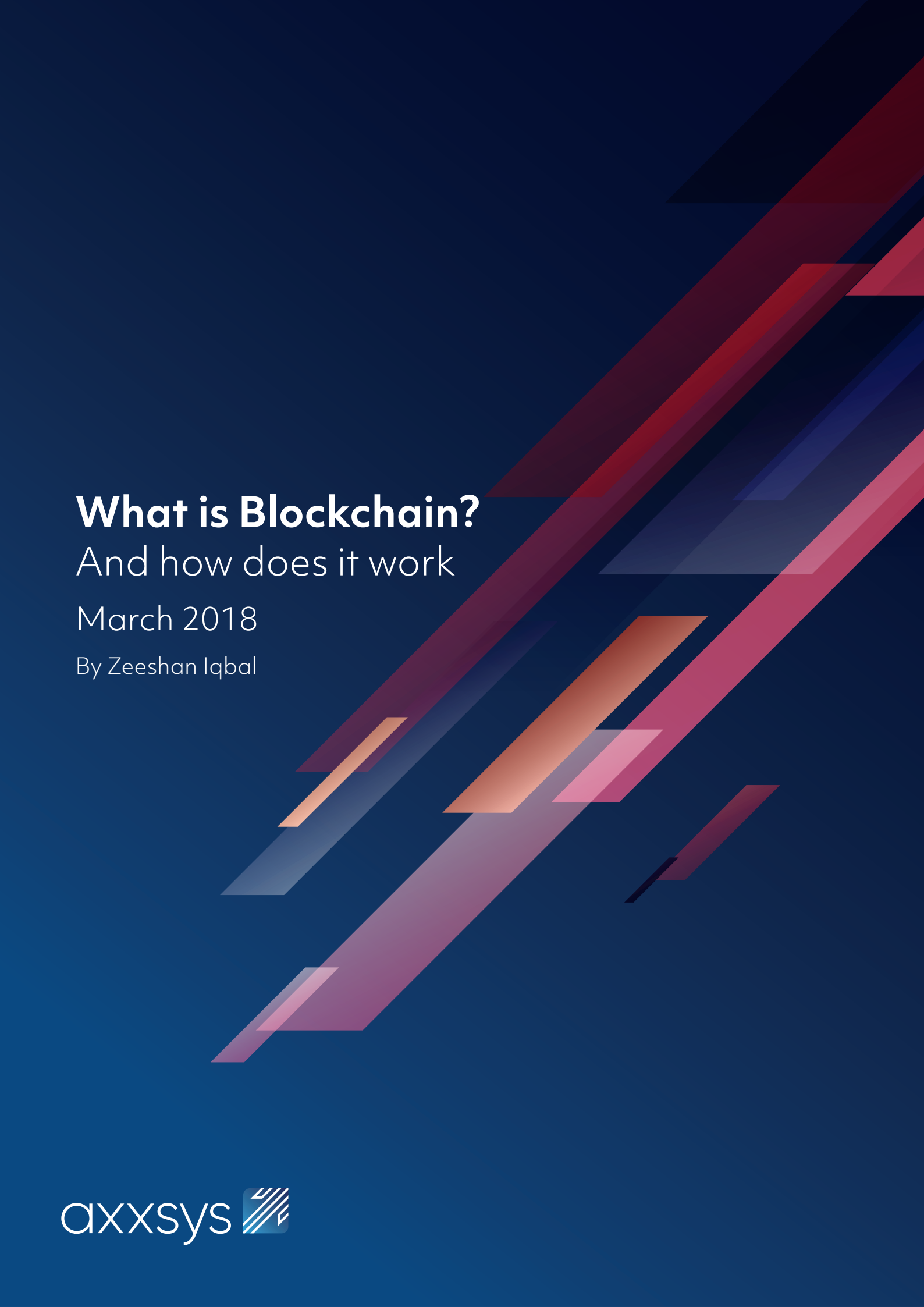
What is Blockchain?

And how does it work

March 2018

By Zeeshan Iqbal



axxsys

Introduction

The topic of blockchain is comprehensive enough that many books have been written about it. This is the first in a series of papers that explore blockchain.

