Locke Lord LLP
solicitors

INNOVALUE

Q3 2015

BLOCKCHAIN AND FINANCIAL SERVICES
INDUSTRY SNAPSHOT AND POSSIBLE FUTURE DEVELOPMENTS

Image: Shutterstock, 149395436 © rvlsoft / Shutterstock.com

FOREWORD

Technological developments, developments in telecommunications and in the new media are reshaping the market in which financial services companies operate and ultimately how they compete. This is an irreversible and ongoing process of change and industry convergence that started in the nineties during the "dot-com" boom and whose outcome is yet to be defined.

INNOVALUE Management Advisors and Locke Lord have joined forces to combine top tier strategic thinking with legal and regulatory expertise for the development of three digital banking thought leadership reports. This is the second of the three and is intended to provide a snapshot of the opportunities, challenges and key success factors for financial institutions looking to leverage the blockchain opportunity.

Enjoy the study and may it increase the wisdom of your decisions.

Robert Courtneidge
Partner
Global Head of Cards and Payments
Locke Lord LLP

Francesco Burelli
Partner
INNOVALUE Management Advisors Ltd

Published by
INNOVALUE Management Advisors Ltd.
3 More London Riverside
London, SE1 2RE, UK

July 2015

Written and edited by
From Innovalue: Francesco Burelli,
Megan John, Edoardo Cenci
and Janne Otten

From Locke Lord:
Robert Courtneidge, Charlie Clarence-Smith

If you would like a copy
please write to:
contact@innovalue.com

For more information on the issues
raised in the report please contact:
burelli@innovalue.com

EXECUTIVE SUMMARY

Seven years after the blockchain was introduced, there is a shift in focus occurring in the discussion around the applications for the technology. Previously, the discussion has focused largely on the Bitcoin – an early application of the technology in the form of a digital currency.

Recently, the discussion has begun to focus more and more on the core elements of the blockchain itself and how its nature as a distributed ledger for transactions could be leveraged to provide new products and services and to improve existing ones.

Blockchain was first launched as an alternative approach to payments (using mathematics to provide an alternative mechanism for the trust between two transacting parties). Now it is being used as a solution for a wider range of transactions.

The potential applications for the blockchain range from methods to transfer funds across currencies in a cost effective way (e.g. as an FX clearing tool for cross-border remittances) to provision of "programmable money" (e.g. transactions that pay only after conditions are met) to digital assets (whereby the record of ownership for an asset is stored digitally) and to peer to peer storage (where data is stored in a distributed way across multiple systems – without a dependency on a central system or provider).

New companies who offer solutions in these areas have already emerged and incumbent institutions in both financial services and technology are considering (and already launching) blockchain based solutions. Moreover, "incumbents" are responding to new entrants by developing in-house solutions, investing in blockchain companies, forming partnerships or leveraging accelerators.

This paper provides an overview of the development of the blockchain, details of the mechanisms of the new technology for processing transactions, a summary of the "new" blockchain initiatives and a discussion of the response that organisations are taking.

1 INTRODUCTION

Currently, transactions between people (where goods / information are exchanged) rely on a trusted third party (such as a card scheme), who mitigates the risk of a transaction between unfamiliar payers and payees (for example through e-commerce) by enabling the transaction and providing a payment guarantee, subject to the payee abiding to set rules.

While this type of risk is not material in cash based face-to-face transactions, during which a deal is settled by cash exchanging hand on the spot, it exists in remote transactions, which rely on a third party to provide the payment guarantee.

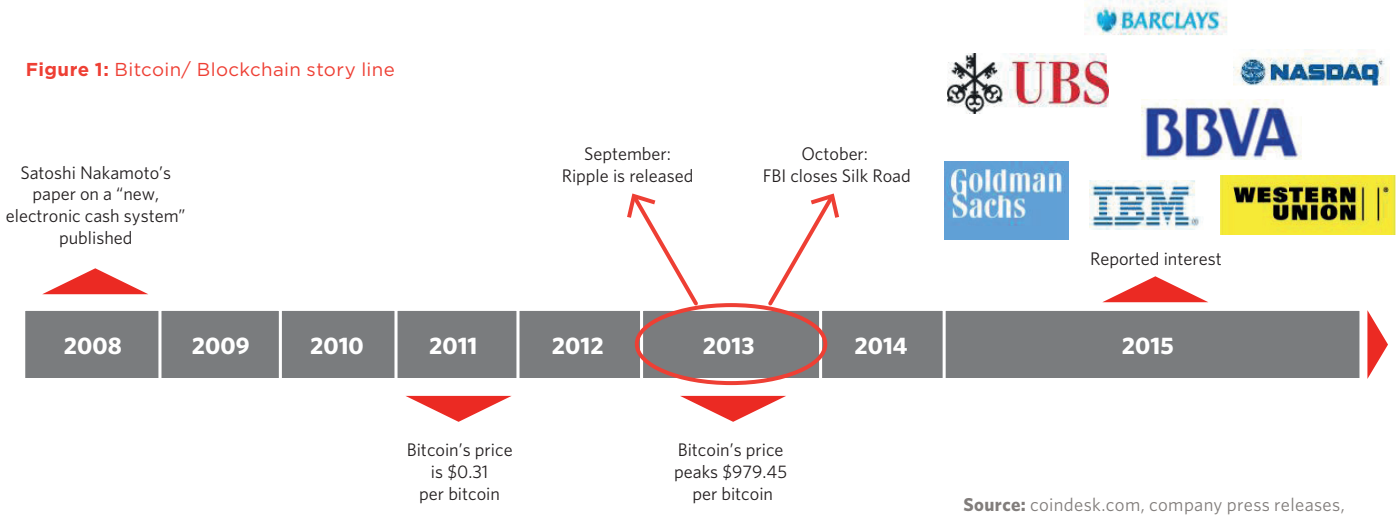
In 2008 Satoshi Nakamoto[1] created a system which replaces these traditional third parties and provides a distributed ledger of verified transactions of a particular unit.

This system is known as the "blockchain" and it is the result of three different and independent concepts: distributed ledger[2], cryptography[3] and open source software[4].

The first and most famous application of the blockchain is a digital currency called Bitcoin. Bitcoin has gained media attention due to its price volatility (reaching ~£1,000 per coin in 2013) as well as due to its use by Silk Road (the biggest online black market, selling illegal goods over the internet and accepting only bitcoins), which has been closed by the FBI and due to the emergence of competitors (such as Ripple).

These events have all increased the interest in the Bitcoin's technological backbone: the blockchain.

Figure 1: Bitcoin/ Blockchain story line



Source: coindesk.com, company press releases, INNOVALUE research

[1] Satoshi Nakamoto is a pseudonym for an unidentified person or group of people
[2] Definition: "a ledger containing the record of all transactions by all users [that] is publically available to all" – Bank of England
[3] Definition: "Cryptography is the use of codes to convert data so that only a specific recipient will be able to read it, using a key" - Microsoft
[4] Definition: "Open source software is software that can be freely used, changed, and shared (in modified or unmodified form) by anyone." – Open Source Initiative

2
OVERVIEW OF BLOCKCHAIN AS A METHOD FOR COMPLETING TRANSACTIONS

As the internet was created to allow computers to communicate across different locations and their users to communicate with people they might not have physically met, the blockchain was originally created to allow value to be exchanged across different locations and between strangers.

The blockchain "is the ledger (book of records) of all transactions, grouped in blocks, made with a (decentralised) virtual currency scheme."[5]

The blockchain enables the exchange of information, in a synchronous and even manner, allowing two parties in a network to complete transactions without the parties being known to each other or guaranteed by a third party. It effectively enables a collective book keeping system on the internet, which constantly updates and, with the aid of a mathematical function, allows participants to reach an agreement on the approval of the transactions. In this system, transactions are made between members of a network and the information concerning the transactions is gathered in "blocks".

