

Blockchain and Fintech

A USER GUIDE ON BLOCKCHAIN

BY DAVID REILLY

LETS LEARN
DIGITALo

LET'S LEARN DIGITALo

Contents

About the author- David Reilly	3
About this Guide	4
What is the Blockchain?.....	5
How Blockchains works	7
The significance of Satoshi's Bitcoin paper	9
How Blockchain enables trust and transparency	11
What does a trusted Blockchain enable	15
Blockchain in the Fintech/ Investment sector	19
Implementing Blockchain- the spectrum of decentralisation	22
The Future of Blockchain in Fintech	24
References	25
Blockchain Jargon Buster	26

LET'S LEARN DIGITALo

About the author- David Reilly

David Reilly is an entrepreneur, technologist and writer on emerging technologies.

He is also the founder of emerging technology training company Let's Learn Digital, Let's Learn Digital has a vision to deliver learning experiences, workshop training and programmes in the emerging technologies which are reshaping the financial services sector including Blockchain, Artificial Intelligence, programming, Data, Virtual Reality and Cybersecurity.

In addition, David provides consultancy around the intersection of technology and business which includes a mix of speaking, writing and digital transformation.

LET'S LEARN DIGITAL_o

About this Guide

This blockchain User Guide is designed and written for financial intermediaries, investment and financial advisers, trust fund managers, fintech professionals and wealth managers seeking a clearer understanding of blockchain technology's potential and why it has been chosen as the underlying technology for Royal Mint and CME's exciting new digital gold standard RMG launching Q4, 2017

We hope this guide will serve as a valuable resource for investment professionals seeking to understand about the unique attributes which blockchain offers as an alternative trading option to purchase physical gold bullion.

It represents the first stage of a series of blog posts and education based content published by the Royal Mint.

We hope you find it valuable and welcome your feedback

LET'S LEARN DIGITAL

What is the Blockchain?

Welcome to the new world of trading on a blockchain platform.

At its core blockchain is a peer to peer technology platform that enable assets of value to be traded without the need for a third party intermediary. It uses software algorithms to record all events reliably and anonymously providing a permanent record of transactions that cannot be easily erased. This technology is also sometimes referred to as 'distributed ledgers' (DL), 'cryptocurrencies' the electronic currencies that first engendered it or 'decentralized verification' which refers to the key differentiating attribute of this type of system. The recent Financial Conduct Authority (FCA) blockchain guidelines referred to blockchain technology as 'distributed ledger technology' The term block-chain emerged as the underlying technology out of the peer to peer digital cash Bitcoin the history of which we describe in more detail in Chapter 3 on page 7

Blockchains are especially significant for trading because they defy legacy systems and challenge the traditional governance, in this case trading gold, which has existed for hundreds of years. Most importantly blockchains challenge the costing models of trading via a blockchain enabled platform which make it a highly attractive investment alternative. Competitive trading on blockchain removes the traditional completion fees costs and ever increasing storage costs thus deterring many investors from considering gold as suitable investment option.



"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

Don & Alex Tapscott, authors Blockchain Revolution (2016)

Another critical benefit of this technology is how it enables trust. Blockchain embeds complete trust into its architecture which we explored in further detail in chapter 4. Trust has eroded since the 2008 global crash and further compounded by increasing frequency of data breaches and at the time of writing the recent global computing hacking of global IT networks. In 2017 the need for greater resilience in IT systems infrastructure to enforce trust has never been more critical to business transactions. Blockchain technology offers an incredible amount of resilience for the corporate business.

LET'S LEARN DIGITAL

Because blockchain verification is handled through algorithms and consensus among multiple computers rather than people there is no single point of failure unlike how bank systems which deploy cloud based services that have with increased frequency been compromised. Blockchains keep provide a trusted secure and robust backbone of trusted infrastructure

But blockchains should not be viewed by prospective investors reading this guide as simply a decription of a new technology platform. It is a type of technology that challenges other existing ways of doing business because it has the potential to replace or supplement existing practices and provides a level of unsurpassed resilience and irrefutable trust. Let us firstly examine how they work in practice to fully understand their potential

LET'S LEARN DIGITAL

How Blockchains works

The blockchain is a distributed database that can be shared across a network of multiples sites, geographies and institutions. Visualise in your mind a giant, global spreadsheet that runs on millions of computers which is distributed and open source, so anyone can change the underlying code, and they can see everything that is going on. This makes it a truly peer to peer and open type of technology which doesn't require powerful third parties like banks to authenticate or to settle transactions.

