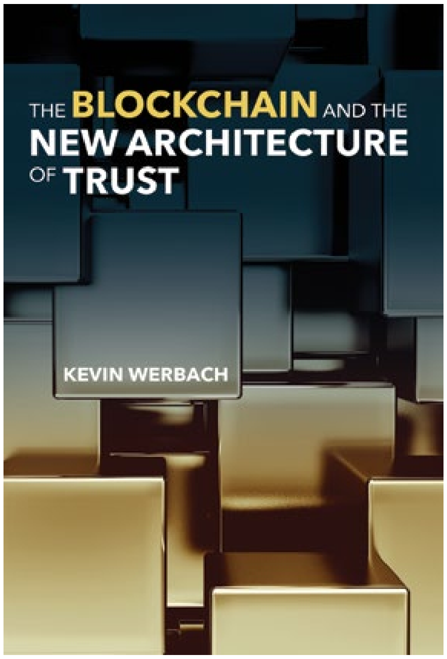
Who Can You Trust?

DRAGAN BOSCOVIC

Kevin Werbach's *The Blockchain and the New Architecture of Trust* offers easy-to-follow explanations of how a technology resting on foundations of mutual mistrust can become trustworthy. If you are interested in gaining a deeper perspective on the blockchain landscape, beyond the hyped claims of techno-utopians or regular reports of cryptocurrency hacking and financial fraud, then this well-researched and well-cited book is for you. It offers an optimistic sense of the possibilities of blockchain technology, supported by governance, regulation, and law, which could have a wide range of important applications.

Werbach is a professor of legal studies and business ethics at the University of Pennsylvania's Wharton School. He is a renowned expert on emerging technology, earning his reputation by using his interdisciplinary research interests to map how business, law, and society are impacted by technologies such as broadband, big data, gamification—and now blockchain. Along with these accomplishments, Werbach 20 years ago helped the US government develop its approach to internet policy as the counsel for new technology policy at the Federal Communications Commission during the Clinton administration.

The Blockchain and the New Architecture of Trust is a balanced book for anyone who wants to sift through the blockchain hype and understand the technology's implications for business and society. Blockchain is essentially a digital public database, or ledger, of transactions that is stored on computers around the world. It is nearly impossible to change or tamper with data in a blockchain, and no single entity controls or owns the blockchain. Although the original blockchain was developed in the late 2000s to track balances for the cryptocurrency Bitcoin, it can be used for many kinds of digital transactions, including verifying contracts, authenticating records, and tracking health records.



The Blockchain and the New Architecture of Trust
by Kevin Werbach. Cambridge, MA: MIT Press, 2018, 344 pp.

The central theme of Werbach's book is how blockchain technology, which relies on building trust in a trustless system, can become broadly accepted as trustworthy—and be used by consumers, businesses, and governments to build real-world applications. Werbach offers his views on what the future might look like for the technology while highlighting the importance of creating legal and regulatory clarity to support innovation and protect consumers. He does an exceptionally good job of explaining how blockchain works, its history, the hype associated with it, and the concerns it has created. The book details concrete examples both from the development of blockchain and the development of the internet, drawing parallels between the two in terms of their relationship to the law.

Werbach offers reasoned explanations as to why blockchain is far more than a slow, immutable database or a difficult-to-understand cryptographic method. Instead, he focuses on the benefits of the supreme efficiency of synchronization in a distributed system such as blockchain. He argues that although blockchain is inefficient and slow in processing and recording individual transactions, it is far more efficient in establishing the global state of the system. This is important because when all the globally distributed nodes in the blockchain ledger work with the same level of information and avoid making irrelevant or wrong decisions, consensus builds up in blockchain's trustless operations.

The book, perhaps uniquely among the many volumes devoted to Bitcoin and the blockchain, explains that law and regulation must play a central role in reinforcing the built-in trust of decentralized digital ledgers. Werbach postulates that blockchain isn't an alternative to trust; instead, it helps remove dependencies on intermediate entities in complex transactional workflows. Contrary to the mysterious Bitcoin developer Satoshi Nakamoto's conclusion in his 2008 white paper that introduced the blockchain, in which he claimed that "We have proposed a system for electronic transactions without relying on trust," the complete circumvention of trust is simply not possible. Trust is essential to how human society functions, and it goes beyond the formal security of consensus on a distributed ledger.