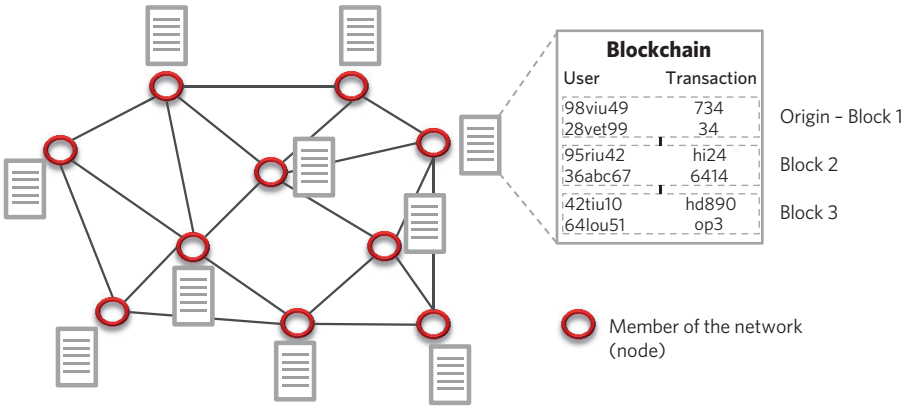
These blocks are reviewed and verified by the network and added in a chronological order (creating the chain of blocks) on the computers of all participants of the network. The blockchain is then the public register (the list) of transactions and is, de-facto, owned by each participant of the network. Thus, all movements of information that has been exchanged in the network can be traced, enabling the transparency of the system, assuming that the IP of the computer being party to a transaction is not masked.

The diagram on page 8 explains how a transaction is processed by a blockchain system. The first is an overview of the blockchain process itself, while the second is an illustration of the blockchain process in a physical marketplace to provide an overview of the concepts in a more familiar setting.

Any usable "value exchange" system for transactions has to satisfy two key features: reliability and safety[6]. These features have so far been ensured by a trusted third party (e.g. a bank, clearing house, government). These organisations are trusted due to their established position in the market and their willingness to undertake the risk of the buyer or seller in case of a default.

They also have mechanisms in place which prevent buyers from "double spending" (using the same funds for two separate transactions), creating structured features that enable trust in the system. The blockchain introduces a way of processing transactions that eliminates the risks connected to a centralized third party and fulfils these roles. It does this through its distributed ledger design and the hash function, which are explained in more detail in the following paragraphs.

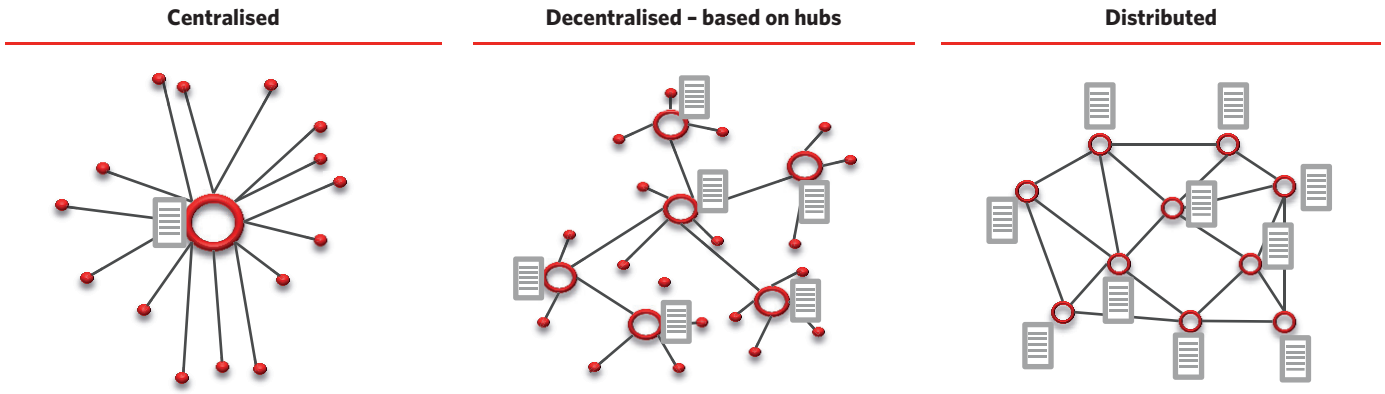
Figure 2: Illustration of the blockchain and of the distributed network



[5] Source: ECB, Virtual Currency Schemes, February 2015

[6] Source: ECB: "The availability of reliable and safe payment mechanisms for the transfer of funds is therefore a sine qua non for the majority of economic interactions (i.e. "no payment, no trade")."

Figure 3: Distributed ledgers compared to centralised or decentralised ledgers



The fact that the blockchain is a distributed ledger maintained by all the members of the network enables transparency and integrity of the system. A distributed ledger works by equally redistributing the control and the risk of the system to each member of the network. On this concept, IT firms (such as Microsoft and Oracle) have developed a method to distribute data among multiple devices in a way that each device can modify and / or update information, making them available to the entire system.

A distributed ledger can be located on any type of company network, intranet or extranet or, more broadly, on network servers connected to the internet. It differs from a centralised and decentralised system since the data is owned by all members of the network and not only by a central entity or a restricted group of hubs.

The architecture of the ledger can be built to provide different layers of security and to connect identical devices (computers) or devices with different components (hardware and software). A distributed ledger can be set up using three variables: access to the network, homogeneity of the devices in the network and the complexity of information included in each block. This leads to different setups illustrated in figure 4. Therefore, a blockchain can be implemented in different ways in order to facilitate different uses, which are considered in the next section of this paper.

In addition to the features enabled by the distributed ledger, the hash function provides a way to maintain the security of the system and ensure that transactions are not duplicated. It provides a method of agreement on the state of the distributed ledger, known as a "proof of work".

This "proof of work" process works as follows:

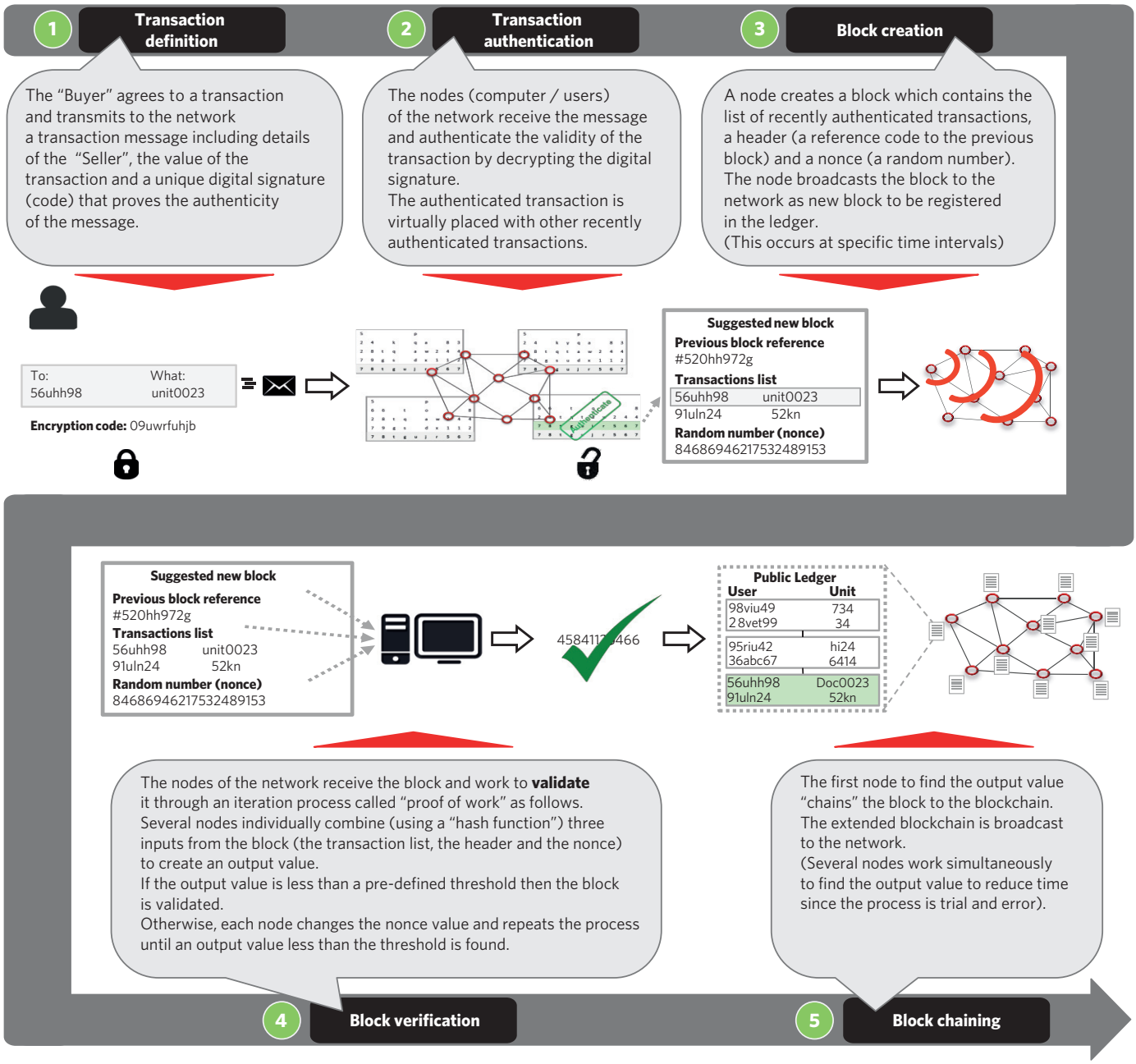
- Each block includes three pieces of information - a reference to the previous block (x), transaction details (y) and a random number called a "nonce" (z). These inputs are transformed into a single output of a defined size using a "cryptographic hash function" (in mathematical terminology if H is the hash function, then the output would be H(x,y,z)). The cryptographic hash function transforms the inputs in such a way that it is effectively impossible to reverse the transformation or predict the outcome.
- This output is then compared to a pre-defined threshold. If the output (the hash value) is not less than the threshold then the node completing the proof of work changes the nonce (for example to z_1) and computes the hash value with these new values (the new output would be $H(x,y,z_1)$).
- Once a node has a hash value ($H(x,y,z_n)$ less than the threshold the block can be added to the chain (figure 5 illustrates the process).