How a blockchain works

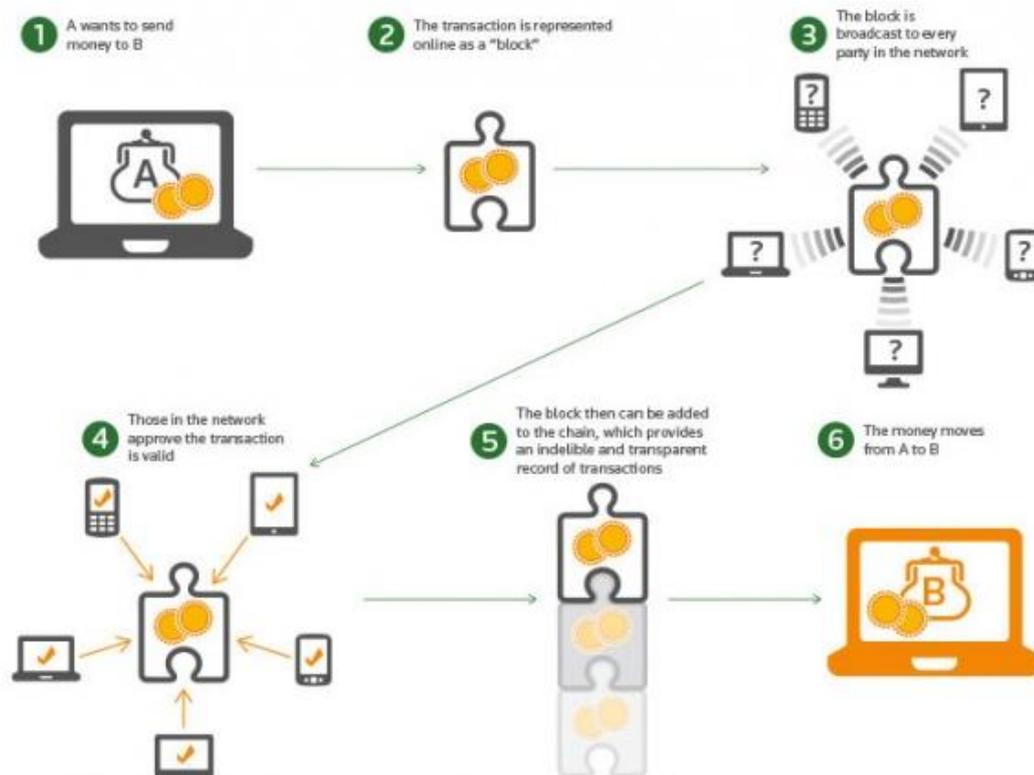


Fig 1: Source: The Financial times, weforumblog

Blockchains are also the latest example of the unexpected benefits of cryptography. Cryptography is defined as a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Simply explained mathematical scrambling is used to boil down an original piece of information into a code, known in cyptocurrecnry as a hash. Any attempt to tamper with any part of the hash or blockchain records is apparent immediately to everyone in the network because the new hash will not match the old ones.

LET'S LEARN DIGITAL

In this way a science that keeps information secret is vital for encrypting messages and online shopping and banking is, paradoxically, also a tool for open dealing. Thus a hash can be described as a unique finger print that helps verify that a

certain piece of information has not been altered, without the need to actually see it. In most blockchain structures keys are used in at least a combination of two; a public and a private one. For example imagine a door needing two keys to open it; the public key used by the sender to encrypt information that can only be encrypted by the owner of the private key. Royal Mint new Gold product have refined this protocol to add an additional layer of reinforced security process which we will explain in further detail on page 11

Conceptually, a blockchain can record and be applied to any structured information, not just who purchased gold from whom at what time but also who owns what property or what light power from what power source. Blockchain is also an immutable, unhackable distributed database of digital assets. This is a platform for truth, or as the Economist have described it in October 2016 famously labelling it "The Trust Machine".

Most blockchains to date are what is called permission-less systems. We can do transactions and satisfy each other's economic needs without knowing who the other party is and independent from central authorities. These blockchains all have a digital currency of some kind associated with them, which is why everybody talks about Bitcoin in the same breath as the blockchain, because the Bitcoin blockchain is the largest and most well known.

The great innovation about the blockchain is that it will enable an increased amount of people and businesses to trade more frequently, efficiently and transparently significantly boosting local and international trade. You can reasonably assume that those companies which get to grips with blockchain first will reap the trading benefits once it becomes popular with users for trading. Blockchain technology will also eliminate expensive intermediary fees that have become a burden on individuals and businesses, especially in the remittances space.

The implications of this technology are staggering, not just for the gold trading and financial services but also right across virtually every aspect of business.

LET'S LEARN DIGITALo

The significance of Satoshi's Bitcoin paper

When we reflect on the history of the internet, it was initially rolled out simply as a networking infrastructure which connected computers together globally. It wasn't until The Web developed new protocols combined with the development of search, publishing, ecommerce, email and social media that the real potential of the internet emerged. Today 47% of world's population has an internet connection while in 1998 that number was less than 1995. We can use this historic analogy and precedent to better understand blockchain and how it materialised out of bitcoin.

