2 Blockchain in a nutshell

1. A brief history

Blockchain is a technology that first appeared in 2008 within the cryptography* expert community.[1] It was conceptualized by an as-of-yet unidentified individual or group of individuals under the alias Satoshi Nakamoto and first implemented in 2009 as a core component of the cryptocurrency Bitcoin.[2] While Blockchain and Bitcoin are historically linked, they are two different things. Blockchain is the technology underpinning Bitcoin; it is the virtual infrastructure that Bitcoin uses. Bitcoin is a cryptocurrency, but the term is often used to refer to both the cryptocurrency and the protocol underlying it – i.e. Blockchain. This confusion may be one of the reasons why it took so long for people to realize that Blockchain can be used in areas other than for cryptocurrencies.

The launch of Bitcoin in the wake of the 2008 financial crisis has caused it to be mistakenly considered as a direct consequence of the latter. The history of cryptocurrencies, however, started before the 2008 financial crisis.

Several older cryptocurrencies had failed to take off and never made it beyond the boundaries of the cryptography community. The ancestors of Bitcoin were developed by members of the "Cypherpunks", a network of activists advocating for the widespread use of robust cryptography and privacy-enhancing technologies as a route to social and political change. The Cypherpunks used peer-to-peer systems and cryptography to process secure transactions without a "Big Brother" element, by which they meant the banking system.

The 2008 financial crisis provided a fertile ground for the operationalization, uptake and expansion of cryptocurrencies, and of Bitcoin in particular (Bustillos, 2013). In a context of loss of trust in the governance of the monetary system, and by extension in public governance in general, Bitcoin was seen by some as a desirable alternative, the achievement of all the ideals advocated by the Cypherpunks. Satoshi Nakamoto's 2008 white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008), described a new model of privacy – a model in which the trusted third party between the two parties undertaking the transaction is replaced by cryptographic