In this document we will explain how blockchain works with the aim of giving the reader enough detail to understand its principles without getting engrossed in excessive detail. In further papers, we will examine how the Asset Management industry is familiarising itself with blockchain and how this could change the industry. We will conclude by seeking to address some of the challenges with blockchain technology, how these can be overcome and what the new alternatives are that seek to out-do blockchain.

In 2017, the price of the crypto-currency Bitcoin skyrocketed, with wild up and down swings, creating news headlines and spreading awareness of this previously obscure topic.

It all started in 2008, when an unknown individual or group called Satoshi Nakamoto published the paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System". The next year, the Bitcoin software was released and the first bitcoin came into existence.

There are no physical coins, notes or any other tokens issued. Bitcoins only exist as an entry in an openly shared electronic ledger – the bitcoin Blockchain.

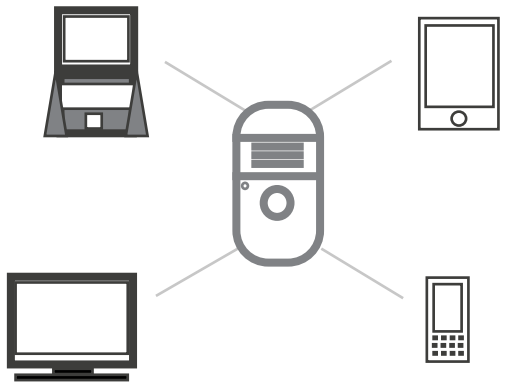
Bitcoin is a crypto-currency that is created and transacted directly between users without the need for a bank or any intermediary payment processing organisation. All you need is the freely available bitcoin software. There are no physical coins, notes or any other tokens issued. Bitcoins only exist as an entry in an openly shared electronic ledger – the bitcoin Blockchain.

Bitcoin is the original and best known implementation of blockchain, hence its mention is almost unavoidable when attempting to understand the workings of blockchain.

From a technical point of view - Bitcoin has survived and thrived in the years since it was created – and this has given enormous credibility to blockchain's resilience. The banking and asset management industry are increasingly interested in adapting blockchain to new uses as they recognise its potential to be a disruptor in the industry, much in the same way that the internet and smart phones have changed the business landscape and interactions. This makes it an essential area of knowledge to invest in, for the future potential it offers to the changing Fintech landscape.

A blockchain is an electronic file, just like any other computer file. It contains ledger entries such as "John pays David 0.05 Bitcoins".

Client Server Architecture



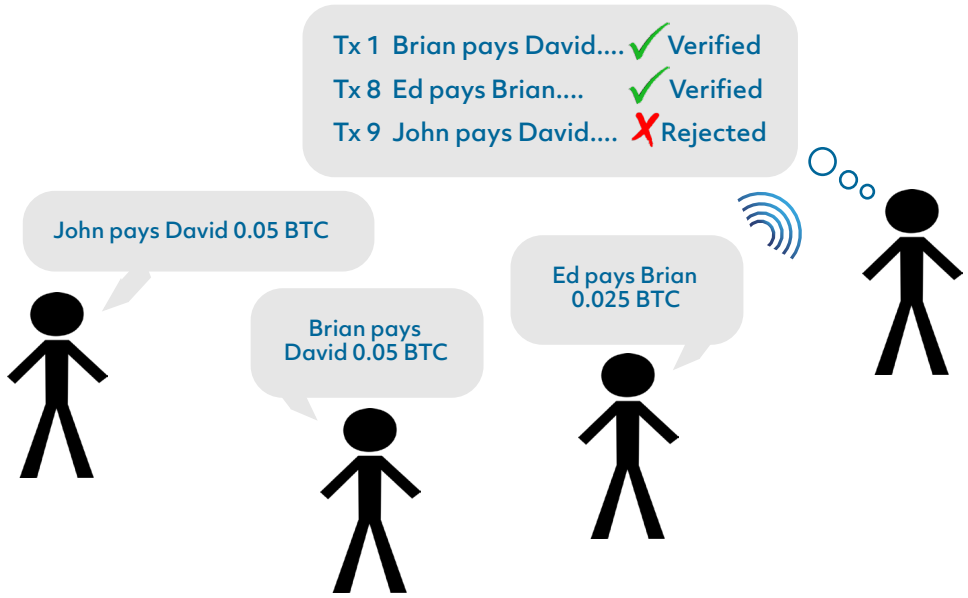
Peer to Peer

From a functionality point of view – blockchain performs the role of a public ledger or database. Anybody can read this database (You can query the bitcoin blockchain online at https://blockchain.info/), and anybody has the ability to make entries into this database subject to its rules.