Blockchain emerged out of the pseudonym group 'Satoshi Nakamoto' behind the creation of the crypto currency, bitcoin. This group outlined the vision of Bitcoin as a new type of cryptocurrency in the ground breaking 2008 paper "Bitcoin; A Peer to Peer Electronic Cash System"

The 2008 Satoshi document was significant and explains Bitcoin's foundation attributes, the features of which are paraphrased below:

- Bitcoin is a peer to peer version of electronic transactions and interactions. Participants interact with one another using pseudonyms, and their real identities are encrypted and remain secret
- The blockchain architecture which underpins the Bitcoin is a decentralized technology, thus a trusted intermediary of third party is not required for trading. When a bitcoin transaction takes place, a number of separate computers, connected across the network, process the algorithm and confirm one another's calculation. The record of transactions thus continually expands and is shared in real time by thousands of people. The ledger stores basic information about each transaction such as sender, receiver, time, asset type, and quantity. The blockchain process ensures validity, by mathematically linking each new transaction to those that came before it and provides the evidence of the provenance of each transaction in a chain of records
- Bitcoin provides a fully transparent encryption process. The ledger uses public-key encryption, which is virtually impossible to break, because a message can be unlocked only when a public and a private element, the latter held only by the recipient are linked.

LET'S LEARN DIGITALo

- The application of cryptographic principles in the form of time stamps are used to verify transactions and storage. The cryptographic connection between each block and the next forms one link of the chain. This process compounds the mathematical difficulty of committing a successful fraud, because blocks of transactions, as well as individual transactions, are continuously validated. The algorithm also incorporate
- The term blockchain is derived from the way transactions are stored. For example, every time a bitcoin is created or changes hands, the ledger automatically creates a new transaction record composed of blocks of data, each encrypted by altering or “hashing” part of the previous block
- The longest chain serves as proof of the sequence of events and also that it came from the largest pool of CPU (Central Processing Unit)
- Trust in a third party institution is replaced by the computer network. This perhaps the most important unique attribute of both Bitcoin and the blockchain platform it sits on which we will explore in the next chapter

The blockchain is thus the invention which underpins the mechanics of Bitcoin as described in Satoshi's 2008 paper. The realization that the underlying technology that operated bitcoin could be separated from the currency and developed into a hybrid flavour of differing blockchain applications used for all kinds of other interorganizational cooperation is a recent phenomenon.

LET'S LEARN DIGITALo

How Blockchain enables trust and transparency

The real innovation that emerged out of blockchain was not the digital currency but the trust and consensus which it engenders. The Economist recently described blockchain as "the trust machine" which rightfully expresses trust and consensus at the heart of a it's potential. The blockchain enables trust to infiltrate in a decentralised way that breaks the old paradigm of centralised consensus, when one central database used to rule the transaction. When transactions are executed and settled on a distributed ledger, counterparties don't need to have an established trusted relationship. If each participant in the transaction trusts the blockchain itself then they don't need to directly trust each other. This opens up new avenues of customers for businesses operating on blockchains.

But blockchains redefine the whole notion of trust. When we think about trust in a trading or any financial services transaction we think of the following definitions: reliance, predictability, confidence, truth, assurance, credence, fast delivery and responsibility, As business people let us examine a selection of trusted third party institutions we interact with on daily basis; banks, credit card companies, mortgage companies and utilities companies to name a few. We trust these companies because they deliver an effective job most of time. Banks do not steel our money, they give us access to our money it 24/7 though cash machines. Yet in a digital world where new customer expectations are being redefined by innovative companies like Apple, Uber and Amazon increasingly we can think of cases where trust which we seemingly granted to these major institutions is being eroded, taken for granted or just being forgotten. Recent examples include creditcards charging us 23% on transactions and the increasing consecutive rises of price of gas and electricity here in the UK with little clear explanation as to why

If we examine the 2017 Edelman Trust Barometer ¹this research reveals the largest-ever drop in trust across the institutions of government, business, media and NGOs.

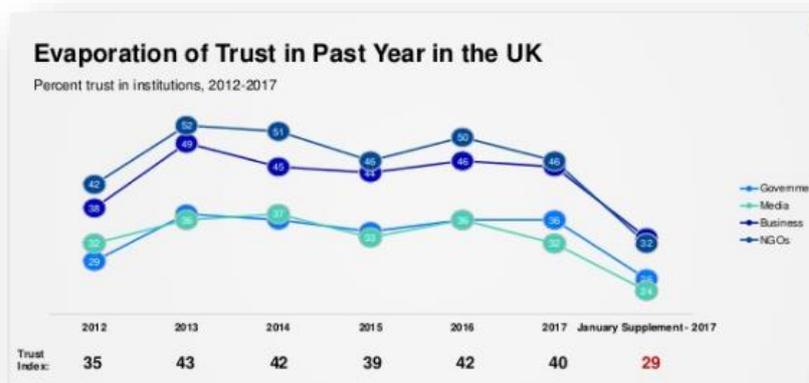


Fig 2 ; the evaporation of UK Trust in the last year (to Jan 2017)

¹ <https://www.edelman.co.uk/magazine/posts/edelman-trust-barometer-2017-uk-findings/>

