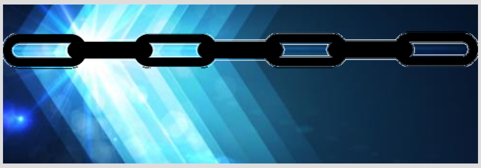
PROGRESSIVE
EQUITY RESEARCH

9 July 2015

# BLOCKCHAIN, BITCOIN AND BEYOND…

## EXCITING TECHNOLOGY WITH CONSIDERABLE PROMISE



### DIGITAL CURRENCIES

*"The emergence of private digital currencies has shown that it is possible to transfer value securely without a trusted third party….the distributed ledger technology that their payment systems rely on may have considerable promise. This raises the question of whether central banks should themselves make use of such technology to issue digital currencies."*

***Source: Bank of England, February 2015: One Bank Research Agenda Discussion Paper***

### TECHNOLOGY HOLDS REAL PROMISE

*"The government considers that while there are clear barriers to digital currencies achieving widespread use in their current form, the 'distributed ledger' technology that underpins digital currencies has significant future promise as an innovation in payments technology. The government wishes to foster a supportive environment for the development of legitimate businesses in the digital currency sector……"*

***Source: HM Treasury, March 2015: Digital currencies: response to the call for information***

### ANALYSTS

Gareth Evans

+44 (0)20 7349 5156

gevans@progressive-research.com

Ian Poulter

+44 (0)20 7349 5156

ipoulter@progressive-research.com

## Blockchain technology – digital evolution

**Blockchain technology is evolving the way that information can be stored, monitored and accessed securely. Blockchains use available computing resource to make accessible ever-changing and growing sets of information. Whereas the internet is good at transmitting data, blockchain technology is good for storing and maintaining an agreed version of a steadily-expanding set of data, to which many participants need access. This is perfect for a stored list of digital currency transactions (such as bitcoin).**

- Blockchain technology facilitates the fast, efficient, and secure transfer of ownership of a digital asset over the internet, providing a permanent record of what has taken place, and without the need for a single trusted third party to oversee the process.
- Network participants make computer processing power available in order to validate sets of transactions (blocks) through solving a proof-of-work "puzzle". Through this process, the new blocks are added to the blockchain.

## Bitcoin – a recognised digital currency

**Bitcoin is a digital currency (often likened to electronic cash) which can be distributed peer-to-peer through instant transfer over the internet. It is a "digital" currency as it only resides in the digital world. Digital currencies both resemble money and need their own dedicated payment systems. Ownership of each bitcoin is recorded in the Bitcoin blockchain. Although not yet classed as legal tender by regulators, digital currencies' growing popularity warrants attention and bitcoin's relationship with existing financial systems is evolving fast.**

- As a peer-to-peer network, bitcoin does not require an intermediary to verify transactions. Each transaction is verified through the bitcoin network using cryptography and computer processing power before it is added to the blockchain.
- Network participants ("miners") receive bitcoins in return for processing and verifying transactions.

## Beyond…other uses of Blockchain

**Blockchain technology has a large number of applications in non-bitcoin related areas such as asset transfers, supply chain monitoring and decentralised telemetry.  See page 6 for more examples.**

- Many companies and organisations - including Nasdaq and IBM - are already using or exploring the potential of blockchain technology.
- Governments are committing significant investment to exploring the technology and to determine the best way to support its development.

**This marketing communication has not been prepared in accordance with requirements designed to promote the independence of investment research. Please refer to important disclosures at the end of the document.**

