



Blockchain: what is it and how will it impact your business?

Blockchain: what is it and how will it impact your business?

Over recent months, the financial services sector has been abuzz with discussion around the transformative potential of blockchain, the danger of Bitcoin, and the significant investment that the sector is receiving.

In 2015 over US\$1bn was invested in Bitcoin, blockchain and associated technologies,¹ with major investments in time and resources from banks, corporates and major software firms. With media coverage across all major publications and focus pieces from *The Economist*,² the *Financial Times*³ and others, the blockchain conversation has moved mainstream – certainly in terms of management time and media attention. This article aims to provide an overview of the basics of blockchain, an insight into its applicability to major corporate and financial institution clients, and how it could affect your business in the medium and long term.

A blockchain is essentially a shared database for recording transactions, cryptographically chained in a way that does not allow the record to be altered at a later date, and can be shared more easily between parties. Depending on its design choices, the blockchain can be very open and decentralised (permissionless), or a more closed system with controlled access points (permissioned).

This article agrees with much of the recent consensus around blockchain within firms and the media; the attributes of the technology behind Bitcoin have significant transformative potential for the financial services sector, government and industry. However, it is unlikely that Bitcoin will be transformative in its current guise.

Nevertheless, any financial institution or corporate function that relies on large data pools – that need to be updated constantly, securely, and agreed upon by multiple parties – might consider a blockchain solution, while remaining aware that a 'blockchain' isn't the solution to all ills. Clients should ask: *could a traditional database be used, and is the immature nature of blockchain technology really appropriate?*



Key senior management questions:

What is the **basic technology** and terminology that I should know?

What does this mean for me? What are the **key characteristics** of blockchain and the problems it solves?

When will blockchain be likely to affect my business?

What is the **likely outcome for the Bitcoin blockchain**, and what are its strengths and weaknesses?

What are the key benefits for my business?

What are the likely **use cases for blockchain** in financial services and the wider world?

Who are the major players I should be aware of and track?

How can I **future-proof** my business to blockchain changes?

For further detail, please refer to the report by the UK Government Office for Science, "Distributed Ledger Technology: beyond block chain"⁴

¹www.money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/

²www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

³www.ft.com/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.html#axzz3yNdThQil

⁴www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Blockchain technology

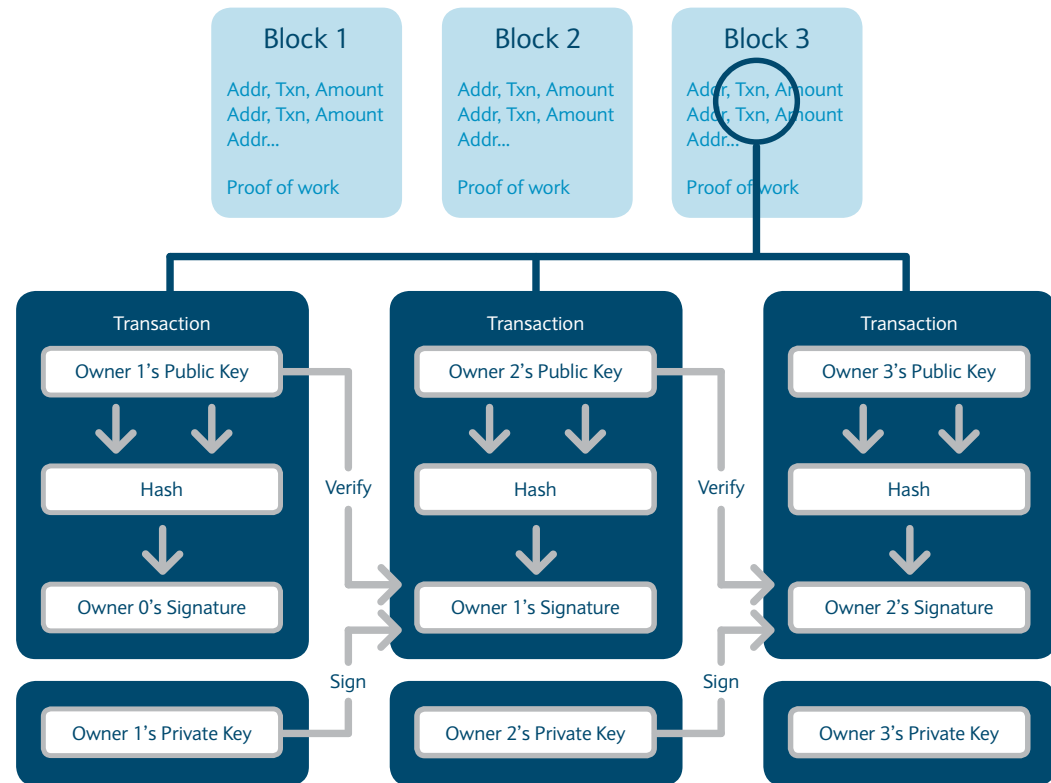
It is impossible to discuss the development of blockchain technology without quickly discussing its first major experiment – the Bitcoin blockchain. Bitcoin is, at its core, a digital representation of value. It was designed as a system to allow the **censorship-resistant** movement of value between counterparties, without the need for either trust, or a third-party entity. The Bitcoin blockchain is an interesting computer science experiment but we contend that there are a few fundamental flaws with the Bitcoin blockchain that make its widespread adoption unlikely by the financial system. Nonetheless, the underlying principles of Bitcoin are useful.