LET'S LEARN DIGITALo

The Edelman report also reveals the credibility of leaders is eroding of time: CEO credibility dropped 12 points globally to an all-time low of 37 percent, plummeting in every country studied, while government leaders 29% , remain least credible. Key findings also reveal the following:

- We are experiencing a total collapse in trust in the institutions that shape our society. Trust in the UK is at a historic low at 29 per cent.
- Trust is in an accelerating spiral of decline. Data from the closing days of 2016 and first week of the New Year shows an unparalleled plunge of 11 percentage points in a matter of weeks.
- There is an unprecedented feeling in the UK that life is not as fair as it used to be. Only one in nine of the UK population think that the system still works, and globally half of those that are high-income, university educated and well-informed. Faith in the system is not about income anymore.
- Loss of belief in the system appears to be fuelled by growing fears of forces beyond our control: immigration, the erosion of societal values and the pace of technological change.
- Trust in authority is draining away and being replaced by trust in those closest to us and most like us.
- Trust in politicians is close to rock bottom, with Theresa May the only politician trusted by just over a third of the population. No other politician scored higher than 25%.
- Business needs to lead. It is just about standing at 33 per cent, but will lose trust unless it engages with the people, and demonstrates solutions to public concerns.

”It is now evident that we have underinvested in the levers of trust across the board. We are experiencing a total collapse in trust in the institutions that shape our society Trust in the UK is at a historic low at 29 per cent” Edelman report 2017

LET'S LEARN DIGITALo

So what does blockchain have to do with this? Blockchain has the potential to transform trust, improve transparency so that the unfortunate breaches of trust.

For example Deutsche Bank's unfortunate gold manipulation fine ²can be eliminated. Blockchain offers truth and transparency as a base layer. But most trusted institutions in 2017 do not offer truth or transparency.

The trust generated in a blockchain is shifting from humans to computers and across the centralised networks via a consensus. In our current business world trust is applied by default by humans through third part authorities In this new paradigm of business the trust will be transferred from humans to the blockchain network that will now serve that trust function. This is absolutely key to understand and gets to the heart of why blockchain is such a transformative technology So with this theory in mind a central question is can the blockchain give us a better form of trust that does not become too complex and large to fail? Although this technology is still very much in its infancy in summary yes. Because blockchain decentralizes trust and makes way to be able to check and verify the veracity and authenticity of facts, data, processes, events or anything by shifting trust to the network.

The challenge of proving something happened is one of the unique powerful tenets of blockchain. The hierarchy of proof method layers are demonstrated in fig 3 below starting with at the bottom layer proof of consensus, for example proof of work or proof of stake to the next layer proof of service such as proving identity or ownership or proof in service where proving something is part of another service such as land registry.

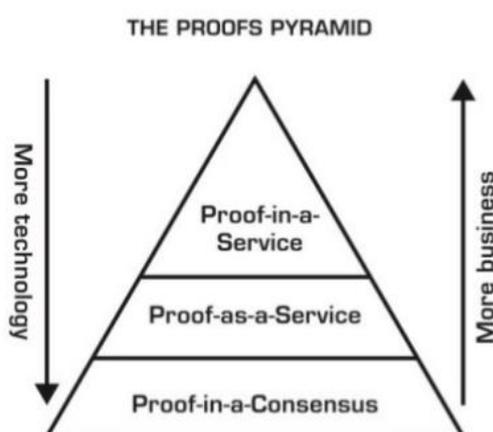


Fig 3 Source: Wiliam Mougarr; The Proof's Pyramid

² <http://www.zerohedge.com/news/2016-12-03/deutsche-bank-pays-60-million-settle-gold-manipulation-lawsuit>

LETS LEARN DIGITALo

Thus the blockchain places trust and transparency at the heart of its central function which moves from a previous third party to being engrained into the network. This is very exciting and gets to the foundation of why it has been chosen for the new Royal Mint and CME Gold Standard.

LET'S LEARN DIGITAL

What does a trusted Blockchain enable

A trusted blockchain is a powerful catalyst with many unique features and benefits which can be used and applied in many business situations. Let us expand below:

- Real time movement of digital assets

Digital assets can be created, managed and transferred on a blockchain network without incurring clearing related delays due to the existence of intermediaries.

- Embedding trust rules inside transactions and interactions

By inserting rules that represent trust inside transactions, the blockchain becomes a new way to validate these transactions not via a central authority but a new trust factor which is created as part of the transaction

- Time stamping and ownership proof

The blockchain enables the time stamping of documents representing the rights or ownership, therefore providing evidence and transparency that are cryptographically secure. This in turn allows a variety of modifications such as RMG multi signature ownership to further enforce trust.