# Blockchain

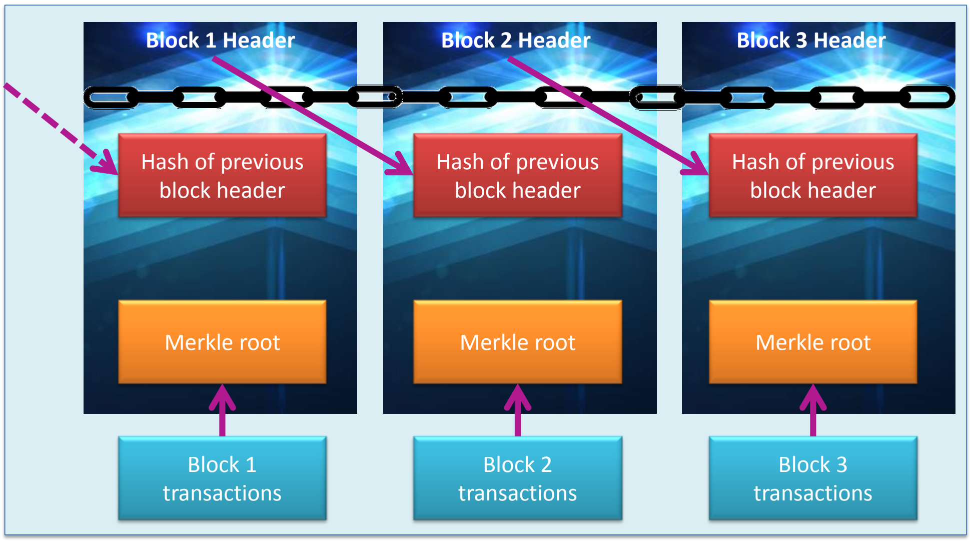
## Transaction database

Blockchain technology has been made possible by advances in cryptography, internet performance and computing power. A blockchain is a transaction database shared by any computer that connects to the network that runs it. It is a method of tracking and transferring digital assets online without the need for a common trusted party. Each block is a permanent record of the transactions that have not previously been recorded in any prior blocks. New blocks are added to the end of the blockchain and they can never be changed or removed.

Today, the most widely used blockchain-based system is Bitcoin and, given its size and historical precedence, it is commonly referred to as *the* blockchain. The blockchain is a public ledger of all transactions in the bitcoin network. For digital currencies like bitcoin, a full copy of its blockchain contains every transaction ever executed in the currency.

A blockchain is built up from the first (genesis) block with each new block adding to the blockchain. The blocks remain in chronological order within the blockchain. Each new block contains references to the previous block through the use of a 'hash function' which is used to create a digital fingerprint of the block contents. This has the effect of creating a chain of blocks from the genesis block to the most current block.

**Adding blocks to the blockchain**



***Source: Progressive Equity Research***

## Mining and miners

Miners are individuals, sometimes working as a group, who make computer processing power available in order to validate a set of transactions (a block) and add this to the blockchain. They run computer systems to repeatedly calculate hashes with the intention of creating a successful block and, in the case of bitcoin, earning coins from transaction fees and new coins created with the block itself. Miners keep a digital currency system running smoothly and prevent the introduction of false units or the double-spending of units. In essence, every blockchain has to have value and mining has to exist to maintain a blockchain.

The process of mining involves solving a proof-of-work puzzle. Miners monitor the blockchain network for new transaction data. This is essentially a trial-and-error process – to which miners have to apply significant computing power – to find the random number that, in combination with the known information on the blockchain and any new transactions, results in confirmation of the validation of a new block.

The key to a proof-of-work puzzle being solved is that the network of miners is so large that someone finds a solution, on average, every 10 minutes. As the chain of puzzles and solutions increases, so the likelihood of it being tampered with reduces. Only the first miner who solves the block "puzzle" receives payment.

Miners receive payment for supporting and administering the blockchain. However, it is worth noting that every four years the amount paid to miners for supporting the blockchain halves – hence their keenness on securing transaction fees and the competitive nature of mining.

The mining system is a clever way of ensuring three things:

- sufficient computing power to manage and store new transactions as they happen
- continual checking of the blockchain for validity of transactions
- distribution of this workload and verification to a number of miners globally, to reduce the risk of any one organisation or miner taking control of the chain

# Bitcoin and digital currencies

## Bitcoin

Bitcoin is a digital currency (often likened to electronic cash) which can be transferred instantly over the internet. It is a "digital" currency as it only resides in the digital world. Digital currencies both resemble money and need their own dedicated payment systems. Some digital communities have created and circulated their own currencies for exchanging the goods and services they offer, and thereby provide a medium of exchange and a unit of account for that particular digital community.

A digital currency can offer pseudo anonymity to its users and operates outside legacy financial systems and jurisdictions. While that is popular with some, it is a concern to regulators and law enforcement bodies.

Bitcoins are the currency units of the Bitcoin system. Bitcoin's value comes from people willing to accept it as payment. However, if no-one is prepared to accept it, the value of bitcoin would be zero. As a digital currency, a bitcoin is just a number associated with a bitcoin address which represents a possible destination for a bitcoin payment.