In short, the Bitcoin system creates a record or ledger (essentially a huge spreadsheet) that all validating nodes have copies of. The ledger records all previous valid transactions of Bitcoin which are cryptographically signed by the sender to move the asset via their wallets. Each wallet-holder submits new transactions to the network. Consensus (which can be thought of as settlement, but this is a complex area) on average takes around 10 minutes, but can be as fast as a few seconds and as long as an hour, depending on processing power and load. The system rewards the validating nodes (miners) via a financial reward and, therefore, records and validates all transactions that have been submitted by Bitcoin wallet-holders. This process creates a **consensus mechanism** that makes it extremely hard to force the blockchain to be rewritten at the time, and near impossible to overwrite the past, as it would take the same amount of processing power to undo as to write.

What is blockchain (the technology)?

- ‘Chaining’ is a database technology that dates back to the 1980s
 - Think of a chain of transactions like a physical chain; links are added one at a time. Just like a real chain, if you pull one of the previous links out, the whole chain breaks
- The ‘block’ refers to a block of transactions.

A blockchain is therefore a database, that you can only ever add to.



Source: www.blockchain.info

Weaknesses in the Bitcoin blockchain

- Data privacy – everyone can see exactly what you have done on the Bitcoin blockchain, provided that they know your wallet address
- Anonymity – wallets are by definition pseudonymous, which creates challenges for KYC, AML and financial crime controls
- Governance around core development is undefined and unregulated
- Validating nodes (miners) are in a variety of locations globally, and of varying risk categories
- Lack of consumer protection – once an asset is stolen, there is no way to overwrite code or refund money
- Speed of settlement – currently between 10 minutes and several hours
- Energy usage has been variably estimated to be somewhere between 250MW and 1GW⁵, which, per transaction, is enough energy to fuel around 200,000 US houses, or roughly 1.6 US households’ daily energy consumption per transaction.⁶

Extensions to the Bitcoin concept

It is worth noting that the Bitcoin blockchain concept has now been amended in a number of ways. First, companies attempted to address perceived weaknesses by forking Bitcoin; then companies built their own versions constructed from the same concepts that further addressed technical weaknesses. This evolution is continuing over time.

Without going into a full description of the market, versions now exist on a spectrum from centralised current payment and clearing systems, to fully permissionless systems with pseudonymous users such as Bitcoin. Alternative systems include Ripple, which uses both financial institutions (and its own nodes at the core) as the transaction processing entities, and Ethereum – which, like Bitcoin, uses a global permissionless blockchain but solves some speed problems of Bitcoin, but retains challenges, and perhaps does not answer questions of integration with the financial system.

The weaknesses of the initial Bitcoin project as a system to be adopted in mainstream finance inform a number of senior management recommendations, and the likely development of the technology in the next few years.

Attributes that make blockchain useful

This technology provides four major characteristics that are useful for finance as well as for other applications:

