Meeting held on 17 July 2018: The BlockChain

Speaker: David Nicholls

Introduction

Blockchain is a C21 response to a basic problem: how to establish a necessary level of trust between parties to enable transactions involving exchange of value to take place. Over a long history this problem has usually been addressed by the use of trusted third parties or institutions such as notaries public, official registries and banks.

Blockchain can be described conceptually as a distributed form of registry. "Distributed" in two senses: (1) copies can be widely held among users and (2) it does not rely on a centrally controlled index or store. The means of achieving this, together with cryptography using public and private keys, are the technical pillars of blockchain.

History

Napster and DigiCash (initiated 1994!) can both be seen as precursors of blockchain. Both used public/private cryptography and peer-to-peer networks rather than a single central database; however, both relied on a central index for validation. This weakness played a crucial part in the downfall of these systems.

In 2008 Satoshi Nakamoto developed bitcoin, a form of "cryptocurrency". The breakthrough was enabling distributed validation, where there is an incentivized "race" to solve a key and thus validated the transaction, which can then be recognized by all the other members, who do not need to repeat the solution. For this to work, the use of computing power needs to be sufficient to deter unwanted attempts at solution but not so much as to require an amount of time that makes the process unusable.

In any case, this solution removed the need for a "middleman" process or registry for validation, while the existence of multiple copies and the process of encryption make it very difficult to corrupt the record by rewriting or removing any part of it after validation of the entry

Developments

Ethereum is an example of a more advanced form of crytocurrency that can also be used for a wider range of purposes.

So-called "permissioned" blockchains are a development that control the users and thus provide an aspect of security not possible in an "open" blockchain, but involve some form of central register, and therefore become a hybrid, with the issues of central control that led to the breakthrough in the first place.

It is important to understand that, though Bitcoin and Ethereum are important instances in the history of blockchain and both are forms of cryptocurrency, blockchain technology (either open or permissioned) have many other potential uses, where centralized databases of one kind or another are used currently, for example: clinical trial data, registries of assets (shares, property), identity management, elections.

Future

Commentators speak of a possible shift of power from institutions governed by law to decentralized networks operating code-based rules, and algorithms. The key difference is decentralization: not necessarily anarchy! Lex cryptographica - rule of code and algorithmic control.

On the other hand, and more probably, blockchain will follow similar pattern to internet, under which state authority is reasserted.