However, we see a role for blockchains when there are concerns around rogue employees, more secure logging (for any application), and also where regulators want to "plug in" to institutions to validate and see transactions in real time.

Fraud prevention

For example, currently system administrators with the right level of access can alter a database, and then modify log files to remove all traces of their activities. In the case of a distributed database running with nodes in separate data centres, a system administrator would need to have access to each of the data centres to make a change to an organisation's blockchain – a significantly harder task.

Improve National and Corporate Governance

Blockchain systems have a lot more potential between entities, i.e. where entities need to work with other entities to achieve a common goal. This is due to governance: Within an entity, bosses and the traditional hierarchy can mandate a golden source of truth and resolve conflict. However where entities interact, there needs to be another method for conflict resolution. The potential for blockchains to add value is higher if used collaboratively across an industry or a workflow.

Reduces risks of double invoicing

It can protect the interests of entities within a nation if used appropriately, for example in invoice financing – if banks within a country can share data (without necessarily revealing the data to each other) about invoices that have been factored, then certain double invoicing scams can be avoided. Looking further afield, if an invoice can be issued on a blockchain by the issuer and signed, then you have a guaranteed unique digital record of the invoice that cannot be copied and cannot be financed more than once.

Replaces centralised registries

As Singapore looks to build a smart nation, blockchains can replace centralised registries with decentralised ledgers. With political will, Singapore can lead the way in creating trusted, tamper-proof repositories. Share registries, property, assets, insurance, and national identity can all be stored in secure blockchains, allowing for easier verification of "the truth", reduce settlement times when assets change hands, and by using smart contracts, even automated title transfers could be done when specific parameters are met. Digital identities can be used across systems without systems necessarily touching or interacting. One blockchain for identity, that is validated against when needed, and with the user in control of which data is shared with the merchant.

Storing national currency

One of the most exciting advances would be for a national currency stored on a blockchain, enabling seamless payments that are much more secure and privacy-aware than credit

cards. Disassociating the transmission of personally identifying information with the transmission of the payment would be a huge improvement over traditional systems.

Streamlines backoffice operations

Additionally, with smart contracts, logic can be written into accounts enabling payments to occur automatically when triggered by events. No longer will we need to rely on operations departments to follow straightforward "if this, then that" rules, and no longer will we need to chase down people who renege on a financial commitment. A smart nation would have front doors that unlock only if the rent has been paid, and have assets that automatically settle according to digital wills, reducing the need for costly probate.

Helps Facilitate Intra Asia Trade and Capital Flows

We believe that blockchains have the greatest potential to increase productivity in Asia if applied regionally, as opposed to constrained within a country or entity.

Before blockchains, we needed to trust entities. With blockchains, trust is assured by mathematics and systems instead. In a region where trust in entities, including companies and governments, is low, blockchains have the biggest potential for impact.

Spur regional trade

While attempts have been made to increase trade within the region, one of the biggest drags to success is low levels of trust in both businesses and political regimes. In Asia, this lack of trust has led to maintaining supply chains with known entities, where changes to the status quo are limited due to the risk of using new suppliers. New business relationships are slow to establish and often based on family ties and introductions by mutual trusted parties. By establishing digital credibility on an open system that is known to be fair and not under the influence of any politician, perhaps this can provide the lubrication that businesses need to open up.

Promote cross border investments and financing

Another example is in lending. Currently, the region has a huge amount of value tied up in assets such as buildings, plant, machinery, etc. If these assets could be recorded and verified on an independent ledger, outside the control of any specific third party or government, then loans can be made against the assets, releasing financing where previously it was impossible. In the initial stages, a blockchain could record ownership and changes of ownership of assets, but in the future, the financing leg could also live on a blockchain.

Other potential use cases for blockchains that have been discussed in the media in the fields of international trade finance, besides being used as decentralised collateral ledgers, are for the creation of decentralised exchanges. Uses outside finance are also being explored, for example digital identity, voting registers, proof of ownership, and tracking items in supply chains.

Although this proliferation of blockchain start-ups is encouraging, the technology is new and immature. The applicability and viability of blockchain solutions to these business problems, from

both the technical and commercial perspectives are yet to be proven. The concept of decentralised or 'trustless' ways of working are seductive to those who are skeptical of powerful entities; however we are accustomed to the comfort of being able to assign liability when things go wrong. When something perceived as unfair or immoral happens, having no organisation to blame or sue will be a good test of our appetite or society's appetite for autonomous organisations.

Hurdles for Adoption

Blockchains are not without their hurdles. Although we believe that the most value would come from blockchains that can share data over national borders, we also recognise that this is also the hardest to achieve without substantial political will and collaborative effort from all parties involved.

Total transparency a double-edged sword

Are we ready for blockchains? Often within organisations, whether businesses or governments, the ability to tweak historical data is a comfort blanket that may not be happily or easily forgone. Total transparency is somewhat of a double-edged sword. The demand for change here will come either from the grassroots demanding that certain data go on a blockchain and form a record which cannot be subsequently edited, or from regulators and policymakers mandating such change.

Requires a lot of coordination

Having said that, blockchains are not just about transparency. Blockchains can also be used in industry platforms for the sharing of data that is helpful to the industry as a whole. In this case, a majority of players in an industry needs to come together and agree on what such a platform would look like, who would pay for it, and what value each participant would get from it. This isn't something that can be done overnight, and it is not a cheap exercise.

Costly to switch technologies

Switching technologies also cost money. In any bank there are legacy systems that are old and inadequate, yet the cost/benefit of replacing the system doesn't make sense. Blockchain solutions will need to have a clear business case before being adopted outside of pet projects.

Regulatory clarity over data sovereignty

Regulatory clarity of on- and off-chain assets is something that is often discussed, in the context of bitcoins and the issues of data governance of a share certificate on a blockchain. What is often neglected is regulatory clarity over data sovereignty. In an industry blockchain, the same data is copied over many data centres, often in different countries. A lot of the data are encrypted so that only the intended recipient can see it.

In some industries this is fine, but in financial services, control of data is heavily regulated. Are banks comfortable sending, receiving, and storing data without knowing exactly what they are storing in their data centres? Are regulators comfortable with banks in their oversight storing unknown, encrypted data? Are banks comfortable with their competitors storing their data, encrypted or otherwise? After all, a blockchain replaces a trusted third party with a network of participants but in the case of an industry blockchain, many participants will be competitors.

New-ness of
blockchain technology

Finally, the technology needs to clearly prove itself before conservative businesses take the plunge. We are still in the early stages as the technology is still immature and hasn't yet been proven at scale. In many of the situations outlined, data volume, transfer speed, and consensus speed will need to be increased significantly for this technology to prove useful given bitcoin is adding just up to 1 megabyte of data every ten minutes. ❌

25

Conclusion

Much of the thought leadership regarding blockchains in financial services has focused on the context of Western Europe and the US but little has been explored within Asia. This is ironic given in the US, trust across state lines is high and uniform; in Europe, the market is more closely aligned by regulation. But Asia is still behind in terms of levels of trust enabling greater economic activity. Asia's geopolitical context is unique globally – the region consists of loosely coupled countries who want to trade with each other, yet levels of trust between countries are disparate, preventing the region from realising its potential.

We believe that the most transformative blockchains will be those that can work across geopolitical boundaries. Southeast Asia has the most potential that can be unlocked with this technology, but we acknowledge that it may also be the hardest blockchains to implement.

We now have the technology for trust. With political will, investment, and industry collaboration, we believe that blockchains can improve the way business is done in Southeast Asia and increase economic prosperity as a result.

Living, Breathing Asia