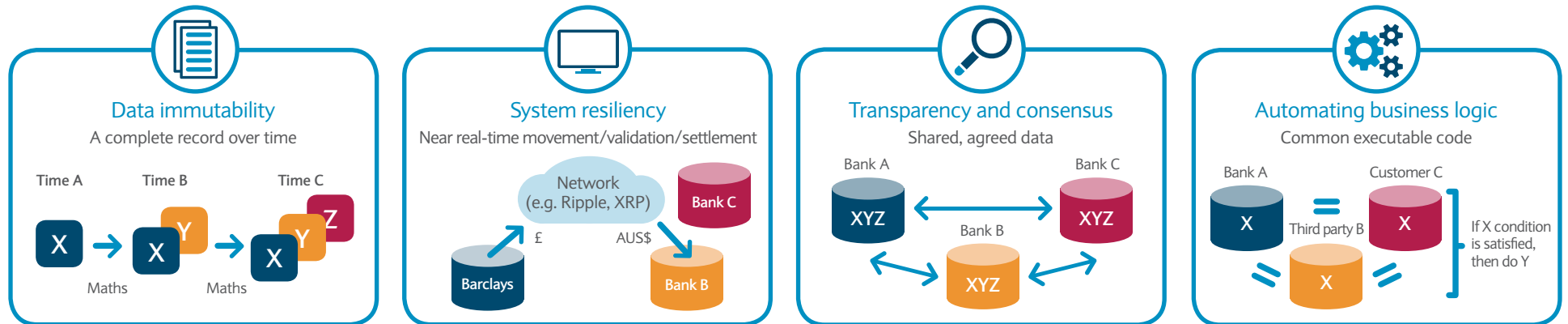
- **Data immutability:** a complete record over time – guaranteed by the tamper-proof mathematical process of ‘hashing’ previous blocks together
- **System resiliency and speed:** real-time movement and settlement of assets registered, provided by the distributed nature of processing – many copies, not relying on one node
- **Transparency and consensus:** shared, agreed data
- **Automating business logic:** ability to write code into the database that will execute if certain conditions are met, i.e. smart contracts.

Executives should ask if a potential use case needs one of these characteristics to be successful – if not, a traditional database may be a better solution.

⁵www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf


⁶<http://motherboard.vice.com/read/bitcoin-is-unsustainable>

Attributes that make blockchain a big deal



Case studies around core attributes:


Wave – trade finance


 Data immutability

 Transparency and consensus

This use case takes cost and operational burden out of the trade finance system, by dematerialising the official trade documents and other documents used for trade that provide commercial, fraud, and AML risks, and then sends these directly between parties involved in the transaction, transferring the title over a private blockchain that only the signed-up carriers and banks can see. There is the potential to save huge operational costs, increase speed, and reduce risk of trade finance.

Identity

 Data immutability

 System resilience

 Transparency and consensus

Key requirements – data privacy, validated information, ownership by the individual, linking to a defined device.

By placing⁷ identity onto a decentralised ledger system, significant opportunities are presented in cost reduction, portability of data, security of data, and the ability to improve financial institution AML and KYC processes. Significant possible benefits also arise for financial inclusion and Third World personal security.


⁷Placing' could be conducted by hashing documents to a chain, and linking to a mechanism controlled by a private key.


⁸www.bloomberg.com/news/articles/2015-12-30/nasdaq-seeks-to-show-progress-using-much-hyped-blockchain

⁹www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329

Capital markets – R3 and distributed ledgers

 Automated business logic

 Data immutability

 System resilience


 Transparency and consensus

One of the most frequently discussed areas which could be prime for upgrade by distributed ledgers are capital markets. The R3 consortium and the Digital Asset Holdings group are both targeting this area. Key to these use cases is not blockchain per se, but rather the establishment of common rules and architecture for transactions made at speed between financial institutions, and the reduction of costs.

Some of the use cases currently underway include asset registries for securities (NASDAQ has already conducted a trial with a number of private firms' shared registries stored on the Bitcoin blockchain⁸), the ability to automate functions such as margin calls on derivatives using smart contracts, as well as a number of other asset settlement and registry functions. A further use case, and one of the mantras that arose at the most recent SWIFT Business Forum, is the virtue of reconciliation using blockchain technology. It is, however, likely that common standards on such technology will be established and then rolled out to the financial system; perhaps this threatens some of the central counterparties and custodians, but is unlikely to affect the broker dealers and traders at the start, beyond a cost reduction and efficiency improvement. We also note the public announcement of the Smart Contract Templates prototype, spearheaded by Dr Lee Braine from Barclays Investment Bank's CTO Office. The proposition links legal prose with business logic to simplify the legal documentation processes.

Large value payments

 Transparency and consensus

 System resilience

AML concerns, financial architecture, and adoption by the banks are major issues.

The Bitcoin blockchain is not appropriate for large value payments replacing the current SWIFT messaging system; we judge it more appropriate for other use cases. However, blockchain technology does have the potential to enhance the current clearing and settlement systems, with SWIFT and CLS looking closely at blockchain systems to improve the current architecture. The use of shared ledgers with data tracking and consensus holds the potential for a massive reduction in the time of settlement, AML controls and cost.