- Self execution of Business Logic

Verification managed within the blockchain enables the trust component to be part of the transactions

- Selective Transparency

Using cryptographic technologies transactions are verified and completely transparent thus enabling new levels of centralised data privacy and security

- Resistance to points of failure

The blockchain consists of several decentralised computers and resources. There is no single point of failure therefore making the network more resilient compared to traditionally centrally controlled models

LET'S LEARN DIGITALo

Obstacles and challenges of implementing new technology

As far back as 550 BC investing in commodities like gold has maintained its popularity in global investment hubs because of its ability to successfully preserve wealth throughout thousands of generations and act as a competent monetary safe haven during periods of political uncertainty and high inflation. This is still true today where the political and economic uncertainty around global upheavals such as the turmoil in Syria and recent Brexit vote, mean once again an investment Gold is being considered by Investors as a favourable investment alternative to preserve wealth.

While new technologies like distributed ledgers, artificial intelligence and the cloud are transforming other financial sectors like insurance and banking, trading in gold has been relatively resistant to change and slow to embrace new technologies. This can be attributed to a number of underlying obstacles:

- **Uncertain regulatory status**

As regulation has tightened across the Financial Services sector since 2008 the guidelines for testing new technologies have been until recently somewhat opaque compounding the UK resistance to test the viability for new technology platforms. This approach more recently in the UK is changing. In April 2016, the London based FCA launched the new innovation sandbox³ encouraging Fin Tech and startups to test innovative products, services, business models and delivery mechanisms in a live environment.

- **Trading systems have been slow to adapt**

Legacy systems for example in the gold industry have been slow to update. The historic London Gold Fix was a telephone-based benchmark price auction when each representative raised a tiny British flag after receiving any price change from their dealing room and as long as a flag was up, the chairman could not declare the price as fixed. This system began in 1909 and did not change for over one hundred years until 2015 when a new modernised electronic system the London Bullion Market Association Gold Price Was implemented

- **Costs have remained static**

The cost of investing in traditional commodities like Gold can be expensive when you consider the transaction trading cost and ongoing cost of storage. Buying Gold through an exchange-traded fund (ETF) typically costs 0.5% while the cost of then

³ Innovation Sandbox; <https://www.fca.org.uk/firms/innovate-innovation-hub>

LET'S LEARN DIGITAL

storing gold is an additional charge. For example the cost of safe deposit box at the Sharps Pixley shop In London costs £250 a year. Despite the growing cost attractiveness of investing alternatives in such as new trading platforms like Hargreaves Lansdown the high fixed costs of investing in gold has remained static and relatively high.

- **Real time access**

A commodity like Gold investment has always considered a good long-term inflation hedge but if you need the cash immediately then volatility may far outweigh the short term gain of immediate access. Speed of access has sometimes made it unattractive to investors. For example gold bought at its peak in September 2011 would today be worth almost 25 per cent less and thus historically it is has been very much geared towards a long term investment

- **Lack of transparency and open to manipulation**

Gold investing has been criticised for lack of transparency and as a result being ripe for open manipulation. This problem has resulted in challenges to investment credibility with high profile law suits launched against high profile banks as recently as October 2016⁴. In these gold rigging legal cases the traders alleged the banks abused their positions of controlling daily silver and gold fixes to reap illegitimate profits from trading

- **Risks of current standards in trading Gold**

As a financial product, ETF's carry counterparty risk. This means that investors must rely on another party to make good on the investment. With a gold ETF, you are dependent upon among other things, management prowess, fund structure, chain of custody, operational integrity, regulatory oversight, and delivery protocols which are available only to very large shareholders. If any of these steps break down, your gold investment is at risk. One primary reason to own gold is for it to be your last line of defence in economic or monetary crises. But since the banking system is also at risk during periods of stress, so are gold ETFs as they are part of that very system thus negating once again their appeal

- **Lack of trust**

Trust is eroding across the board (see endelman data on Page 10) The recent crippling of the NHS through the cyber data hacks combined with the lack of trust which infiltrated the financial system around the global financial crash of 2008 have created a risk averse culture in some sectors such as gold for testing new technology platforms and new ways of investing in Gold

⁴ <http://www.reuters.com/article/us-gold-lawsuit-decision-idUSKCN125292>

LET'S LEARN DIGITAL

All these obstacles have combined to necessitate a market appetite for a new type of technology which addresses to above issues and places transparency, trust, efficiency, more competitive costs and security at its centre

“Gold trading still isn’t easy and it’s costly. There’s annual management fees, and it’s a negative return investment now. Royal Mint Gold (RMG) will address the issue.” Royal Mint’s director of business David Janczewski told City A.M

LET'S LEARN DIGITALo

Blockchain in the Fintech/ Investment sector

The unique qualities of blockchain have not gone unnoticed in other financial technology or (fintech) hubs in the UK, Europe and across the world. Part of the investment in blockchain has been assisted with the collaborative and UK's recent open regulation approach initiated by the Financial Conduct Authority who have actively encouraged new technology innovation with the creation of the Innovation Hub5, launched in 2015. The purpose of this new unit is to encourage both established and new startups to test new innovative financial products like blockchain through their regulatory sandbox. This unit was supported by a new paper the Discussion Paper on distributed ledger technology⁶ examining blockchain regulation in a Q and A format

Inspecting the London fintech community what can it teach us about the current state of blockchain and its attractiveness as a product to investors. One key underlying trend is that blockchain is disentangling itself from the unwanted media attention around bitcoin and the online black market websites like Silk Road associated with bitcoin payments. It is now emerging as its own robust entity evolving into other significant industries like, healthcare, energy and government services like identity.