Figure 4: Matrix of distributed ledger permutations

Access	Infrastructure	Block's content size
Public The participation to the network is open to the public / those interested in taking part to the network	**Homogeneous** System requires same hardware and software	**Limited** The blocks within the blockchain are of limited size (in bits) and contain limited amounts of information
Private The participation to the network is restricted to a selected number and type of participants	**Heterogeneous** System is able to operate on multiple hardware and software	**Extensive** The blocks within the blockchain have a size such it can contain a larger amount of information

Source: INNOVALUE research

Overview of the blockchain process



Source: INNOVALUE research

The process takes time to complete as it envolves the computation of a random number, minimising the possibility for transactions to be duplicated. However, duplication would occur if two blocks were added to the chain at the same time, creating a "fork" with parallel "side chains". This would happen if two nodes simultaneously solved the hash function for different blocks and concurrently add them to the chain.

When nodes look to add a new node to the blockchain they consider always the longest chain (which is regarded as the most reliable). When the blockchain has two side-chains the addition of subsequent blocks to these chains leads to one of the chains being longer than the other (because the hash function makes it unlikely that the nodes continue to simultaneously solve the function) and the nodes all continue to work on this longest chain. At this point the transactions on the shorter chain are removed from the blockchain and must be re-added as authenticated transactions.

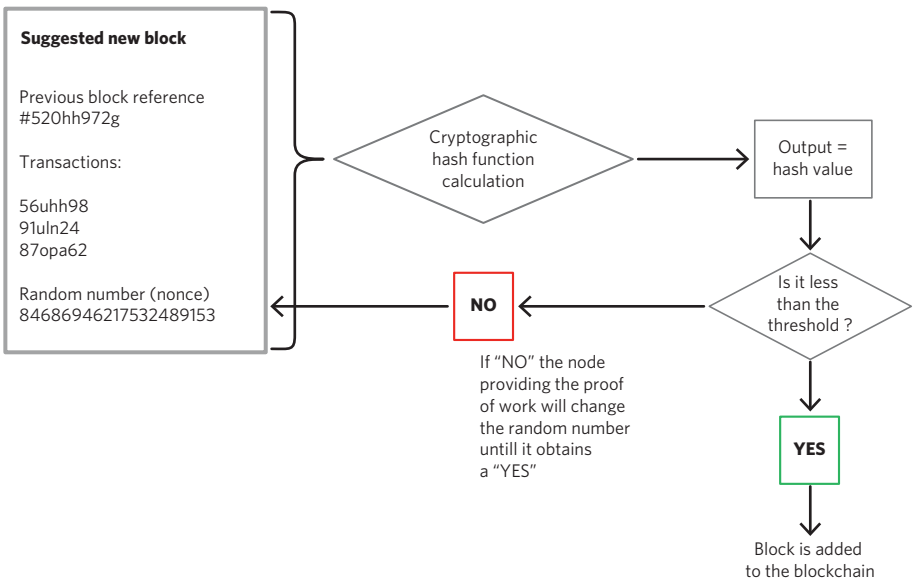
In this way, even if duplication occurs, the blockchain uses this mechanism to correct itself and therefore prevent any potential double-spending.

This process also takes significant computational power and, in this way, acts as a security feature for the blockchain. The system's security could be compromised if a user was able to change existing transactions. To do so a user would need to replace a block in the blockchain and create a new side chain that adds blocks more quickly than the original one, therefore becoming the longest. This would require repeating the process of solving the hash function for each block in the blockchain; estimates on the amount of effort required for this vary between one third and one half of the current processing power of the network (with one half being the most frequently quoted amount).

This approach is expected to be sufficient to maintain the security of the system, in a similar manner to methods in place today that maintain the security of traditional payment systems.

It goes without saying that the system is able to operate effectively when the computing power and the number and speed of transactions are balanced and transactions are authenticated within a reasonably short period of time, hence providing the confirmation of the transaction that would be guaranteed in real time in the case of third party authentication.

Figure 5: Proof of work process and hash function



Source: INNOVALUE research

Image: Shutterstock, #765731981 – rvlsoft / Shutterstock.com

3
CASE STUDY: VIRTUAL CURRENCIES

Although Bitcoin may be the most famous virtual currency, virtual currencies are broader than just Bitcoin as they are any "virtual representation of value".[7] The European Central Bank defines them as: "A type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"[8].

Virtual currencies are classified into three categories based on how they interact with the real economy: (1) closed virtual currencies, (2) Non-convertible virtual currencies and (3) Convertible virtual (digital) currencies

1. Closed virtual currencies

- This category of virtual currencies is not connected to the real economy and can be used only in the platforms they were designed for[9]. Their use is mainly related to online gaming such as "World of Warcraft"

2. Non-convertible virtual currencies

- This category of virtual currencies can be bought, but cannot be exchanged back to fiat currency (once you own this kind of currency you can only use it for the purpose it was acquired). This type of virtual currencies is often used for engaging customers' loyalty for promotional purposes for example with coupons or loyalty points (e.g. Amazon Coin, Facebook credits)

3. Convertible virtual (digital) currencies

- These currencies can be bought and converted back into fiat currencies. This fundamental property means that they are strictly "digital" currencies. The two terms "virtual" and "digital" currencies are often used synonymously; however they have different meanings. The aim of virtual currencies is to purchase virtual "goods / services" (goods or services that exist only on the internet). Digital currencies, instead, are constructed to pay for exchange of goods in "real life" and can be classified in two categories:

  - a. Centralised: currencies that have a centralised depository (like a central bank in the real economy) and a principal administrator (fiat currency). Example: Tibado[10] has launched a digital fiat currency that can be exchanged using mobile and web applications. Tibado uses a cloud-based architecture to enable payments

  - b. Decentralised: currencies that do not rely on a central authority; instead, completely depend on a distributed system of trust. Example: Bitcoin

The most developed and used digital currencies are the decentralised convertible ones, which exist thanks to the blockchain, the underlining technology that allows the exchange. The relation between decentralised digital currencies and the blockchain is indissoluble and is analogous to the relationship between the internet and email (email was the first consumer product that used the technology enabled by the internet).

There are more than 500 decentralised digital currencies (the most popular of which is the Bitcoin)[11] and the market is volatile, with considerable price fluctuations over a short space of time. The total market capitalisation is ~$ 4 billion[12], with Bitcoin accounting for nearly the entire capitalisation of the industry at ~$ 3.45 billion[13]. The second most used virtual currency is Ripple with a market capitalisation of $ 292 million, followed by Litecoin with a market capitalisation of $ 97 million as of June 2015.

