FROM JULIUS CAESAR TO THE BLOCKCHAIN: A BRIEF HISTORY OF CRYPTOGRAPHY

By **Côme JEAN JARRY** & **Romain ROUPHAEL**, cofounders of BELEM

The world's most important asset is information. Now more than ever. With computer theft and hacking becoming a common threat, protecting information is crucial to ensure a trusted global economy. E-commerce, online banking, social networking or emailing, online medical results checking, all our transactions made across digital networks and insecure channels of communication, such as the Internet, mobile phones or ATMs, are subjected to vulnerabilities. Our best answer is cryptography. And it has always been. As a science and as an art, it is an essential way to protect communication. Cryptography goes back to older times, as far back as the Ancient World.

Early cryptography was solely concerned with concealing and protecting messages. In modern times, cryptography has grown from basic message confidentiality to include message integrity checking, digital signatures, sender and receiver identity authentication. Today's cryptography safeguards the general public from being compromised by those who monitor private communications. Hackers constantly challenge it and cypherpunks[1] privacy activists keep watching. So let us look back in time to understand how cryptography has evolved from simple methods of dissimulation to ultra-sophisticated mathematical algorithms.

From the Greek scytale and the Caesar cipher to the mechanization of coding.

THE ART OF TRANSPOSITION

The earliest known use of cryptography dates back to Ancient Greece. During the Peloponnesian War, the Spartans used a wooden stick, called scytale, with a strip of parchment wound around it on which the message was inscribed lengthwise. Once the parchment was unrolled, the letters of the message were mixed up and the message meaningless. The receiver would need an identical stick to decipher the text. The scytale transposition cipher relied on changing the order of the letters, rather than the letters themselves. This cryptographic technique still prevails today.

THE ART OF SUBSTITUTION

Julius Caesar was also known to use encryption to convey messages to his army generals posted in the war front. The Caesar cipher is a simple substitution cipher in which each letter of the plaintext is rotated left or right by some number of positions down the alphabet. The receiver of the message would then shift the letters back by the same number of positions to obtain the original message. It is the very first system to use a coding parameter called the encryption key. The encryption key, secretly shared by the sender and the receiver, becomes an essential feature of cryptography. Without it, the only option to decipher the scrambled text would be to do a brute-force check and try all the possible keys. A very tedious work.

Modern cryptology owes a lot to the Arabs, their study of the Coran, its phonetics and syntax. Around AD 800, Al Kindi is the first to document cryptanalytic methods, developing a frequency-analysis technique able to break monoalphabetical substitution ciphers by using the occurrence of letters in language.

Despite this discovery, cryptography remains very basic, until the 16th Century when Frenchman Blaise de Vigenère created a polyalphabetic cipher known as the Vigenère Cipher. It works like the Caesar Cipher but changes the key throughout the scrambling process, using a grid made of 26 alphabets offset from each other by one letter called the Vigenère Square. The Vigenère Cipher is said unbreakable as it resists frequency-analysis. In 1854, Charles Babbage, an eccentric Englishman, solves the Vigenère Cipher by discovering that enciphering the plaintext with a keyword renders the ciphertext subject to modular arithmetic.

1 A cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Source: wikipedia.

ENIGMA AND THE BIRTH OF THE COMPUTER

In 1918, the German Arthur Scherbius patented the Enigma, an electromechanical machine used for encryption and decryption made of several shiftable rotors and electronic gears that converted every letter typed on the keyboard. The different scrambling configurations and initial settings of the machine allowed a nearly endless number of encryption keys. It wasn't until World War II that Enigma gained its fame. Nazi Germany, overconfident about its security, used it to encode most secret messages. It drove Enigma, and to some extends Hitler, to their end. Poland, and later the Allied, exploited the built in weaknesses of the machine and the German operators errors to decrypt many coded messages. During the 1930's, Poland's Marian Rejewski built the first "bomb", an electromechanical machine that mimicked Enigma's process to brute-force test potential encryption keys in order to find the correct one. This "bomb" was later improved by British Alan Turing who eventually cracked Enigma.