A copy of the blockchain is held by all its users, instead of it sitting on a central server

So what is the difference between blockchain and a traditional database? The main difference is that blockchain is distributed – a copy of it is held by all its users, instead of it sitting on a central server somewhere. This has some important implications – It is not owned and controlled by any one user. "The blockchain" generally refers to the bitcoin blockchain, but any technology that satisfies the requirement of a multi-user peer-to-peer database can be referred to as a "Distributed Ledger Technology" or DLT. With a traditional "Client-Server" based system – a user logs in and communicates directly to one database through an application. All functionality – from access privileges, validation of business rules, and timestamping of events are centrally controlled by the owner of that central database.

In a blockchain application - since it is distributed, there is no such central server to log into, to perform these functions. This creates some technical challenges - like how do you make an entry to a public database that you can't locate? How can you be sure that all users on the network have seen your entry and have updated their copies of the blockchain?



When a user submits a transaction – it is "broadcast" to other users on the network, who will be actively listening for new transactions. On receiving a notification of a new transaction, they validate it by checking that it conforms to all the business logic (e.g. account balance must not be negative) and then further relay this as a "confirmed" transaction to other users.

A transaction gets more confirmations as it propagates through the blockchain network. At any point in time, a number of users will be aware of new transactions. These new transactions are not yet recorded in the blockchain. First – there has to be "consensus" amongst all users on a way to permanently order and record these new transactions into a "block".

The action of collecting transactions together into a block and linking it to the previous block, and therefore making it permanent is called mining and is carried out by users that act as miners. Any of the users on the network can choose to become a "miner" and attempt to create or "mine" a new block, since a reward of bitcoins is offered for this activity.

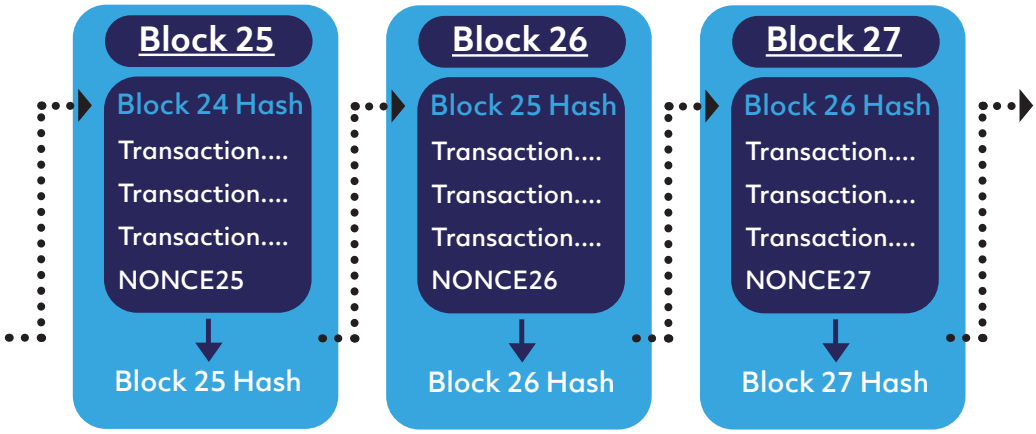
Mining involves gathering new confirmed transactions, the hash value of the previous block, and a random number called a "nonce", and then calculating the hash of these inputs. A hash value is a small piece of data with a fixed size that can be thought of as a fingerprint of a much larger piece of data. It is generated by applying a mathematical function on the larger piece of data. It is important to note that the smallest change in the input to a hash function will result in a completely different hash value. The probability of two different inputs generating the same hash is extremely low. The hash value cannot be

The action of collecting transactions together into a block and linking it to a previous block is called mining and is carried out by users that act as miners

reverse engineered to discover its inputs. This is makes it invaluable in ensuring the integrity of data. The resulting hash of the newly formed block must meet blockchain's "difficulty" criteria: i.e. it must start with a certain number of zeroes. If the result doesn't meet the difficulty criteria, then it is rejected.