However, several fundamental challenges need to be addressed for digital currencies to become more suitable to enable day-by-day transactions for the wider public:

- High volatility with no central authority monitoring or mitigating fiat currency exchange rates
- The risk of inflation or deflation cannot be mitigated or controlled
- Basic concepts of money value, such as time value, are not applicable
- Interest rates for lending and borrowing are arbitrary as there is no reference base rate
- There are practically no monetary policies as there is no supervising or regulatory authority

All these points raise the question about the current suitability of decentralised digital currencies as a widespread payment instrument or as an asset class. Regulators are taking different positions in regards to virtual currencies.

[7] EBA Opinion on 'Virtual Currencies', European Banking Authority, 4 July 2014
[8] 'Virtual Currency Schemes', European Central Bank, October 2012
[9] Although the exchange and interaction with real economy is forbidden, a black market has been developed which allows this exchange to occur
[10] Source: www.tibado.com
[11] http://coinmarketcap.com/all/
[12] Ibid.
[13] Ibid.

The European Bank Authority (EBA)[14] believes that virtual currencies should be regulated at a European level to protect consumers, enhance financial stability and reduce the risk of financial crime. The EBA also argues that pan-European regulation would enhance the single European market. It has therefore invited the European Parliament, council and commission to develop an appropriate virtual currency regulatory regime that includes: a system of authorization, segregation of client accounts, capital requirements, the creation of scheme authorities, customer due diligence, fitness and proprietary standards, transparent price information, and systems and controls to reduce the risk of market abuse.

It is likely to take some considerable time before a regime of this type is developed and brought into force. In the meantime, the EBA has recommended that

(a) national supervisory authorities should discourage credit, payment and e-money institutions from buying, holding or selling virtual currencies

(b) EU legislators should consider declaring market participants, in particular virtual currency exchanges, to become subject to the requirements under the EU Anti Money Laundering Directive.

The current position of the European Central Bank (ECB) is that although virtual currency schemes (virtual / digital currencies) have numerous potential risks, the materialisation of these risks depend on certain risk drivers such as the volume of virtual currencies issued and traded and the rate of user acceptance. As these risk drivers remain low, the ECB's stance is therefore that there is no need to amend or expand the EU legal framework of payment systems. The ECB will however continue to monitor developments in the virtual currencies sector with a view to reassessing the risks over time.

In addition to this, each regulator within a country has often its own perspective. The UK government, has announced as part of its 2015 budget that it will be investing £10 million into a research initiative to study digital currencies.
The government considered that while there are clear barriers to digital currencies achieving widespread use in their current form, the blockchain technology that underpins digital currencies has significant future promise as an innovation in payments technology.

At this early stage, the UK government's objectives[15] for digital currency technology and the sector more widely are as follows:

- to provide clarity and certainty on the application of existing legislation and regulation for users
- to limit any opportunities for criminals or terrorists to use virtual currencies for illicit activities, applying anti-money laundering regulation. The Financial Action Task Force (FATF) has noted the legitimate use of virtual currencies and identified characteristics of virtual currencies that present potential anti-money laundering and counter-terrorist financing risks
- to create the right environment for legitimate virtual currency entrepreneurs to flourish
- to support the research, development and application of new technology
- to support monetary and financial stability in the UK

The UK Government widely perceives[16] the blockchain technology as a positive innovation that facilitates the fast, efficient and secure transfer of ownership of a digital asset over the internet.

Despite this there is currently no specific legislation that addresses virtual currencies and their accompanying risks, however there have been a number of recent suggestions listed in the HM Treasury's 'call for information' report confirming that the UK government intends to apply anti-money laundering regulation to digital currency exchanges in the UK, to support innovation and prevent criminal use. That said, nothing has been confirmed yet.

[14] EBA Opinion on 'virtual currencies' dated 4 July 2014
[15] Digital currencies: response to the call for information, HM Treasury, 3 November 2014, last updated 18 March 2015
[16] Virtual Currencies: the other side of the coin, PLC, October 2013

The biggest challenge is to work out where digital currencies fit within the UK's regulatory financial framework, especially in relation to the following UK legislations:

- Payments Services Regulations 2009 - implementing the EU Payment Services Directive
- Electronic Money Regulations 2011 - implementing the second Electronic Money Directive
- Money Laundering Regulations 2007 - implementing the third Money Laundering Directive

Recent reports have hinted that virtual currencies may be incorporated into the definition of electronic money in the Third Electronic Money Directive although there is very little information thus far.

Furthermore the UK's independent inter-governmental body that promotes policies to protect the global financial system, the Financial Action Task Force (FATF), has recently published their 'Guidance for a risk-based approach for virtual currencies'. This guidance is intended to explain the application of the risk-based approach to anti money laundering measures in the virtual currency context and identify the entities involved in virtual currency payments products and services.[17]

The UK has a number of potential digital currency regulators[18]: the Financial Conduct Authority (FCA), the Bank of England, the Prudential Regulation Authority (PRA); the Payments Systems Regulator (PSR) and HM Treasury.

The FCA has established an 'Innovation Hub' to help innovators develop FinTech products and services that meet the FCA's requirements but there are no FCA publications which suggest that they are proposing to regulate digital currencies just yet. The Bank of England does not believe that digital currencies pose a material risk to monetary or financial stability in the UK, although admitting this could conceivably change, but only if digital currencies were to grow significantly. The Bank will, however, continue to monitor digital currencies and the risks they pose to its mission.[19] The PRA regulates banks, insurers and designated asset managers but not digital currencies. It has the power to discourage some credit institutions from buying, holding or selling, digital currencies, as the ECB has recommended (above), although there is no current reason to think that it will do so. The PSR has not said anything to date which suggests that it may designate or may be required to regulate, any digital currencies in the short or medium term.

In relation to Value Added Tax (VAT), the HM Revenue and Customs have confirmed, for now, that income received from Bitcoin mining activities will generally be outside the scope of VAT. Income received by miners for other activities, such as for the provision of services in connection with the verification of specific transactions for which specific charges are made, will be exempt from VAT under Article 135(1)(d) of the EU VAT Directive as falling within the definition of 'transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments'.[20]

On the other hand, the US government has taken several steps towards regulating digital currencies, in particular Bitcoin. The most important law leveraged by the government has been the Bank Secrecy Act. In 2013, FinCEN, the Agency authorised to enforce the Bank Secrecy Act, issued guidance on the applicability of regulations to digital currencies[21]. Since then, both federal and state authorities have been actively scrutinising Bitcoins activities.

In the US, the New York Department of Financial Services (NYDFS) published its final BitLicense regulations for virtual currency businesses in June 2015. The BitLicense was officially adopted by the NYDFS on 24th June 2015 after it was published in the New York State Register. Although the measures contained in the BitLicense are specific to New York, they are certain to have wider relevance. The state's importance as a financial centre and the lengthy consultation process mean that other states will likely look to New York for guidance on how to deal with digital currency services. Furthermore, the release of the BitLicense sets a precedent for other states that have been holding back to see what the final iteration of the regulation looked like in practice – as well as how it was received by the businesses and customers affected by it –. For digital currency initiatives, however, the full impact of the BitLicense has yet to play out.

The above provides an illustration of the different regulatory frameworks in which digital currencies are currently operating. Different countries have taken different positions in regards to digital currencies, and in particular in regards to the Bitcoin, and hold very different views on its supervision, monitoring and tax treatment. Overall it is likely to see an increase of regulation on digital currencies.

[17] FATF – Guidance for a risk based approach – Virtual Currencies dated June 2015
[18] HM Treasury – Digital currencies: response to the call for information
[19] Bank of England Quarterly Bulletin 2014 Q3: The economics of digital currencies
[20] HMRC - Policy paper: Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies
[21] Ibid.

4
BLOCKCHAIN DEVELOPMENT AND FUTURE APPLICATIONS

If Bitcoin was v1.0 of the blockchain's application, then v2.0 has already launched with a plethora of companies leveraging and developing new applications for the blockchain and serving a range of customer needs. Similar to the evolution of the internet, each phase of development leads to new applications and each phase is a significant development compared to the previous phase.

