Bitcoin and blockchain
What you didn't know but always want to ask

Johann Palychata
Research Analyst at BNP Paribas Securities Services

The wave of interest or Cryptomania – is still growing. The word blockchain that is a part of the bitcoin jargon is now often used to describe the technology of distributed ledgers. Some think it can reshape many industries, others think it has still everything to prove. We would like to spend more time to explain the paradigm shift introduced by this new technology. Johann Palychata discusses why Bitcoin creates hopes and passions around the world.

A short history of money

Could you imagine the surprise of a farmer, living in the 7th century before Christ being told that he would be paid using coins? He probably did not understand how a piece of metal could be worth as much as his entire annual production. Grasping the Bitcoin concepts for modern society implies understanding the new codes introduced by crypto-currencies. How can a digital currency invented 7 years ago now have a market cap of over 3.8 billion USD with significant volumes exchanged every day? What is its purpose? Is it useful or simply a speculative instrument? Why do many think the new underlying technology is more important than the currency hosted on it? This is the subject of this introduction, which starts by a short – and therefore selective – history of money.

For centuries we have used commodities as money. Gold had a major impact on trade, blocks of salt were used in Ethiopia until the 19th century and "salary" comes from "salarium" in Latin. Fiat currencies, "monnaie fiduciaire" for French readers, emerged later in history. They have no intrinsic value but they are backed by a state or an economy. Coins or bank notes are the best example. Money moves from one hand to the other easily: there is a physical delivery occurring and it is irrevocable. Then people kept their fortune in their pockets or under their mattress.

Banking emerged when money was not only represented by physical objects but by entries in an accounting book. Deriving from this we have many modern representations: a check book, a bank account, a credit card or even on-line payment systems like PayPal. The benefits it brought our economy are numerous: transfer of money without physical delivery and the concept of commercial bank money that is the fuel of the economy. In this form money was already digital and created more than 300 years ago. It was no longer a material reality but a sum of discrete entries in accounting books. This digital revolution, as well as many others, implied tragedies and great losses. The system of John Law, the Scottish economist who introduced paper money in the 18th century and the Assignats during the French revolution ended by the default of the issuer.

In fact all these new representations of money require an honest intermediary to keep the book records. Otherwise the issuer can issue as much

cash as desired. There was no way to eliminate this central authority or third party. Between me and you there is a bank that we both trust and that keeps the book records. Otherwise I could print my own money or spend my money twice. There was even a time when banks could not be trusted. During the free banking period in the US, banks were able to issue their own bank notes. The value of these notes could decrease with the declining creditworthiness of an issuer who did not behave. To ensure the safety of the paper money system, public authorities gradually entrusted one single bank with the task of issuing bank notes and central banks were created[1]. Their mighty power is the ability to print new money to their convenience. These examples show that getting rid of the central authority is impossible – or more accurately – it was impossible, because in 2008, the bitcoin was invented.

Bitcoin finds its roots in computer science and cryptography. In 1982, a group of researchers in this field published a paper where they describe a problem that they call the "the Byzantine General Problem" [2]. It refers to the Byzantine army camps around the enemy city. The generals must agree on a common battle plan otherwise they will lose. They cannot sit around a table and can only communicate using messengers. As some generals are traitors and messengers could be intercepted and then corrupted by the enemy, the voice of those must be ignored. Otherwise confusion will spread. How can they succeed? You can see that it has an application in the subject that interests us here: how a number of people who do not trust each other can agree on accounting entries in a distributed manner and eliminate those who might want to cheat by minting their own money, falsifying their accounts or spending their money twice. This is this challenge that bitcoin solves.

A new technology for the banking world: "The internet of money"

In 2008, an individual or group writing under the name of Satoshi Nakamoto published a paper that described a peer-to-peer version of electronic cash that "would allow online payments to be sent directly from one party to another without going through a financial institution". The first implementation of this concept is known as Bitcoin. Today, 'crypto-currencies' is the label used to describe all networks and mediums of exchange that use cryptography to secure transactions – as opposed to systems in which transactions are secured through a third party, such as a bank.

The author of the first paper wanted to remain anonymous or so we think since no one knows Satashi Nakamoto to this day. A few months after the first paper, he released an open source program implementing the new protocol. Anyone could install it on their computer and become part of the bitcoin network. Its popularity has never ceased to increase ever since. Today the word Bitcoin designates the currency used as a unit of account on this network. It has the interest of economists due to its unique monetary policy. Bitcoin can also designate the technology and the protocol Satoshi invented. It allows a removal of the central third party in financial transactions and offers a new range of possibilities well beyond finance.

So how does it work?

At this point, convincing you that it is really an innovation will require a dive into some technical details. Bitcoin (the technology) is relatively simple to use, like cash. Users send and receive Bitcoins using a wallet software on a personal computer, mobile device or a web application.