According to digital currency data provider Coindesk, blockchain startups investment increased more than fourfold year on year in the first quarter of 2016. Total venture capital funding nearly doubled to over \$1.1 billion. Blockchain wallet users doubled to nearly 7.8 million in the second quarter of 2016 from 3.7 million in the second quarter of 2015. In March 2016, JPMorgan Chase unveiled a blockchain prototype, codenamed Juno. Other large banks like Barclays, BNY Mellon, Goldman Sachs and UBS have quietly amassed teams for blockchain development.

Data supplied by Chris Skinner's blog showed in the first half 2016 InsurTech and blockchain were the major winners during 2016. What this shows is that funding in the first half of 2016 for Blockchain related start-up firms is almost the level of funding for the whole of 2015.

⁵ Innovate and Innovation Hub, Financial Conduct Authority: <https://www.fca.org.uk/firms/innovate-innovation-hub>

⁶ <https://www.fca.org.uk/publication/discussion/dp17-03.pdf>

LET'S LEARN DIGITALo

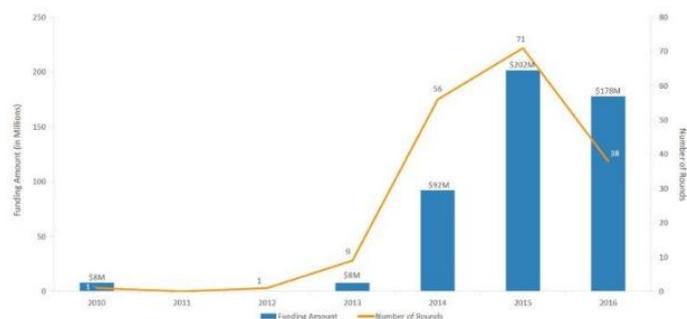


Fig 7 Total of rounds of funding and total investment in fintech

The enthusiasm and collaboration of blockchain related projects within established banks is also very positive. According to the World Economic Forum, over 80% of banks are expected to initiate blockchain projects by 2017, while more than 24 countries and 90 central banks have already engaged in discussions. What's more, over 2,500 patents have been led in the past three years.

“Blockchain technology continues to redefine not only how the exchange sector operates, but the global financial economy as a whole.” Bob Greifeld, Chief Executive of NASDAQ

Much of the blockchain's technical innovation in the Financial Services sector is being driven by start-ups and the Fin Tech community. The positive repercussion of this dynamics is the increased collaboration between established players and small startups. Mark Buitenhek, the Global Head of Transaction Services at ING Bank, and a widely recognised keynote speaker on FinTech topics reinforced this view by stating “One thing that is clear is that industry collaboration will be the driver behind any blockchain success....”.

Rather than buying fintech companies established players are looking for a new type of partnership, companies of all sizes within fintech and more established institutions are realizing that industry wide collaboration and acceptance need to materialize for block chain technology to really succeed and for more widespread adoption to take place. A recent example of this collaboration in practice between Ripple a London based global financial settlement startup and Santander Innoventures which uses its fund of \$200 million to invest in startups. Santander's investment is yielding benefits for both sides. According to Danny Arunda MD of Ripple this tie up has been hugely beneficial for his company; “When you first launch a product, it will almost certainly have some issues. Working with the bank has helped us improve our offering to the market” Creating a collaborative environment in the fintech sector and a robust support for next- generation financial services consortiums like R3 now has a backing of over 50 banks and can only be positive.

LET'S LEARN DIGITAL



Fig 7: London fintech hub Level 39 hosting the Prime Minister and Chancellor

In spring 2017 the two most senior figures in the conservative government Prime Minister Theresa May and chancellor of the exchequer Philip Hammond in advance of the General Election held their party conference among 200 ambitious tech businesses driving innovation at the heart of Canary Wharf. This was a landmark occasion and symbolised the importance of Fintech as critical hub to the UK economy. It is easy to see why many technology innovations like blockchain resonate with Theresa May's vision of a 'strong and stable' UK.

The blockchain infrastructure is showing a promising future within the Fintech community, with diverse potential applications that could reshape how business is being conducted not just in gold trading but also across payments, loans and trading. Blockchain will not signal the end of banks but the innovation unlocked in fintech and the start up communities like Level39 is critical to springboard the technology and enable it to truly flourish

LET'S LEARN DIGITALo

Implementing Blockchain- the spectrum of decentralisation

The term distributed infrastructure implies that companies that consider applying blockchain should be willing to share control over the infrastructure they wish to distribute it on. The extent to which the infrastructure is shared can be plotted along a spectrum that ranges from fully centralized to fully decentralized. This range is called the spectrum of (de)centralization and is a critically important concept to understand when evaluating the security of RMG's new blockchain. Let us explain some more.