Focus: R3 banks consortium activity

An interesting use case for large value payments and settlement between banks was highlighted on 20 January 2016 by the R3 consortium. 11 global banks, including Barclays, have united to conduct trials of instant settlement across continents. Most recently, on 3 March 2016, the R3 consortium announced that 40 banks had trialed commercial paper trading. While these trials are linked to capital markets trials at present, the technology (running over the Ethereum blockchain, hosted on the Microsoft Azure Cloud) does present a quicker than expected test of such technology. In addition, R3's distributed ledger, Corda, was successfully demonstrated for the first time at the Barclays Accelerator programme's public demo day via the Barclays Smart Contract Templates proposition.⁹

Small value payments

An area ripe for disruption is the archaic system used to move money globally. A global blockchain gives the possibility of true, instant P2P payment without relying on money parked around the world. With the right controls, Bitcoin firms could be candidates for small retail payments; however, regulation and control of on and off ramps remain a challenge.

Readers may wish to study Circle Internet Financial as an example of how user experience can be transformed in small value payments using an underlying 'internet of finance'. Barclays has a relationship with Circle, allowing it to develop a more mature understanding, along with the use of technology such as Chainalysis. However, for Bitcoin to be adopted at scale, it needs to professionalise, evolve and mature – which it has not done as yet.

The regulatory environment

Discussion of the regulatory environment could cover many hours, and multiple pages. For now, it is instructive to be brief. In New York, a strict regime under the BitLicense has been established, with a more certain environment created for US firms. Companies are becoming licensed, working within the rules set, and starting to become regulated.

The Bank of England has begun discussions on the design of a digital sterling.

In the UK, a number of think pieces and calls for information have been published. It appears possible that the Government will write legislation in Parliament to bring cryptocurrencies in line with regulations such as eMoney and, therefore, provide building blocks for regulation. The Bank of England has begun discussions on the design of a digital sterling, and Project Innovate at the FCA is positively encouraging applications.

Recently, China has appeared to be softening its view on cryptocurrencies with discussion of a digital RMB; this could help their global trading strategy, and the internationalisation of the currency. Japan has recently asked a number of industry players to assist in the development of a FinTech strategy and view. Industry discussion suggests that, far from the Mt Gox debacle, the Japanese regulator is encouraging certain firms who wish to establish in Japan.



Predictions for senior management

To conclude, I will now try to answer the key questions senior management may be asking when attempting to future-proof their business.

When will blockchain be likely to affect my business?

We expect some limited encroachment of small value payment systems (likely based on Bitcoin) to ramp up throughout 2016, but this is likely to be a very small proportion of volume and could be hampered by the technological development of Bitcoin. It is possible that only large and regulated firms will succeed in this sector, with many participants remaining cautious. We expect that 2016 will continue to see small trials within banks on wider technologies, with little market adoption.

Major effects are more likely from market counterparties and governments moving faster than small start-ups. Organisations such as DTCC, CLS and SWIFT appear engaged in blockchain discussions, and may update their systems and processes in response to the challenge. Bank consortiums with smaller iterations of blockchains tied to real currencies and assets are possible in the next 12 months, but are more likely to become a reality over a three-year time horizon. More likely in the short term is the use of private blockchains to store and move data on specific use cases such as trade finance start-up Wave, which aims to dematerialise bills of lading onto a blockchain – this is possible in the next 12 months but will require adoption and scale.

Over the next three to five years, we expect market infrastructure in capital markets to begin to be updated, with settlement and clearing infrastructure being amended and challenged. We expect that this change will be driven by both disruptors and large incumbents. At present, partnership and collaboration are the main watchwords in FinTech.

What is the likely outcome for the Bitcoin blockchain, and its strengths and weaknesses?

We have answered much of this in the earlier section, but whilst Bitcoin has significant flaws in its processing capacity, energy usage and pseudonymity, it is the largest and most liquid digital currency. It might be most useful for tracking and storing assets using 'coloured coins', which then refer to other assets stored off-chain, such as diamonds in the Everledger business model on an immutable chain.

Bitcoin remains liquid, global and well supported. With governance changes, it could retain popularity, and thus immutability, and find a long-term role for small value transfers and asset tracking.

Who are the major players that I should be aware of and track?