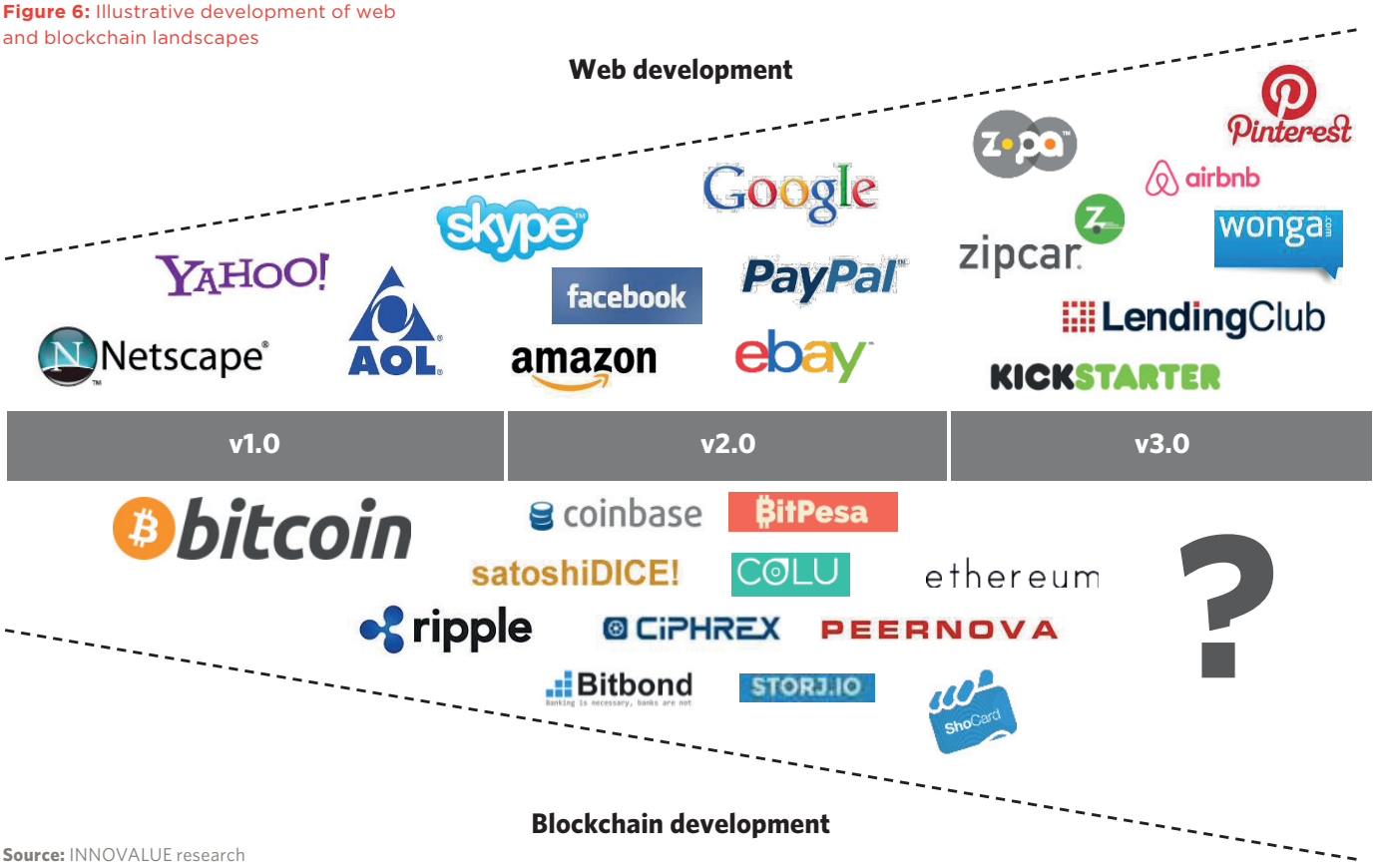
The variety of companies working on v2.0 of the blockchain shows evidence of its potential versatility.

Not only is it used to support value exchange in the form of a virtual currency, but it is also being used to support "programmable money" where a transaction can occur only if certain conditions are met (e.g. to make a crowdfunding donation only if the required threshold for pledges is met).

The blockchain is also being used for the more complex transactions, whereby the ownership of an asset is defined in the digital world and changes in ownership are managed through the blockchain (e.g. documenting intellectual capital for an idea to provide proof of ownership during patent disputes).

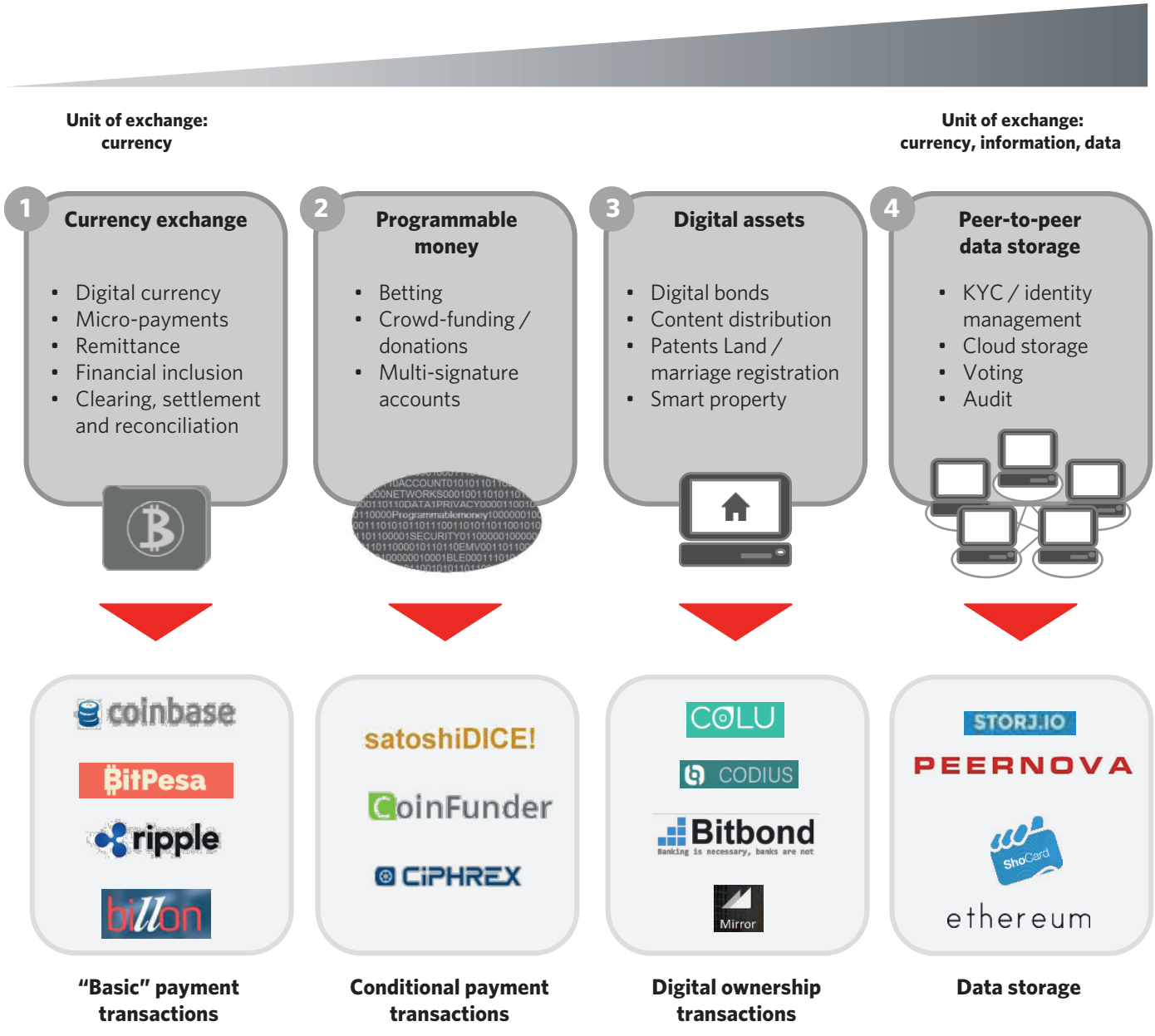
Finally, the distributed nature of the blockchain is facilitating a new range of databases, where each member of the network can access and store information (e.g. peer-to-peer data storage). Figure 7 and the following paragraphs provide illustrative examples of these opportunities.

