Trust, Decentralization, and the Blockchain

Author : Andres Guadamuz

Date : December 12, 2019

Kevin Werbach, **The Blockchain and the New Architecture of Trust** (2018).

The distributed ledger technology known as the blockchain has continued to gather interest in legal academia. With a growing number of books and academic papers exploring almost every aspect of the subject, it is always good to have a comprehensive book that not only covers the basics, but also provides new insights. Kevin Werbach's *The Blockchain and the New Architecture of Trust* provides an in-depth yet easy-to-comprehend analysis of the most important aspects of blockchain technology. It also manages to convey astute analysis and some needed and sobering skepticism about the subject.

Werbach describes the characteristics of blockchains, providing a thorough and easy-to-understand introduction to key concepts and the reasons why the technology is thought to be a viable solution for various problems. A blockchain is a cryptographic distributed ledger that appends information in a supposedly immutable manner. An open record of all transactions is made public, which then communicates a "shared truth", that is a single proof that everyone trusts because it has been independently verified by a majority of the participants in the network. This technology is thought to be a solution for problems such as the lack of reliability in accounting records, and for double spending, where the same amount of currency is used in two different transactions. While the first half of the work is likely to be the most useful for those who are not familiar with the underlying technical concepts, the book really makes its best contributions in its later chapters, where the author begins to criticize various aspects of the technology.

A core topic of the book is that of "a crisis of trust," and Werbach explains how the blockchain has been repeatedly offered as a possible solution to this problem. Everyday life is built on trust, and we are always engaged in rational calculations based on trust-related questions: Can I trust this person with my car keys? Can I trust my bank? Can a lender trust a borrower? We have built systems of risk assessment, of managing trust, and of redress when trust breaks down. While our financial and legal systems rely on a good measure of trust, it is seen by many as an added expense and an obstacle to a well-functioning economy. Werbach explains how in some circles the concept of trust has become "almost an obscenity." The need for trust is a vulnerability, a flaw that should be remedied.

Enter the blockchain, a distributed ledger technology that is supposed to solve this perceived crisis of trust by being "trustless"—that is, doing away with the need for trust. The blockchain is proposed as a better solution than past architectures of trust, such as centralized "Leviathans," third-party arbiters, or peer-to-peer systems. States or other large central authorities historically addressed the problem of trust through enforcement. Alternatively or additionally, intermediaries have acted as arbiters and providers of trust. In peer-to-peer systems, trust is built on an assumption of shared values and norms, and on principles of self-governance.

Werbach explains why the blockchain is characterized as better:

> In any transaction, there are three elements that may be trusted: the counterparty, the intermediary, and the dispute resolution mechanism. The blockchain tries to replace all three with software code. People are represented through arbitrary digital keys, which eliminates the contextual factors that humans use to evaluate trustworthiness. (P. 29.)

Werbach identifies a problem, however: for a system that appears to rely so much on the concept of trustlessness,

there is still a lot of trust required in intermediaries in the blockchain space. This observation proves Nick Szabo's comment that "there is no such thing as a fully trustless institution or technology". Very few people have the technical know-how to become fully self-reliant in the use of blockchain technology, so most people end up having to trust some form of intermediary. The book covers several disasters, such as the infamous QuadrigaCX fiasco, where users lost millions due to either negligence or fraud. "The blockchain was developed in response to trust failures, but it can also cause failures." (P. 117.)

Werbach cites other examples where intermediaries have exercised a large amount of control, such as the Decentralized Authority Organization (DAO) hack. The DAO was a way to manage transactions on the Ethereum blockchain using smart contracts and a shared pool of funds. A hacker found a way to syphon out funds through a bug in the code. A truly trustless decentralized system would allow this to happen, but the DAO developers decided to fork the code, re-writing history, erasing the bug, and creating a new version of the blockchain where the hack never occurred. This has been seen as evidence that trust is still involved—a trust in blockchain developers and intermediaries.

Werbach also identifies that the blockchain failed in practice to be a fully decentralized system. Satoshi Nakamoto, the pseudonymous inventor of the concept of the blockchain, dreamt of a system where millions of individual miners would come together to verify transactions, making the blockchain a truly decentralized endeavor. But what has happened is more centralized, with mining concentrated in a few massive conglomerates.

Werbach makes some very good criticisms of another use of the blockchain, namely smart contracts. There are various reasons for distrusting smart contracts, but one of the most compelling offered in the book is that despite advances in machine learning, "computers do not have the degree of contextual, domain specific knowledge or subtle understanding required to resolve contractual ambiguity." (P. 125.)

Finally, Werbach goes into several interesting discussions specific to some platforms, and looks at regulatory responses. I found the regulatory discussion interesting, but perhaps the least useful aspect of the book. The attempts to regulate the blockchain phenomenon move so fast that a few of the examples offered are already outdated, even though the book was published in 2018. As a European reader, I would also have liked a bit more coverage of international developments; while the author cites several cases from abroad, these were not dealt with in depth.

However, these are minor concerns. This is a thorough, informative, and highly readable book that should be the go-to reference for anyone interested in the subject of blockchain and the law.

Cite as: Andres Guadamuz, *Trust, Decentralization, and the Blockchain*, JOTWELL (December 12, 2019) (reviewing Kevin Werbach, **The Blockchain and the New Architecture of Trust** (2018)), https://cyber.jotwell.com/trust-decentralization-and-the-blockchain/.