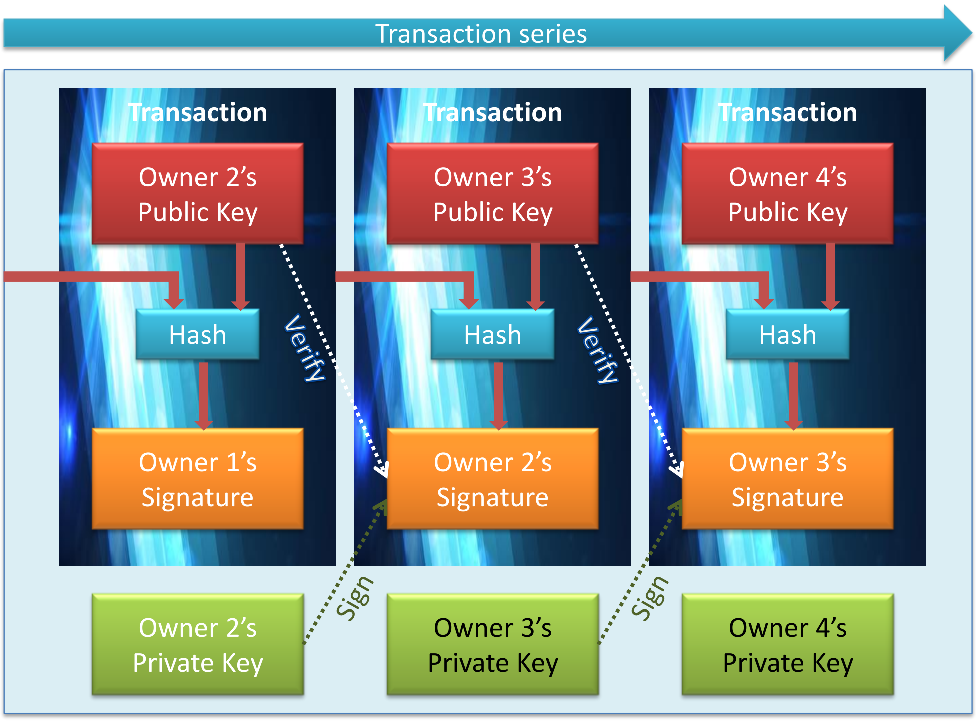
### Wallets

Bitcoin wallets are used to store the secure digital keys which are used to access bitcoins and sign transactions. There are a variety of wallets including desktop wallets which are installed on a computer, mobile wallets which are run as apps on smartphones, web-based hosted wallets, and hardware wallets which are dedicated devices. These can all store the private keys for bitcoin addresses.

## Making and recording transactions

Ownership of a bitcoin is recorded in the Blockchain as described above. Owners of bitcoins have Public Keys and Private Keys with which they can receive, and make payments in, bitcoins. The Public Key is the address to which bitcoins are sent. A Private Key is a secret code which allows the user to cryptographically prove the ownership of his or her bitcoins. The bitcoin blockchain address can be derived from the Private Key, but not vice versa.

**Bitcoin transaction process**



***Source: Progressive Equity Research***

## Micropayments/Nanopayments

A micropayment is an e-commerce transaction involving a very small sum of money often in exchange for something made available online, such as an application download, a service or reading content. Small amounts can also be paid by advertisers to those hosting or delivering their marketing content. These payments can be as low as a fraction of a penny and are also known as nanopayments.

Bitcoin blockchain technology offers huge potential for enabling nanopayments. Unlike the traditional payment model where security is handled within the transaction itself and by the authentication of the issuer, security for nanopayments is associated with the token or means of payment – ownership of the bitcoin (or fraction thereof) is built in to the blockchain; by removing the need for formally identifying both parties to the transaction, major cost savings can be achieved.

The large number of tiny transactions has implications for the size of the blockchain and the value to miners of validating transactions. The recent implementation of 'payment channels' has made it possible to overcome this challenge by aggregating very small payments.

## Digital currencies generally

Historically, digital currencies were a type of unregulated digital money which was issued and usually controlled by its developers, and used and accepted among the members of a specific digital community – often associated with gaming. Currently, they are likely to be more global in nature such as bitcoin or Ven. Those digital currencies act like any other convertible currency, with two exchange rates (buy and sell), which can subsequently be used to buy digital goods and services, but also to purchase real goods and services.

### Digital versus electronic money

Many people use electronic money and e-wallets or similar products have been available for a number of years. Digital currencies differ from electronic money because the currency being used as the unit of account has no central authority counterparty with legal tender status. There are several points to note as a result:

- As digital currencies are usually issued by non-financial private companies – and there is no involvement of traditional financial participants such as central banks - typical financial sector regulation and supervision arrangements are not applicable.
- Forex is unregulated but participants in foreign exchange are mostly regulated. Similar regulation is likely to apply to participants in the exchange of digital currencies.
- As the currency is denominated differently, complete control of the digital currency lies with its issuer who has the freedom to govern the currency and manage the supply of money. Without the need for a trusted third party, regulation of the supply of coins in a digital currency system is upheld by the protocol of the system.