Typically, the level of centralization results in a trade-off: the more decentralized the infrastructure, the less trust is required between participants. However, this leads to less efficiency in computing power because additional verification is required.

Each position on the spectrum impacts who is allowed to do what on the infrastructure. These user rights can be divided into three types:

1. Read (view the history of activity of the ledger)
2. Write (commit activity to the ledger)
3. Validate (validate authorized transactions and prevent incorporation of unauthorized transactions)

The three main positions along the (de)centralization are described below

Centralized control

A centralized configuration reflects the current structure of business transactions: one party controlling the infrastructure. This central party alone is able to perform and validate data transactions. Other parties may be provided with read-only rights to review the ledger history on their distributed copy, for example, for auditing or regulatory purposes. The advantage of such a system lies in its cost-effectiveness. It requires no consensus mechanism and provides full control over the transactions that take place within the chain. This, however, requires participants to trust the central party which for a completely new platform product trading gold could be a potential hurdle. Another disadvantage is that the central party is potentially a single point of failure, resulting in a system that is potentially vulnerable to malicious attacks or fraud.

Fully decentralized

Bitcoin is an example of a decentralized ledger. Given sufficient participants, it is unlikely in a well-designed infrastructure that any one party could gain enough control over the network to tamper with transactions.

LET'S LEARN DIGITALo

While a fully decentralized infrastructure may be the ideal end state for establishing decentralized markets that can run independently of trusted parties, certain considerations are impacting their full implementation at present.

Some of these issues require an understanding of how public ledgers operate. While activity recorded in a permissioned ledger is validated by participants on an equal basis, public ledgers require arbitrary parties to validate activity. Consequently, an incentive to validate transactions is required. This incentive is based on most public ledgers' designs, which require tokens to perform functions on the network. Consequently, these tokens' value are based on market demand. When tokens are provided as an economic incentive to participants who assist in the validation process, public ledgers can operate in a fully decentralized manner. This leads to three considerations. Firstly, to engage with the ledger, participants will need to purchase tokens at the market price. As many of these ledgers are very new and the market is still being developed, this price can fluctuate extensively. Consequently, basing a company's operations on a public infrastructure has monetary exchange risk implications that are not present in centralized infrastructures or permissioned ledgers. Secondly, the validation process itself for most public part of the group being allowed to validate the transactions. Viewing rights could be provided to regulators or other third parties for real-time reporting. Permissioned ledgers allow semi-trusted parties to share infrastructure among themselves and interact directly with each other, without requiring the establishment of a single trusted party or a separate, distinct infrastructure to coordinate between them. Trading partners in certain markets, or distinct legal entities among conglomerates or joint ventures, could benefit by using this technology: while there is a sufficient level of trust to engage with each other in mutually beneficial trade, there may not be enough to have a single party manage the books and records required to manage the trade effectively. The advantages have inherent trade-offs, however.

Hybrid

Between a fully centralized and fully decentralized infrastructure sits a hybrid permissioned ledger. In this structure, control over a ledger is distributed across a group of trusted peers. Through a consensus mechanism, parties with the right to validate new transactions can update the ledger. Because this group may be small, the involvement of a malicious party could expose the network to the risk of tampering. This risk can be partially mitigated via due diligence procedures regarding the selection of peers who are allowed to join the network. A group of banks that wish to transact with one another could opt for a permissioned ledger, with each or Implementing blockchains and distributed. The RMG product is built on a hybrid model using a centralized asset issuance, someone who is responsible for physically vaulting the gold with a decentralized ownership and verification.

LET'S LEARN DIGITAL

The Future of Blockchain in Fintech

New technology innovations, new expectations around costs, changing customer expectations combined with a greater need for transparency and trust are forcing the gold markets and how gold has traditionally traded to reassess the way it transacts business. Trust in the context of the recent NHS hacks and data provided by the 2017 Endelman research is a declining and much needed commodity to provide a more viable and compelling future for gold investment

If we consider the history of the internet there is a precedent when we consider the future potential of blockchains and their future potential. With the Internet, we had e-commerce, e-business, services, e-marketers and social web arriving in large scale social networks. Each one of these segments has created its own wealth. Trading on a blockchain will succeed by creating a new ecosystem enabling a new flow of value creating large market opportunities where trust, price and transparency is built into the heart of its infrastructure

Until recently the price of gold was still fixed twice a day by a small group of banks conferring over the phone with clients. This century-old methodology has now been replaced by the dramatic launch of RMG Gold. The push for greater transparency and trust has been seized upon through the vision and collaborative partnership of the Royal Mint Gold and CME heralding the launch of the exciting new RMG gold. This represents a new decisive chapter in the history of gold trading with the first trading platform launching on blockchain providing a new layer of speed, security, transparency, pricing, trust and direct ownership through the Royal Mint.