Figure 6: Illustrative development of web and blockchain landscapes



Source: INNOVALUE research

Figure 7: Possible applications of the blockchain



Source: INNOVALUE research

4.1 CURRENCY EXCHANGE

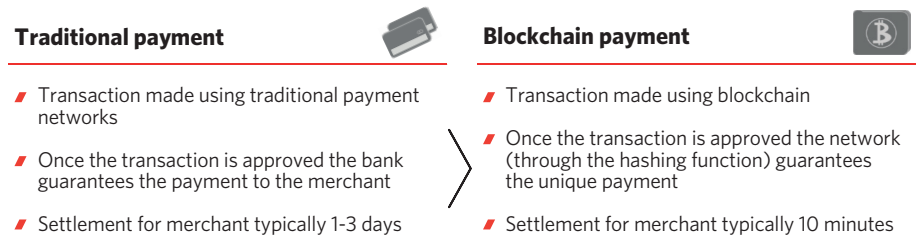
The blockchain is able to provide real time payments, 24/7 with rapid settlement and without requiring a bank account. Bitcoin has been the first application of the technology to gain consumer interest, nonetheless those capabilities can also be leveraged to enable other type of payment functionalities.

Examples of how this is being leveraged are below:

- Coinbase[22] (and others) are looking to apply the blockchain to micropayments, offering to process micro transactions for free and instantly.
- BitPesa[23] (and others) are leveraging the blockchain aiming to gain a share of the $540m[24] remittance industry by offering cheaper, "instant" remittances. BitPesa's business model is based on the ability to use Bitcoin as a foreign currency clearing and international transfer instrument between two different currencies. This is done by converting the sender's value denominated in a fiat currency into Bitcoin at point of receipt and, almost at the same time, to re-convert Bitcoin into the receiver's fiat currency – de facto bypassing the complexity, cost and lengthy clearing and settlement processing cycles required by a correspondent banking network. The instant conversion into and from a Bitcoin, minimize the volatility risk derived from using the Bitcoin.
- Billon[25] is utilising the fact that an internet connection, and not a bank account, is required for payments to provide a potential solution for financial inclusion. Billon allows a mobile device or a computer to become a wallet and enable peer-to-peer payments by leveraging the blockchain technology.
- Commonwealth Bank of Australia has set up a blockchain application to clear and settle payments between its subsidiaries[26] since a pure payment system powered by the blockchain could eliminate the clearing and settlement process.

While the Bitcoin is a virtual currency, other alternative network models based on fiat currency are emerging, potentially creating new clearing networks for transactions.

Figure 8: Comparison between traditional payments and blockchain-based payments



[22] Source: www.coinbase.com
[23] Source: www.bitpesa.co
[24] Source: World Bank
[25] Source: billoncash.com
[26] Source: CIO Australia

4.2 PROGRAMMABLE MONEY

Industry professionals characterise digital currencies as 'programmable money', or money with 'in-built functionality', enabling users to encode requirements into a payment instruction in order to achieve autonomous, self-executing contracts ("smart contracts").

The blockchain is an enabler for transactions where the payment is made only after specified conditions are met (i.e. "programmable money"). Software is used to set up a contract to specify the payment details and the conditions required to be met before the transaction takes place. The conditions can be based on publically available information (e.g. a bet on who will win the world cup). As such, the software is programmed to check when the conditions are met and instruct the payment.

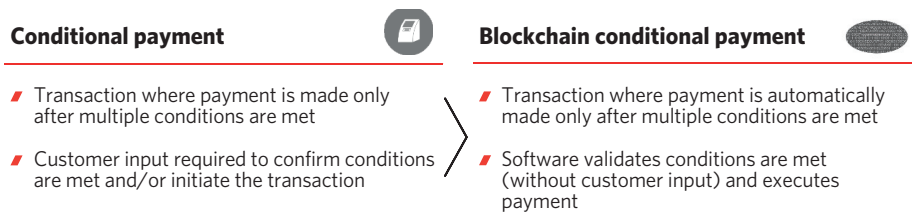
Examples of companies offering these services are:

- SatoshiDice ("The original blockchain based bitcoin dice game") which at times has comprised ~50% of blockchain transactions[27] is perhaps the most prominent provider of gambling / betting services on the blockchain.
- CoinFunder[28] has developed a donation based crowdfunding tool in order to finance new projects with Bitcoins.
- Ciphrex[29] provides a digital currency wallet that requires signature from multiple parties, relevant for payments that require the agreement of several parties before the payment is made.

Contributors to the HM Treasury's 'call for information' said "the technology could be used for more efficient property transfers, or for loan repayments, where payment could automatically take place or be adjusted once specified conditions are met".

However, smart contracts raise a number of legal issues. Firstly, their automatic and enforcing nature would make it difficult to apply conventional contract law. They may not be voidable or there may not be any form of consumer protection. Resolving any disputes over the irreversible and 'automatically completed' nature of these contracts may be very hard to deal with. Furthermore, privacy concerns would also be a factor. Contracts between parties would be publicly viewable in the ledger.[30]

Figure 9: Comparison between conditional payments with a traditional method and blockchain conditional payments



[27] Source: Bitcoin magazine
[28] Source: coinfunder.com
[29] Source: ciphrex.com
[30] Bloomberg Banking Report, 104 BNKR 654, 31 March 2015

4.3 SMART PROPERTY

In addition to transactions that are largely payment / currency focused, the blockchain can also be leveraged to support "transactions of information". Transactions in the blockchain can include additional details about the unit being exchanged. Smart property is property whose ownership is controlled via the blockchain using 'smart contracts' (above) which are contracts enforced by computer algorithms that can automatically execute the stipulations of an agreement once predetermined conditions are activated.

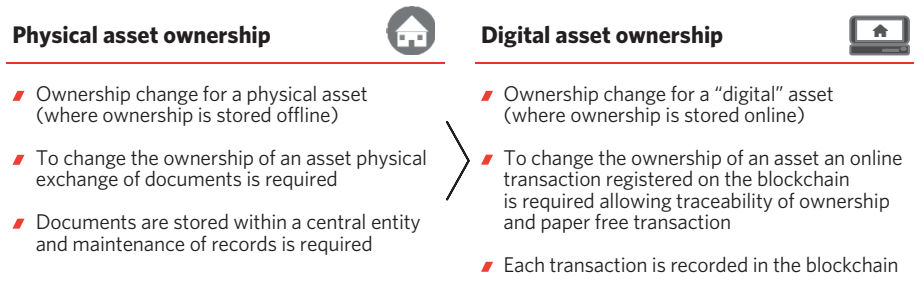
Examples of smart property include stocks, bonds, houses, cars and commodities. By harnessing the blockchain technology as both a ledger and trading instrument, the "Coloured Coins" protocol functions as a distributed asset management platform, facilitating issuance across different asset categories by individuals as well as businesses.[31]

Examples of companies leveraging this are below:

- Colu[32] uses this protocol to digitalise the assets of a corporation and transfer ownership of them on the blockchain with the aim of simplifying their exchange and maintaining a transparent record of ownership.
- Codius[33] provides platforms to securely encode smart contracts in a blockchain. They claim that this technology can be applied to any asset or contract that can be digitalised.
- Bitbond[34] provides peer-to-peer lending services which provide loans without requiring the lender to hold or borrowing a bank account.
- Mirror[35] has implemented a system to exchange financial contracts by using the Bitcoin blockchain. The company enables the creation and the settlement of P2P smart contracts.

This type of application may have the potential to transform businesses such as custody banking, as assets would not be required to be held physically by custodians banks in order to provide guarantees of ownership. This could have a significant impact on the global economy as the technology permits property ownership to be transferred in a safe, quick, and transparent manner without an intermediary. There are many other potential opportunities including linking telecommunications with blockchain technology. This could, e.g., provide car-leasing companies the ability to automatically deactivate the digital keys needed to operate a leased vehicle if a loan payment is missed.