## The balance between regulation, innovation and investment

While most commentary acknowledges the potential usefulness of blockchain technology, financial bodies and governments often cite the need to regulate digital currencies such as bitcoin. Consequently, if digital currencies want to interact with traditional financial markets, they face increasing regulation. The question is: will it be a heavy, or light, touch approach to regulation?

Essentially, regulation needs to reflect the risks but the protocols which underlie digital currencies should add inherent protection to the currency systems in terms of the supply of money and the valid completion of a transaction.

In March 2015, the UK's Treasury published comments on perceived benefits and risks associated with digital currencies which were identified by respondents to its call for information on the subject. It noted that respondents had identified potential benefits offered by digital currencies as a payment method – particularly the potential for cheaper and faster payments. Decentralised digital currencies could also provide a more efficient infrastructure for the transfer of money by removing the need for traditional intermediaries. In addition, digital currency networks could aid the provision of payment and other financial services to those currently unable to access such services such as individuals who cannot open traditional bank accounts.

The risks which were identified in the Treasury's publication fell into three broad categories:

- Crime;
- Risks to users; and
- Monetary and financial stability

There are a number of initial, proposed, responses to those risks which include respectively:

- the intention to apply anti-money laundering regulation to digital currency exchanges, to support innovation and prevent criminal use;
- a framework for best practice standards for consumer protection developed by the government and the digital currency industry; and
- monitoring of developments by the Bank of England

It is worth noting that, in September 2014, the Bank of England stated that digital currencies did not pose a material risk to financial stability in the UK at that time. However, it did note that this could change if digital currency usage was to increase significantly.

Importantly, though, The UK's Financial Conduct Authority has committed to open its doors to financial services firms who are developing new approaches, to help them navigate the regulatory system and identify areas where the regulatory system needs to adapt to new technology.

Clearly, the regulation of bitcoin is in its infancy – but it is recognised as a legitimate means of payment (although not legal tender) in a number of jurisdictions. Most EU central banks have issued warnings to consumers about using digital currencies. However, governments are also keen to explore the potential of blockchain technology and digital currencies. In August 2014, the UK government announced a major programme of work looking into the benefits and risks associated with digital currencies and underlying technology, with a particular focus on the question of regulation. The UK Government's early strategy is to create a supportive environment for the development of businesses in the digital currency sector while also creating barriers against illegal activity – including the application of anti-money laundering regulation to digital currency exchanges.

Referring to this programme generally and alternative payment systems specifically, UK Chancellor of the Exchequer George Osborne said *"…I want to see whether we can make more use of them for the benefit of the UK economy and British consumers....We stand at the dawn of a new era in banking. Mobile banking apps, peer to peer lending, digital currencies -- technologies such as these are going to transform our lives, and create huge economic opportunities."*

# Uses for blockchain technology

## Potential (outside of bitcoin)

Blockchain technology solved the problem of how two people can exchange a piece of digital property, without any prior relationship, and in a secure way, over the Internet. The first application is bitcoin. However, it has potentially many uses:

- Monitoring supply chains, storing land and property title records, maintaining secure identity information, keeping records of contracts, royalty payments, certificates for authenticating art and recording local or national government budgets and spending.
- In financial services, the creation of one repository of transactions or other successive events over a shared network without maintenance or administration by a central authority – for instance, share registers or stock exchange trades.
- Asset-centric technology and its application to the transaction banking and payments domain as the current focus.
- Secure voting systems for elections

## The Internet of Things (IoT)

The Internet of Things refers to a wide variety of devices such as biochip transponders, sensors or anything which monitors or collects data with the help of existing technologies. Each ‘thing’ is uniquely identifiable and can interact with other ‘things’ through the existing Internet infrastructure. So there is an opportunity to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.

Blockchain technology could provide a way to track the unique history of such individual devices through the recording the data exchanges. Blockchains could also enable smart devices to conduct associated transactions on their own. Uses could include “smart” contracts which would complete when specified data sets are monitored and defined criteria fulfilled.

## Investment in blockchain / bitcoin

The development of this technology is in its early stages and it has been likened to the development of the internet. It is the very existence of the internet that increases the likelihood that the development of blockchain technology will occur at a fast pace.