To that end, Werbach argues that society needs a better understanding of what kinds of problems blockchain is capable of addressing, based on the kinds of trust needed for particular classes of applications. He puts forward a thought-provoking thesis that the legal system will be the primary force that determines whether a given blockchain ecosystem succeeds. That should not be surprising, bearing in mind that law, regulation, and governance are mechanisms of trust in conventional socioeconomic structures and, as such, will be used to promote trust in blockchain-based solutions as well. But this has not been part of the hype around blockchain, whose advocates claim that the technology can bypass traditional institutions entirely.

Despite the fact that the book was published in November 2018, in the midst of the most recent cryptocurrency market crash, it portrays the blockchain technology that underpins cryptocurrency as the next great digital platform, whose future—not necessarily linked to crypto asset boom and bust cycles—is incredibly bright. Although cryptocurrencies are prone to price volatility, Werbach doesn't question the sustainability of the whole blockchain concept for applications of trust. This can be seen in cases in which the cost of trust is a problem (typically proportional to the number of trust layers or intermediaries in a given workflow; think of all the entities involved in a simple credit card transaction, for example), or where there is a "trust gap" among coordinating entities. The first case applies to most cryptocurrency or digital asset use cases, while the second generally represents enterprise applications, such as corporate supply chains.

Werbach identifies three main blockchain applications. The first uses cryptocurrency to create financial inclusion opportunities for the so-called unbanked by removing inefficiencies related to financial transactions. The second tracks assets using the distributed ledger technology that blockchain enables. This is particularly important in financial services and in supply chains, where there are multitrillion-dollar problems associated with a lack of unification across the system. The third involves regulated asset trading through security token offerings and crypto-derivatives; these are basically blockchain-based coins or tokens that are sold to investors to raise money for a project. (Most of these endeavors, it should be noted, fail within the first few months; the system is plagued with scams and securities law violations—hence the need for *regulated* asset trading.) The prospect of a secure, programmable, digital token that represents assets or intangibles is a Wall Street dream, and financial communities around the world are racing to turn that dream into a reality.

The book identifies four different trust architectures. The first is peer-to-peer trust, which typically comes about when individuals learn to trust each other based on morals and reputational systems. The second is leviathan trust (so named after the English philosopher Thomas Hobbes's conception of the state), which corresponds to an institutional trust that allows distrustful parties to enter into agreement because they trust that a government system will help resolve disputes. The third is intermediary trust, in which parties do not need to trust each other if they trust the intermediary; a good example is the credit card system, which allows buyers and sellers to engage in commerce. The fourth—the "new architecture of trust" of the book's title—is distributed trust. This refers to the users' trust in the particular decentralized system that is blockchain, without requiring trust in any of the system's individual components.

Blockchain solutions don't eliminate the need to continue to trust human institutions. There will always be a need for institutional sources of trust that can't simply be replaced by technology alone. Any blockchain system will have to coexist with other, more conventional systems. Humans need to stay in charge, and there is always a need for governance and oversight outside the system. As long as "hard forks" are a possibility—that's when the people in charge of a blockchain step outside the system to change it—people will need to be in charge.

What blockchain does, and where its value lies, is to shift some of the trust in people and institutions to trust in technology. Blockchain users trust the cryptography, the protocols, the software, the computers, and the network, but this trust must be embedded in larger governance systems. Blockchain-based contracts, for example, need viable dispute resolution mechanisms, which will be a combination of traditional legal recourse and arbitration, on one hand, and novel decentralized approaches on the other.

Currently, when user trust in blockchain turns out to be misplaced, there is no recourse. If a Bitcoin exchange gets hacked, or you forget your log-in credentials, you lose your money. If there's a bug in the code of your smart contract, the contract could be invalid. In many ways, trusting technology is harder than trusting people. Would you rather trust a human legal system or some computer code you don't have the expertise to audit? On the organizational side, the biggest challenge in most business and financial service implementations of blockchain technology is getting the participants to cooperate. Just because blockchain technically offers secure data sharing without giving up control doesn't mean companies will feel comfortable ceding power to blockchain-based ventures involving their competitors.

Werbach offers an insightful explanation of blockchain's relationship to internet architecture. Many factors, mostly having to do with security, have led to a centralization of some of the internet's key architecture. Blockchain could function as a new layer in the internet's structure, one that can strengthen such functions as identification, authentication, attestation, and property rights. In other words, blockchain could not only remove some of the reasons for strong centralization, but also create a favorable climate for decentralized applications—and presumably for the innovation and experimentation that characterized the early internet.

***Dragan Boscovic** is a research professor in the School of Computing, Informatics, and Decision Systems Engineering at Arizona State University. He also is the director of the university's Blockchain Research Lab, whose mission is to advance the research and development of blockchain-based technologies for use in business, finance, health care, and other areas of potential impact.*