Blockchain technologies in construction.

DOUNAS, T. and LOMBARDI, D.

2022

Blockchain Technologies in Construction

The purpose of the book

The purpose of this volume is to inform the reader on the state of affairs of a new subset of construction informatics, Blockchain (B) and Decentralised Ledger Technologies (DLT)s. The initial motivation for writing and editing this volume was that we noticed the emergence of a range of ideas as a loose 'body of work', produced from a variety of lenses and research stances in the informatics of construction. To shape this into a volume for a book, we made an international call for chapters and established a system of peer review as the basis of the editorial work we subsequently executed with the collaboration of all authors. The book comes out at a turning point for the world, and it would have been a cliché to say this, however, it is true not just because of the efforts to recuperate from the COVID-19 global crisis. Construction, as a component of the Architecture – Engineering – Construction industry in general faces a series of challenges, which amount to a radical shift in business and operating models.

Most readers unfamiliar with Blockchain would suppose that the purpose of B/DLT in construction is tied with economics and finance. This is of course one of the strands of research and industrial application that B/DLT has an impact on, however the applications are wider and deeper, involving not only supply chains but also governance of projects, re-shaping the industry landscape and successfully enabling new modes of collaboration. On a more fundamental basis, blockchain technologies, by creating peer-to-peer economies, have the potential to reshape the manner in which we think about resources, the design and structure of our (circular) economies, debt, trust, collectives and collaboration.

This particular introductory text is placed here to deliver for the lay reader a series of definitions that will make the rest of the book accessible, but also to speculatively frame exciting ideas about blockchain in construction in a manner that positions some of the chapters as answers, and other chapters as questions for the community to resolve in the future. This is only true and brave for both blockchain in construction and crypto-economics as young fields of practice and research.

We would like to thank all authors for their tenacity and efforts to tackle important questions in a field that is still young, but highly promising in terms of shaping our collective future.

Some definitions:

DLT – Decentralised Ledger Technologies

Distributed ledgers are distributed databases where each participant holds a copy of the data (across sites and geographies) and supported by a mechanism to synchronise and achieve consensus between these copies. DLTs also offer the feature of having the data accessible to multiple parties. The questions arise then of the need for a peer to peer network between the computing nodes holding the data and a consensus mechanism to synchronise the data unto a single version, as DLTs do not have a central administrator, in distinction to distributed databases who might be subject to a central control. This lack of a central authority is a feature rather than a weakness. When a new update to the ledger is needed, all nodes construct a transition which is then voted on by use of a consensus algorithm, i.e. a process by which nodes vote for which update is true and which is not. Security is achieved by using public key cryptography and cryptographic signatures to establish identities. Consensus mechanisms follow in many cases scenarios of the "Byzantine Generals problem" (Lamport et al, 1982]: a set of actors in a network need a reliable mechanism with which to arrive at a single version for the truth, even if some of the participants fail or actively undermine the network.

Blockchains

Blockchains are a special version of distributed ledgers which were invented to facilitate the idea behind digital cash in Bitcoin (Nakamoto 2009]. In the Bitcoin blockchain, Nakamoto introduces a series of features the free the bedrock of what we call now a public permission less blockchain:

- Incentives for the computing nodes to stay honest via the awarding of new crypto-tokens to the nodes,
- the collapse of all transactions at a given moment in a cryptographic hashing mechanism called a Merkle tree, where transactions are reduced to a single hash by progressively hashing them in pairs,
- a timestamp feature,
- a consensus mechanism using a proof of work algorithm,
- a number used only once, the previous hash in a block of information which the computing nodes store on their ledger.

Each block is connected with the previous one by containing its root hash, creating a chain of blocks, hence the term blockchain. This mechanism along with the incentivisation, secures the immutability of the blockchain, as users cannot go back and change the data, while incentives holds computing nodes true to the purpose and mission of the network which is the reliability and security of the transitions in a peer to peer fashion.

Inspired by the Bitcoin blockchain, or rather attempting to expand its mechanisms for holding values, where the blockchain operates additions and subtractions, a group of programmers created the Ethereum blockchain, which expands the blockchain computing paradigm, acting as a decentralised, global, distributed computing platform capable of any Turing Complete computation (Turing 1937).

Ethereum behaves as a state machine, i.e. a Turing machine that allows nodes to change its state. Thus, it is possible to record a variety of information on the Ethereum Blockchain. It also presents the benefit of being programmable through code, either in its native language solidity or even python. A code executed on the Ethereum blockchain is called a 'smart contract' as its immutable nature equates the concept of code execution with law.

Smart contracts

Smart contracts precede the "Ethereum" blockchain, having been introduced earlier by cryptographer Nick Szabo, who described them as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" (Szabo, 1997). Note that a smart contract does not necessarily have to constitute a valid binding agreement by law, as compliance with the valid legal framework is needed. However, smart contracts can be explained as the computing code equivalent of automated vending machines [Savelyev 2016]. Smart contracts get deployed unto blockchain packaged unto a transaction. The Byzantine-fault tolerance mechanisms of the blockchain ensure then that the smart contract can not be tampered within the same manner that transactions are secured, allowing only validated accounts on the network to act on the smart contract. Deployed smart contracts act then as automatons, with the blockchain automatically executing their code when specific events trigger the computation. This creates then an infrastructure automation layer where public permission blockchain can be used such as Ethereum as global computing state machines.

Cryptoeconomics

Cryptoeconomics have emerged as an experimental and intra-disciplinary field of economics, peer-to-peer cryptography, systems design and various other concepts such as game theory. Cryptoeconomics

attempt to guarantee certain outcomes and information security properties using incentives and penalties, to self-regulate digital economies. As such, the idea of external regulators and the state as guarantors of the validity of financial transactions do not exist as the system relies on the computing protocol for regulation. Part of the epistemic and practical novelty of blockchains as crypto-economic systems lies in that trust, transactional infrastructure and incentives are encoded in the computing protocol of the network rather than decided by existing structures. As such Cryptoeconomics have the potential to radically change the manner in which various industries operate.

References

'Ethereum Whitepaper'. n.d. Ethereum.Org. Accessed 27 January 2022. https://ethereum.org.

Szabo, N (1997): Formalizing and Securing Relationships on Public Networks'. n.d. Accessed 27 January 2022. https://firstmonday.org/ojs/index.php/fm/article/download/548/469.

Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982 The Byzantine Generals Problem'. *ACM Transactions on Programming Languages and Systems* 4 (3): 20.

Nakamoto, Satoshi. 2008 'Bitcoin: A Peer-to-Peer Electronic Cash System',

Savelyev, Alexander. 2016. 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law'. SSRN Scholarly Paper ID 2885241. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.2885241.

Turing, A. M. 1937. 'On Computable Numbers, with an Application to the Entscheidungsproblem'. *Proceedings of the London Mathematical Society* s2-42 (1): 230–65. https://doi.org/10.1112/plms/s2-42.1.230.

'Wood - Ethereum a secure decentralised generalised transaction layer. n.d. Accessed 27 January 2022. https://ethereum.github.io/yellowpaper/paper.pdf.