Finding a nonce that generates a qualifying hash is computationally very resource intensive. The miner must repeatedly try different nonce numbers until it finds a correct one. Once a qualifying nonce is found, the miner broadcasts this solution to other users on the network as a "proof of work". They can easily verify the broadcast solution – and this new block is added to the blockchain. At this point – the block takes its final shape. In the case of Bitcoin, the size of a block is limited to 1 megabyte, which typically holds somewhere between 2,000 to 3,000 transactions.

A look inside a Blockchain Block



This process then continues with the next set of confirmed transactions. Since every block's hash includes the previous block's hash in its input, this means that all blocks are linked to their previous block. Any change in a block (e.g. somebody attempting to hack a transaction) would change its hash value and invalidate all subsequent blocks which would have a domino-effect.

Such a change would require an attacker to mine all subsequent blocks again, whilst the blockchain is still growing. This would require the attacker to employ greater computing power than the rest of the mining network which is implausible.

This is what makes the blockchain immutable.

Conclusion

Blockchain is a technology that has its origins in Bitcoin. It has features that allow individual entities to work on a shared ledger that has self-managing methods of creating consensus without appointing any individual as a guardian of the ledger. This is a paradigm shift in the way management and business processes have interacted with each other. It opens up possibilities on reshaping the way business is conducted and how complex processes are managed in the industry. New applications of blockchain are still in the experimental processes and the race is on amongst innovators to develop the next generation of applications leveraging the strengths of blockchain technology. It remains to be seen if the future is blockchain, or perhaps blockchain will serve as an inspiration for even newer mechanisms of achieving decentralised consensus at a fraction of the cost and complexity of blockchain.

The next paper will explore how the Asset Management industry is responding to the potential offered by blockchain by experimenting with new applications within their niche areas. We will also investigate some of the challenges that need to be overcome for decentralised ledger technologies to become mainstream.

From Theory to Application – Axxsys Consulting

Innovation requires time, resources and expertise. Not all investments will pay off, and there is a long way from concept to its effective application.

How can asset managers – whose core business is not innovation but managing money – navigate the ever-changing and increasingly complex technology and vendor landscape, and effectively exploit innovation?

At Axxsys Consulting, we are in a unique position to help effectively navigate these challenges.

We make it our business to keep up-to-date with relevant developments, developments that will enable our clients to save money, resource and reduce risk.

We make it our business to identify opportunities for innovation, opportunities that will impact our clients in terms of revenue and scale.

We make it our business to understand which aspects of new technology are relevant for our clients, and how they can be applied successfully.

With our extensive knowledge of the buy-side, our experience in delivering projects from inception to completion, our network of technology vendor and market participants, and our implementation and advisory work, we offer a unique proposition to our clients.

About Axxsys Consulting

Axxsys Consulting is an international consulting firm with a proven track record in the Financial Services industry in EMEA and North America with offices in London, New York, Toronto and Copenhagen.

We provide specialised Management and Technology consultancy to today's forward-thinking Investment firms, covering everything from Advisory Services and Strategic Planning right through to Major Change Programmes.

Our trusted, highly skilled and knowledgeable industry practitioners can help you achieve outstanding outcomes from your chosen business or technology integration project.

We are a delivery-orientated team, with senior leadership expertise in Management Consultancy, Portfolio Management, Performance & Risk, Sales & Distribution, and the strategic implementation of data and technology systems.

Core to our service offering is the Axxsys Axxelerator™ Platform. Years of accumulated knowledge have allowed us to create a unique and complementary range of Axxelerators™, tools and templates specially designed to help organisations achieve their business goals faster and more efficiently.

This makes us pioneers in the consultancy field, leading the way with innovative new disciplines that effectively integrate technology within the Investment Management community.

Contact Information

Zeeshan Iqbal, Consultant
+44 (0) 7789 711 028
+44 (0)20 7526 4900
info@axxsysconsulting.com
www.axxsysconsulting.com

GLOBAL OFFICE NETWORK

LONDON	COPENHAGEN	LUXEMBOURG	PARIS	AMSTERDAM	EDINBURGH
TORONTO	GENEVA	ZÜRICH	NEW YORK	BOSTON	SINGAPORE

axxsys

www.axxsysconsulting.com

info@axxsysconsulting.com