Figure 10: Comparison between physical asset ownership and digital asset ownership



[31] CMM Research Note – The Internet of Finance: Unleashing the Potential of Blockchain Technology, 16 April 2015
[32] Source: colu.co
[33] Source: codius.org
[34] Source: www.bitbond.com
[35] Source: mirror.co

4.4 PEER-TO-PEER DATA STORAGE

The blockchain can be used as a trusted P2P network for document storage. Applications for the blockchain can be used to "upload" files to the network. The file is "split" into several parts and each part is separately encrypted with the digital signature of the sender (this process follows the same procedure explained in the illustration on the "overview of the blockchain process"). The parts are then stored on network users devices if they have available space and have agreed to "rent" this space in return for a fee. The blockchain records this as a "transaction" with the details of the sender, the receiver and the unit.

This allows the application to locate the document parts for the user when they wish to retrieve it.

- Storj[36] has applied this principal to create a system for which information and documents can be stored using an encrypted peer-to-peer network and exploiting the available space on a computer of another user. Storj's users can rent out the available space in their computer.

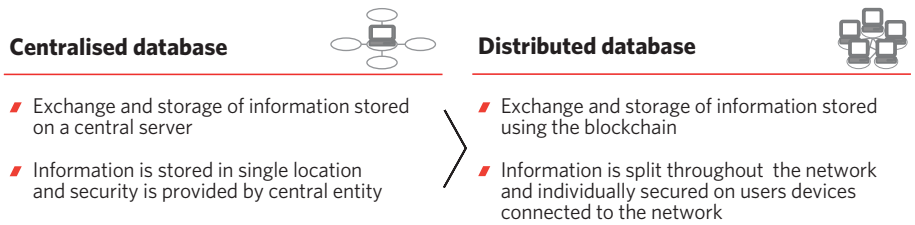
- Peernova[37], using the same technique as Stroj, is able to build a system to store any sort of documentation using the blockchain such as: audit archives, healthcare records, government information and financial reports.

- Leveraging the same principal, ShoCard[38] has developed a way to store your personal information and identity documents using the Bitcoin's blockchain, simplifying the document collection that would be part of a KYC process required by financial institutions.

Companies such as Ethereum[39] have also been implementing the blockchain technology to provide end to end services, covering the majority of four categories described in this section. Therefore, they are able to provide solutions for crowdfunding, voting systems, smart properties, financial exchanges and company governance.

The companies described above, and more, are providing new solutions to meet customer needs that can be serviced through the blockchain. This could lay the foundation for future developments where peer-to-peer transactions are conducted through the blockchain.

Figure 11: Comparison between centralised database and distributed database



[36] Source: storj.io
[37] Source: peernova.com
[38] Source: www.shocard.com
[39] Source: www.ethereum.org

Figure 12: Different reported approaches to leverage the blockchain technology

Strategy	Incumbents	Blockchain company	Description
1 In-house development	NASDAQ	In-house	Record-keeping and transfer security for its private market platform
	citibank	In-house blockchain system and digital currency (Citicoin)	Cross border transactions
	LHV pank	In-house through CuberTechnology	Programmable money for the storage, management and transfer of liquidity
2 Investment	Goldman Sachs	CIRCLE	Digital currency storage, conversion and transaction services
	BBVA, USAA, NYSE	coinbase	Bitcoin platform and wallet. 2.3 mn users and 39k merchants (June 2015)
3 Partnership	WESTERN UNION	ripple	Faster international payments, real time clearing and settlement (Western Union)
	fidor BANK		Instant € / $ FX transaction (Fidor)
	cross river bank		International real-time payments (US – Western EU)
	PayPal	coinbase, bitpay, GOCOIN	Bitcoin payment acceptance methods for merchants (via subsidiaries)
4 Accelerators	UBS, BANK OF ENGLAND	L39	Fintech accelerator focussed on blockchain
	BARCLAYS	safello, Atlas Card, Blocktrace	Fintech accelerator with 2015 focus on blockchain solutions for the insurance industry
Interest announced	ING, intel, RBS, IBM, Santander, BNP PARIBAS, Deutsche Bank, Board of Governors of the Federal Reserve System	n.a.	Public announcements of interest in blockchain and potential future developments (details not released)

Source: company press releases, INNOVALUE research

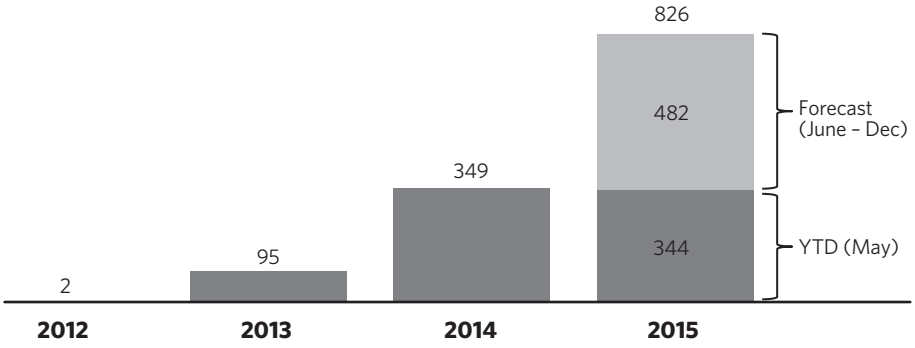
5
HOW INCUMBENTS ARE LEVERAGING THE BLOCKCHAIN

Four different strategies have been adopted by established business models or "incumbents" to leverage blockchain technologies:

- Develop an in-house platform - e.g. in May 2015, NASDAQ launched a blockchain ledger to improve the stock management capabilities of its private market platform[40], and a month later, announced a partnership with Chain, a provider of blockchain infrastructure, to optimise the exchange processes of shares.
- Directly invest in blockchain companies - e.g. Goldman Sachs acts as a Venture Capitalist in the Bitcoin's blockchain space[41].
- Partner with existing blockchain companies - e.g. during the 'Milken Institute's Global Conference 2015,' Chris Larson (CEO Ripple) and David Thompson (CIO Western Union) announced a partnership between the two companies to implement a remittance blockchain system.
- Study the possible application through an accelerator - e.g., UBS opened an office in Level39, a London based FinTech accelerator, to research innovative Eblockchain applications[42].

A growing number of both corporate and institutional incumbents are announcing their interest in the possible implementation of the blockchain[43] and the pace of investment in Bitcoin / blockchain companies is increasing with ~$95mn invested in 2013, ~$350mn invested in 2014 and ~$344mn already invested from January to May 2015[44].

Figure 13: Venture Capital yearly investments ($m) in companies developing Bitcoin's blockchain applications (Global)



Source: coindesk.com, INNOVALUE research

[40] Source: Nasdaq official press release, 11/05/15
[41] Source: Finextra
[42] Source: Level39 press release
[43] Different stages of interest are shown by incumbents. E.g., Santander has published a paper that includes the potential benefits of the blockchain to financial institutions (see The FinTech 2.0 Paper). RBS, as part of its plan to invest £3.5 bn in technological development, is discussing a 'proof of concept' with Ripple to automate bank transfers
[44] Source: Coindesk.com

6 CONCLUSIONS

The blockchain is an innovative solution to the process of completing information exchanges and transactions. As with all technical advances, it is undergoing progression from initial launch for niche applications (e.g. a digital currency) to potential large scale adoption by businesses and governments.

The internet revolutionised how people communicate with each other across the globe and it is conceivable that the blockchain could have potential to change the way information is exchanged and transactions are completed.

While the usage of digital currencies is presently low, and there are a variety of challenges that are likely to prevent their widespread adoption in the long run, digital currencies may still pose a threat to traditional fiat currencies in the future. What digital decentralised convertible currencies (like Bitcoin) have proven is that they are just the tip of the iceberg of what the blockchain is capable of. It remains to be seen whether the innovative blockchain technology will be adopted widely enough to become a force in the global economy. Many technical modifications and improvements to its design including regulation, governance procedures and costs would still need to be considered.

Moreover, the blockchain is promoted as an inexpensive payment technology, there are still associated costs which can be significant. The blockchain relies on nodes that store a copy of the ledger as well as nodes that compute the hash function both of which require time, electricity, maintenance and appropriate hardware.