LET'S LEARN DIGITALo

References

The Pulse of Fintech; KPMG 2016

<https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/pulse-of-fintech-q4-2016.pdf>

RMG: The New Gold Standard

<http://www.royalmint.com/rmg>

How Blockchain will change the Future of Financial Services

<https://www.finextra.com/blogposting/13823/how-blockchain-will-change-the-future-of-financial-service-sector>

Blockchain Training Workshops in London: 1 Day training

<https://www.letslearndigital.com/courses/>

LET'S LEARN DIGITAL

Blockchain Jargon Buster

API: API stands for application programming interface. It is a set of requirements that dictate how two pieces of software talk to each other. It is basically what allows you to move data between applications.

BaaS: A relatively new term for 2016, coined by William Mougayar of Virtual Capital Ventures in early 2015. It means Blockchain-as-a-Service. Equivalent terms include Ethereum Blockchain-as-a-Service (EthBaaS), or "Blockchain-as-a-Platform" (BaaS). It refers to the growing landscape of services based around blockchain technology. The best example of this we have so far is Microsoft launching its own EthBaaS on the Microsoft Azure cloud platform this year. This platform will allow companies to begin working with blockchain technology without having to first make significant investments in hardware.

Bitcoin: Bitcoin is a decentralised digital cryptocurrency that was invented by the pseudonymous Satoshi Nakamoto in 2008. In the past few years, Bitcoin has evolved from being a murky money of the digital underworld to an increasingly mainstream digital currency.

Blockchain: Blockchain is the technology that underpins Bitcoin transactions. The most simple explanation is a decentralized digital ledger which records all digital transactions as a string of data stored on a global network of computers. Every time a new batch of transactions is encrypted by the network, it is added to the string (or chain) as a "block."

Crowdfunding: There are two types of crowdfunding: rewards-based crowdfunding and equity-based crowdfunding. The first relates to platforms like Kickstarter or Indiegogo, where startups raise pledges and in return offer buy-in incentives for anything they produce. Equity crowdfunding is a more recent phenomenon where pledgers are actually investors that receive a small share in the business in return for their contributions.

Cryptocurrency: A cryptocurrency is a digital currency in which uses encryption to secure transactions and control the creation of new units. Cryptocurrencies typically operate independently of any central bank. Bitcoin and Ether are the most notable examples of this.

DRaaS: This is a term that has emerged in the area of cyber security and means Disaster Recovery-as-a-Service. It refers to the hosting of physical or virtual servers by a third party as a security measure to protect a business' infrastructure in case of a cyber attack, natural disaster, or man-made catastrophe.

Digital native: A digital native refers to a person who has grown up with the availability, and use of, digital technology. This group includes millennials, or post-millennials AKA

LET'S LEARN DIGITAL

Ethereum: Ethereum is a blockchain-based cryptocurrency platform that runs Smart contracts. It was originally authored by Vitalik Buterin and Gavin Wood. Ether: The currency unit of Ethereum. It is used to pay for computational services on the Ethereum network.

Generation Z. Digital wallet: This refers to any electronic device or application that allows an individual to make electronic transactions. This can be either using cryptocurrency or real money which is often pre-loaded onto a digital account.

Internet of Things: Internet of Things (IoT) refers to the development of everyday internet-connected objects that have the ability to record, receive, and send data. This covers internet-connected cars, light bulbs, fridges, clothes, pedometers, and everything in between.

Nodes: participants on a distributed ledger. Different nodes may have different rights to read, write and/or delete data.

Miners: this is a participant on a distributed ledger that adds new records by solving a cryptographic puzzle and is rewarded in the protocol's digital currency.

P2P lending: P2P means peer-to-peer, or person-to-person, and refers to anything that is decentralized and direct. P2P lending is loaning money to individuals without the systems and processes typically put in place by traditional financial institutions. Instead, the transactions are often handled by digital platforms that use an algorithm to manage transactions between parties.

'Public' DLT networks: these are networks where all users of the network can see records being added or changed. The opposite, 'private' DLT networks, are those where visibility is restricted to a subset of users.

Smart contracts: Smart contracts are computer protocols that facilitate, verify, or enforce a digital contract. The idea is that these programs will eventually be used to replace lawyers and banks when handling common legal and financial transactions.

SaaS: This means Software-as-a-Service. It is a software distribution model used by many fintech software startups. It basically means applications that are hosted by the vendor on the cloud and can be accessed by the users online for a subscription fee,

Unpermissioned/permissionless DLT networks: these are networks where anyone is allowed to validate and add new records to the existing set of records. The opposite, 'permissioned' DLT networks, are those where only users with specific rights are allowed to do this.

LETS LEARN
DIGITALo

Contact Details

David Reilly: david@letslearndigital.com

07989 985922