On the network there is a public database and sequential record of all transactions, known as the blockchain. It records current bitcoin ownership as well as the ownership in the past. In a traditional world, the register is centralised. Here it is on internet, everyone has a copy of the register, every can see the balance of all accounts however no one can counterfeit it. This consensus for a unique valid register is obtained by a methodology which represents the real innovation of Bitcoin. In addition to this unique feature, the network is designed as a decentralized peer to peer network to ensure its resilience against any shut down attempt, very much like the internet.

Let's now see how people can exchange their coins on the network. It is based on asymmetric cryptography to secure the wallets of people and widely used in the internet today. Cryptography is sometimes a means of sending an encrypted message securely. It is also a means to create a digital signature. The purpose of cryptography here is to ensure that the message comes from a trusted source. To sign a message (that anyone can read) one has to use a private key. Anyone with the public key can check that the writer of the message is the owner of the private key. Having a Bitcoin address (a public key) is the prerequisite to receive a bitcoin. Unlike opening a bank account, which requires the acceptance of the bank, you can create a bitcoin address without any help and without any authorisation. In summary with bitcoin you are holding your digital cash yourself, without using a bank and the network is also a messaging system where you can send orders.

[1] The payment system – payments, securities and derivatives, and the role of the Eurosystem in this field, ECB, 2010
[2] The Byzantine Generals Problem, LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE

Bitcoin is also a settlement system. A new block is added approximately every 10 minutes to the blockchain, containing the transactions of the last 10 minutes. The explanation can get very technical on these details, but you can take for granted that a transaction is irreversible when a couple of blocks had time to follow the one where your transaction is included.

While many describe the bitcoin as a currency, it is in fact primarily a disruptive open source technology for the financial world. Bitcoin is therefore sometimes called the "internet of money". Its core is the first successful attempt for a secure and decentralized register. It should be considered as an invention like the steam or combustion engine.

A new currency hosted on a blockchain

On 22 May 2015, groups gathered around the world. They celebrated the fifth anniversary of the first recorded purchase made using Bitcoin. A pizza was bought for 10,000 Bitcoins in 2010. Before, Bitcoin had no recognised value. A couple of months later an online exchange opened and people started trading dollars for bitcoins. The value of a Bitcoin has since peaked just above 1200 USD in December 2013 and is currently around 240 USD. Why do some people have faith in this currency?

The main reason is probably that the monetary mass is circulation is known in advance. It is written in the protocol. In 2009 the first coin was minted and at the time 50 coins were created approximately every 10 minutes. The number of bitcoins created every 10 minutes, however decrease by half every 4 years so that the amount of bitcoins in circulation will ultimately reach the limit of 21 million. Bitcoin is a scarce resource and what makes it valuable. People see it as a reserve currency with a deflationary behaviour. Who are the prime owners of the newly minted coins? People who provide processing power (by making available computing power to solve the huge mathematical calculations required to maintain the register) are rewarded through the creation of new money and by transaction fees. This is called "mining" and it is the incentive that makes the network grow.

Two scenarios for the integration of the technology in the post trade infrastructure

What would happen if the ownership of securities were recorded in a blockchain? We envisage two scenarios for the integration of this technology in the post trade world.

The first scenario creates a total disruption. In its purest form, a distributed blockchain system allows all market participants direct access to the DSD (Decentralised Securities Depositary), to the exchange and to the post trade infrastructure (clearing & settlement). If this setup develops then existing industry players might be redundant. However, given the challenge of keeping the private key of the account safe, it is possible that investors will entrust an authority to safe keep the private keys. It is also possible that custodians will be responsible for the application layer over the blockchain or that they will launch their own network.

The second scenario is an integration within the post trade ecosystem. The distributed ledger might only be the next generation of IT infrastructure. In this scenario custodians or settlement infrastructures might use the blockchain to record the ownership and trades between themselves; however end investors will still need to use a custodian to have access to the market. The ledger will only be accessible to authorised market participants. Existing actors will remain in charge in this scenario however their level of service could change and they may deploy new services that they could not in the past because the investments required were a huge barrier to entry.

The virtue of decentralisation and the promises of blockchain

Bitcoin has solved a technical challenge and the currency it hosts has been successful so far. Today, anyone can create their own blockchain based network. Dozens of them now exist, some have value, others are completely worthless – many have unique features. Some raised millions to deliver the promises of their business plan or white paper. They usually have their own unit of account, but their purpose sometimes goes beyond. The most ambitious think that tomorrow; storing files, executing code or even running businesses will use this infrastructure. It is however wise to consider most of the initiatives as research and development projects. It remains to be proven if scale can be obtained and costs managed to allow for a true revolution.

securities.bnpparibas.com

@BNPP2S

BNP Paribas Securities Services

youtube.com/BNPParibasSecurities

Printed on recycled paper with vegetable inks – Designed by the graphics department, corporate communications, BNP Paribas Securities Services.

BNP PARIBAS SECURITIES SERVICES | The bank for a changing world