Currently, for example, the nodes are incentivised by Bitcoins – they receive an amount of "new" Bitcoins with the creation of the block and they receive any transaction fees that the sender had elected to pay (e.g. for complex transactions). At today's market value for Bitcoins, the average node's revenue per transaction[45] is ~$7. It is up to the nodes to ensure that this value is sufficient to cover their running costs (many speculate that only those users with a very efficient IT infrastructure can achieve profitability). Anyone receiving payment in Bitcoins (nodes and merchants) is also subject to volatility risk due to the fluctuations in price. This can be mitigated with a value guarantee, which is offered by some Bitcoin exchanges for a fee of 2-3% of the transaction value. This leads to the conclusion that, despite the Bitcoin's marketing message that a Bitcoin transaction cost is very low, the actual total full-cost of a Bitcoin Fx guaranteed transaction for a merchant could be much more expensive than the vast majority of any domestic or international card transaction.

» …companies should develop strategies and business models that leverage the blockchain as an enabler that can be core or complementary to their business.

[45] Source: blockchain.info

In general terms, there are several factors which could potentially increase the costs of using blockchain for the applications discussed in this report:

- Regulation: Currently, the blockchain is not subject to the same level of regulation as traditional payment / banking institutions and therefore, blockchain companies do not need to invest at the same levels to ensure regulatory compliance.

- Incentives: Solving the hash function is time and energy consuming for the nodes and incentives in the form of Bitcoins are used; appropriate incentives need to be considered for new applications/ chains (Bitcoin or others).

- Computational power: lower computational power reduces the effort required to recreate the proof of work for all the blocks in the blockchain (which would potentially allow a hacker to manipulate the system); sufficient power in the network is required to create a barrier against hacking.

- Space: as a ledger, the blockchain is increasing in size as more transactions are completed (growing from ~8,000MB in June 2013 to ~36,000MB in June 2015). The size of the blockchain ledger is already exceeding the capability of some devices (e.g. mobile phones with memory of 32Gb or less). As this growth continues it will exceed the storage space available from average users, leaving a vast part of the public unable to participate or resulting in delays in processing transactions.

These points should be considered when developing a strategy to adopt blockchain technology since they could increase the actual total cost (inclusive of power, hardware and software depreciation, etc.) that is incurred by the network participants to validate a transaction.

However, the number of organisations leveraging the blockchain as well as the range of initiatives from established organisations suggest that this is a technology that is being seriously considered although its full potential and applicability is still far from having been fully explored. At this point in time, organisations should be considering the potential of the blockchain and the level of disruption it will cause them based on their industry, positioning and organisational maturity. On this basis, companies should develop strategies and business models that leverage the blockchain as an enabler that can be core or complementary to their business. It is also important to keep in mind that an implementation doesn't necessarily need to be designed in-house, but can rather take the form of selective partnering or investing.

Image: Shutterstock, 110678570 = rvlsoft / Shutterstock.com

ABOUT LOCKE LORD

www.lockelord.com

Locke Lord is a full service, international law firm with offices in London, Hong Kong and 11 U.S. cities, and a full range of practice and industry areas that serve international and domestic clients worldwide.

Our London Office is a gateway for the Firm's international work in the UK, Europe, the Middle East and Asia, and is home to a world-class team of lawyers dedicated to providing the best service possible to clients around the world.

Having established a presence in London more than 25 years ago, Locke Lord opened a much larger, full-service office in early 2012, and as part of the Firm's strategic plan, assembled a team of leading lawyers with many years of experience. From major corporations and financial institutions to individuals and overseas-based investors, our clients trust the Firm's strong capabilities and excellent representation in the areas of, banking and finance, cards & payments, capital markets, corporate M&A, dispute resolution, employment, energy, insurance & reinsurance, real estate and restructuring & insolvency.

As an integral part of Locke Lord's global presence, the London office collaborates daily with the wider network of the Firm's 650-plus colleagues across the U.S. and Hong Kong. Our combination of proactive, barrier-free communication offers clients the best resources available to tackle their issues both complex and straightforward.

Our strength is understanding the challenges faced by our clients and delivering a tailored solution to meet their individual objectives. In particular, our lawyers employ a very entrepreneurial approach to their client relationships. As well as providing sound legal advice and guidance to meet client expectations, they also regularly bring together parties when they believe that such introductions would be beneficial to their clients.

Strong leadership and deep roots in the UK are the essence of Locke Lord's London office. Our London lawyers are consistently recognised by well-regarded law firm ranking organisations, including Chambers UK 2013, and the Legal 500 2012, which list them among leaders in their fields. Along with our many London and U.S. clients, Locke Lord's London office also serves clients throughout Europe and Asia.

For further information, please contact:

Robert Courtneidge
Global Head of Cards & Payments
rcourtneidge@lockelord.com

Siobhan Moore
Senior Associate, Cards & Payments Team
shmoore@lockelord.com

Vicky Lloyd
Senior Associate, Cards & Payments Team
vlloyd@lockelord.com

Charlie Clarence-Smith
Member of Global Cards & Payments Team
cclarence-smith@lockelord.com

ABOUT INNOVALUE MANAGEMENT ADVISORS

INNOVALUE is a leading strategic management advisory firm dedicated to the financial services industry. INNOVALUE's clients are global or national market leaders, regional specialists, innovators and entrepreneurs that have trusted INNOVALUE for over a decade as their preferred advisors. In the three practices – Payments, Banking and Insurance – INNOVALUE has a distinctive industry know-how based on years of experience, deep and tested insights and established methodologies. The industry practices are complemented by two cross-functional service lines: Corporate Finance and INNOVALUE Solutions.

What makes INNOVALUE unique is our value proposition that is based on:

- **Excellent industry knowledge:** INNOVALUE's expertise is a result of deep and unrivalled knowledge of the financial services industries Payments, Banking and Insurance. Since our founding, we have consistently focused on those industries strengthening our comprehensive and deep topical knowledge.

  Our clients have realised that few management advisory firms hold a comparable level of expertise in our industries of focus.

- **Collaborative advisory:** the best advice is never developed in isolation, behind closed doors, but in partnership with the client. Hence INNOVALUE's team work as "one team" through a collaborative approach with the clients' team. This partnership not only makes a difference in terms of quality and value of our advice, but also contributes to a positive impact at a personal level through mutual trust. These factors provide the foundation for recommendations and conclusions that are endorsed, shared and supported, and ultimately implemented, within the client's organisation.

PAYMENTS EXPERTISE

- Card Issuing
- Merchant Acquiring
- Processing
- Consumer credit
- Loyalty and Value Added Services
- Core and corporate payments
- Transaction banking
- Online Payments
- Mobile Payments
- Digital Commerce
- Digital identity
- Digital industry convergence
- ATMs, mobile, branch and distribution channels

FUNCTIONAL EXPERTISE

STRATEGY

- Market Entry Strategy
- Product And Pricing Strategy
- Regulation
- Sales And Marketing

OPERATIONS

- Operating Model
- Restructuring
- Cost Reduction
- Post Merger Integration

CORPORATE FINANCE

INNOVALUE SOLUTIONS

www.innovalue.com

- **Actionable strategies:** the value of a good strategic analysis which does not stand a chance of being implemented for whatever reason is none. This is why INNOVALUE's consultants take particular care that recommendations are realistic, feasible, endorsed, shared and supported, and ultimately implemented. At INNOVALUE, this is one of our core principles – as INNOVALUE delivers "high-value consulting, down to earth".

- **Tangible results:** feedback that INNOVALUE receives at the completion of each project shows that INNOVALUE's work provides genuine added value. INNOVALUE strives to create an extraordinarily high "return on consulting investment" – and practically all of INNOVALUE's clients would unreservedly recommend us. These are values which bring back to INNOVALUE's fourth, and perhaps most important principle: INNOVALUE always makes a tangible and relevant contribution to the competitiveness of its clients.

INNOVALUE supports its clients internationally from the offices in Hamburg, Frankfurt and London.

FRANCESCO BURELLI
Partner

INNOVALUE Management Advisors Ltd.
3 More London Riverside
London, SE1 2RE
United Kingdom

E-MAIL burelli@innovalue.com

Financial Services and Social Media // Francesco Burelli // **Q3** 2015

INNOVALUE

HAMBURG

Heimhuder Straße 69
20148 Hamburg
Germany

FRANKFURT

Siesmayerstraße 21
60323 Frankfurt am Main
Germany

LONDON

3 More London Riverside
London, SE1 2RE
United Kingdom

www.innovalue.com