There are already a number of significant investments which have been made in either exploring the technology or using it. For instance, the British Business Bank has committed over £200 million of new funding to Fin Tech companies and to the development of new and innovative forms of finance. According to Coindesk, the first quarter of 2015 saw US$229m of venture capital investment in bitcoin startups taking the total to US$676m.

Bitcoin has its detractors, but it has also spawned much interest and comment from governmental bodies and commercial enterprises. Blockchain technology is undeniably a valuable and powerful system, allowing storage and upkeep of agreed and validated sets of data.  Large numbers of material entities are now involved in both bitcoin and blockchain. We note the UK Government’s interest as described earlier in this document, and the table below gives a snapshot of the diverse nature of those getting involved:

### Involvement and investment in blockchain technology

| Entity | Date | Technology | Use |
|---|---|---|---|
| Nasdaq | May 2015 | Blockchain-enabled digital ledger technology that will be used to expand and enhance the equity management capabilities offered by the Nasdaq Private Market platform | Fully-electronic services that facilitate the issuance, transfer, and management of private company securities |
| IBM | Jan 2015 | ADEPT concept - Autonomous Decentralized Peer-to-Peer Telemetry | Decentralised  Internet of Things , using blockchains and utilising a mix of proof-of-work and proof-of-stake to secure transactions |
| Overstock.com | June 2015 | Bitcoin blockchain | Launch of U$25m digital bonds to trade on a cryptographically-protected distributed ledger |
| Honduras Government | May 2015 | Bitcoin blockchain via Factom | Development of a secure land title record system |
| UBS | April 2015 | Blockchain technology | Launched ‘Innovation Lab’ to explore how blockchain technology could improve the banking sector |

***Source: Relevant company data, Progressive Equity Research***

## Glossary

**Blockchain:** The ledger (book of records) of all transactions, grouped in blocks.

**Fiat currency:** Currency established by governments to centre an economy onto one kind of transaction medium (e.g. euro, US dollar and yen).

**Fiduciary currency:** A currency without intrinsic value; it derives its worth from the trust users have in the issuer of the currency.

**Hash:** A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes.

**Merkle:** Every transaction has a hash associated with it. In a block, all of the transaction hashes in the block are themselves hashed and the result is the Merkle root - the hash of all the hashes of all the transactions in the block. The Merkle root is included in the block header. By downloading just the tiny block headers and Merkle tree, it is possible to securely verify that a transaction has been accepted by the network so downloading the entire blockchain is unnecessary.

**Mining:** The validation of a set of transactions (a block) made with a decentralised digital currency and adding this block to the ledger of all transactions (the blockchain).

**Digital currency:** A digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.

### Disclaimers and Disclosures

Copyright 2015 Progressive Equity Research Limited (“PERL”). All rights reserved. PERL provides professional equity research services, and the companies researched pay a fee in order for this research to be made available. This report has been commissioned by the subject company and prepared and issued by PERL for publication in the United Kingdom only. All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable; however, PERL does not guarantee the accuracy or completeness of this report. Opinions contained in this report represent those of the research department of PERL at the time of publication, and any estimates are those of PERL and not of the companies concerned unless specifically sourced otherwise. PERL is not regulated by the Financial Conduct Authority (FCA).

This document is provided for information purposes only, and is not a solicitation or inducement to buy, sell, subscribe, or underwrite securities or units. Investors should seek advice from an Independent Financial Adviser or regulated stockbroker before making any investment decisions. PERL does not make investment recommendations. Any valuation given in a research note is the theoretical result of a study of a range of possible outcomes, and not a forecast of a likely share price. PERL does not undertake to provide updates to any opinions or views expressed in this document.

This document has not been approved for the purposes of Section 21(2) of the Financial Services & Markets Act 2000 of the United Kingdom. This document is a marketing communication under FCA Rules. It has not been prepared in accordance with the legal requirements designed to promote the independence of investment research. It is not subject to any prohibition on dealing ahead of the dissemination of investment research.

PERL does not hold any positions in the securities mentioned in this report. However, PERL’s directors, officers, employees and contractors may have a position in any or related securities mentioned in this report. PERL or its affiliates may perform services or solicit business from any of the companies mentioned in this report.

The value of securities mentioned in this report can fall as well as rise and may be subject to large and sudden swings. In addition, the level of marketability of the shares mentioned in this report may result in significant trading spreads and sometimes may lead to difficulties in opening and/or closing positions. It may be difficult to obtain accurate information about the value of securities mentioned in this report. Past performance is not necessarily a guide to future performance.