There is a large universe of Bitcoin and blockchain firms and consortia, but for ease we suggest tracking:

- The UK Government. The recent Government Science Office report is very helpful
- Ethereum. A blockchain 2.0 concept, behind many recent tech developments and usages
- R3. The consortium of UK banks
- Corda. R3's distributed ledger for recording, synchronising and managing financial agreements
- Digital Asset Holdings
- Hyperledger Project. A global collaborative effort to identify and address the key features for a cross-industry open standard for distributed ledgers
- Circle Internet Financial. A blockchain social payments company
- SETL. An institutional payment and settlement initiative with a blockchain infrastructure

- Everledger. A permanent ledger for diamond certification and related transaction history
- Tallysticks. An immutable record-keeping framework with smart contract functionality, automating the invoicing and invoice financing processes
- Wave. A peer-to-peer and entirely decentralised network, connecting all parties of the international supply chain, allowing the direct exchange of documents
- Chainalysis. Allows financial institutions greater insight into movements on the Bitcoin blockchain for AML and other purposes. Barclays' use of Chainalysis has allowed us to monitor and understand companies leveraging the Bitcoin blockchain.

Please note: Barclays neither promotes nor endorses the aforementioned parties; the above list is not exhaustive.

How can I future-proof my business to blockchain changes?

Financial consortia are more likely to make a major impact on the financial system than individual start-ups, with developments from networks and consortia more appropriate to track and follow. However, Bitcoin and digital currencies retain the ability to disrupt and challenge cross-border small-value payments and areas such as identity. Closely tracking and working with major players will assist in this area, while challenging current business models on small value payments and FX.

There are also a series of London-based start-ups and academic groups which are examining amendments to settlement systems and payment platforms.

A true advantage to banks and corporates is likely to come through cost reduction and an increase in efficiency provided by market infrastructure.

About the author



George Osborne
Innovation Director
Financial Institutions Group

George Osborne is Innovation Director for the Financial Institutions team within Global Transaction Banking at Barclays. He is charged with ensuring that the best of Barclays' innovation work is brought to bear for clients, and works closely with innovation functions across the bank. He has been a mentor on the Barclays Accelerator programme and is leading on a number of areas in Barclays' positioning for new sectors within FinTech.

George has previously managed banking relationships in the FinTech and Financial Intermediaries teams, where his interest in strategic innovation and disruption was developed.

George is studying an Executive MBA at the London Business School.

Key takeaways

- The blockchain conversation in the industry has now moved mainstream, but remains very early stage
- The Bitcoin blockchain has introduced interesting concepts, but has weaknesses that likely prevent widespread adoption for large financial transactions
- As long as there remains a financial incentive, the Bitcoin blockchain is a useful system of record that can be used to write code or assets to. It is so far immutable, with a relatively long-term record
- The technological development of a transaction, signed by two or more users cryptographically, and then stored in a shared immutable record, is the key underpinning element. Technical development, coding and common standards are the next step
- The attributes of shared ledgers have many applications where multiple entities need to share data, act on it and move assets at speed. Cost is the biggest driver but it will not be quick; architecture and design of a system is the challenge at present
- In the long term, firms will be interested in the characteristics of a blockchain (i.e. system resilience, data immutability, transparency and consensus, etc.). A key example is in smart contracts which provide the automatic execution of formerly manual tasks, only executing when pre-determined conditions are met or when data is changed by permissioned parties; this opens the door to effective implementation where multiple counterparties are required to provide data in order for a contract to be enforced (e.g. mortgages, investment vehicles, billing/tariff contracts, letters of credit, etc.)
- We do not expect blockchain technology to largely impact our corporate clients over the next three years. In the next 12 months, we anticipate seeing limited encroachment in the smaller payments space, as well as the use of private blockchains to move data for specific use cases. Over the three-to-five-year time horizon, we envisage the updating of market infrastructure in capital markets and possibly payments and data applications.

barclayscorporate.com

Every attempt has been made to ensure that the information provided is accurate. However, neither Barclays Bank PLC (“Barclays”) nor any of its employees makes any representation or warranty (express or implied) in relation to the accuracy, reliability or completeness of any information or assumptions on which this document may be based and cannot be held responsible for any errors. No liability is accepted by Barclays (or any of its affiliates) for any loss (whether direct or indirect) arising from the use of the information provided.

Barclays is a trading name of Barclays Bank PLC and its subsidiaries. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register No. 122702). Registered in England. Registered number is 1026167 with registered office at 1 Churchill Place, London E14 5HP.

July 2016. BD02530.