The Britih cryptanalysts also broke the Lorentz cipher used by Hitler to communicate with his generals. The German dictator made use of an electromechanical machine that exploited the binary code to convert the letters of his messages into a sequence of 0 and 1 called "bits". In order to mechanize the codebreakers' breakthrough, Max Newman designed the very first programmable electronic computer, Colossus, built by Tommy Flowers in 1943. Cryptology was at a new turning point. It could now count on the computer's efficiency and velocity, paving the way to new means of coding.

ON THE TRAIL OF ASYMMETRIC CRYPTOGRAPHY

By the end of World War II, both cryptography and cryptanalysis had become very mathematical. With businesses using more and more computers, it had become necessary to standardize cryptography to enable firms to safeguard their transactions and secure their data from competitors. In 1976 the Data Encryption Standard answered just this requirement. Cryptography was no longer a government and army prerogative. Ciphers were getting harder and

Source: GNU free documentation license

harder to crack, mostly because computing power was not yet strong enough to brute-force attack every possible encryption key. The longer the key the safer it would be. Yet, an old issue remained, making it the Achilles heel of cryptography: the key distribution. Encryption keys were often locked inside briefcases carried around by secret agents, just like in Hollywood movies. The digital era of the 1970's caused a need for a more secured system.

In 1976, Martin Hellman, a Stanford professor, along with Whitfield Diffie and Ralph Merkle, introduced a revolutionary method of distributing cryptographic keys, known as the Diffie-Hellman key exchange. The answer came from non-reversible mathematical functions and modulo arithmetics. Sender and receiver could now agree on a key without meeting in person, and despite being spied on. Each one would choose a secret number that he would keep to himself, sending to the other the result of a modulo arithmetic computation. But sender and receiver were still dependent on each other. This solution had room for improvement.

It triggered the discovery of a new coding method, the asymmetric key algorithm, also known as public-key cryptography. Up to this point, every method of encryption required a special secret key previously and securely established, shared both by the sender and the receiver, distributed through a confidential channel. Using the same key for encryption and decryption is the principle of symmetric key encryption.

The asymmetric key algorithm requires two different keys, one is made public and shared with all, whereas the other one is kept secret. The sender uses the receiver's public key to encrypt his message and the receiver uses his own private key to decrypt it. The challenge was to find a mathematical function that could generate two keys independent from one another. In August 1977, Ronald Rivest, Adi Shamir and Leonard Adleman, researchers at MIT, solved the problem by accident. They were trying to prove that Diffie's idea was going nowhere. The RSA (Rivest, Shamir, Adleman) Cipher was born and soon became a universal protocol for businesses. It is still believed to be unbreakable, all hacking attempts having failed. But time is pressing, its security only relying on today's computers' low computing power.

PRIVACY: FROM PRETTY GOOD PRIVACY TO CRYPTOCURRENCIES

The Age of Information that followed the democratization of private computers and the development of the Internet in the 1990's presented a new challenge: securing private data. The RSA was not scaled for personal computers. In 1991, the American Phil Zimmerman was adamant about finding a cipher freely accessible to all and easy to use. He combined the simplicity of a symmetrical algorithm (to encrypt the message) with the technicality of an asymmetrical algorithm (to encrypt the key), naming his cipher PGP (Pretty Good Privacy).

Private communications through digital channels were now safe but governments had other tricks up their sleeves to monitor their citizens such as tracking financial transactions, enraging cypherpunk privacy activists. This is when cryptocurrencies emerge.

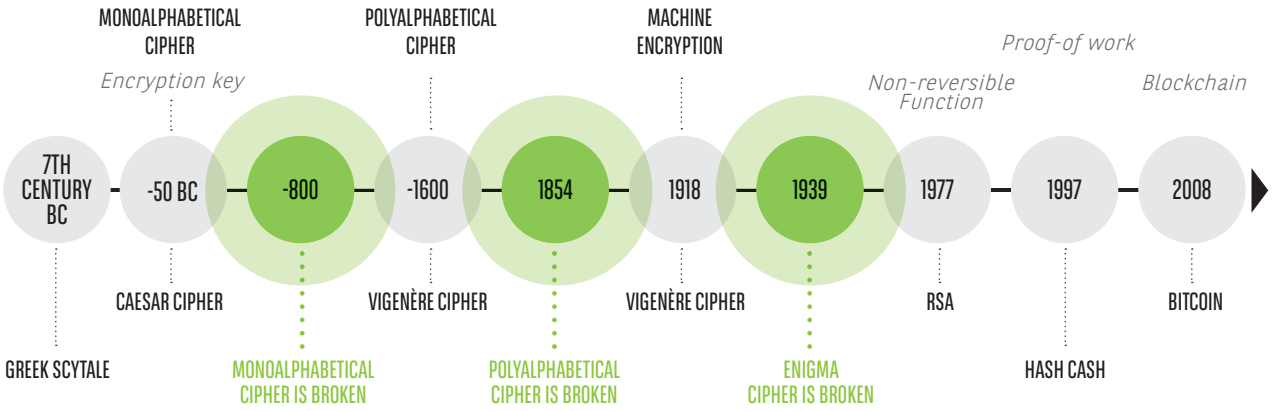
In the early 1990's, David Chaum creates DigiCash, the first digital currency of many, designed to allow secured and anonymous financial transactions. Unfortunately the cryptocurrency fails at preserving the money's independence as Chaum introduces a central authority to validate the digital signatures behind every transaction.

In 1997, Adam Back introduces the Hash Cash, a cryptocurrency relying on a revolutionary protocol called "proof-of-work": the participating members to the network are challenged to recover a specific hash print using their computer's calculating power. The first one to find the answer receives a specific amount of money. This is how the currency is issued. Adam Back creates an independent currency but he is unable to find a way to exchange each unit of money more than once.

Other cryptocurrencies are conceived - Nick Szabo's Bit Gold, Wei Dai's B-Money, Hal Finney's Reusable Proof of Work - but a major weak point remains: a contributor to the network with a disproportionate computing power can win more easily the competition, producing more and more currency units, thus mechanically reducing its value.

Satoshi Nakamoto finds a way to solve this deficiency and the double spending problem in October 2008 with his Bitcoin thanks to a new coding protocol called the "Blockchain". It is a distributed database that validates transactions inside records called "blocks", every block including a hash of the previous one, linking them one another as in a chain. It combines asymmetric ciphering, digital signature, hash functions and the proof-of-work protocol. The system uses a unified and public ledger, approved by all members of the network, to track the Bitcoins and make sure they are not copied or spent more than once at a time. It uses a peer-to-peer network to manage autonomously the database. To solve the Hash Cash's weakness, the system sets the time necessary to validate a block of transactions to 10 minutes, hence regulating the currency production. The units are now gradually introduced. For the first time in History, a currency is created and transferred without a centralized trusted third-party. The Blockchain is a revolution. As a disruptive innovation it promises to bring significant changes to many business structures. •

TRANSPOSITION ENCRYPTION → SUBSTITUTION ENCRYPTION → PUBLIC-KEY CRYPTOGRAPHY → CRYPTOCURRENCY



BELEM

Founded by Côme JEAN JARRY & Romain ROUPHAEL, **BELEM** (**www.belem.io**), is a start-up that relies on cryptography to deliver the next wave in data sharing. BELEM enables independent parties to organize decentralized calculation on private data without revealing their inputs.

"Any organization can easily set up a community of players, customize all calculation rules, and may decide to share the result directly with an external party, like a client or a regulator. Transparency and data privacy are no longer antithetical."