New Kids on the Blockchain

Author : Andres Guadamuz

Date : April 3, 2018

David Gerard, *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts* (2017).

Bitcoin was created in 2009 by a member of a cryptography mailing list who goes under the pseudonym of Satoshi Nakamoto, and whose identity is still a mystery. The project was designed to become a decentralized, open source, cryptographic method of payment that uses a tamper-free, open ledger to store all transactions, also known as the blockchain. In a field that is replete with hype and shady operators, David Gerard's book *Attack of the 50 Foot Blockchain* has become one of the most prominent and needed sceptical voices studying the phenomenon. Do not let the amusing title you deter you; this is a solid book filled with solid and thorough research that goes through all of the most important aspects of cryptocurrencies, and it is one of the most cited take-downs of the technology.

The book covers a wide range of topics on cryptocurrencies and blockchain, and does so in self-contained chapters that can be read almost independently. The book does not follow a strict chronological order. This structure actually makes the book entirely more readable and a delight from cover to cover, not only because of the interesting subject matter, but also because of Gerard's wit and knowledge.

The work follows three main themes: explaining Bitcoin and unearthing its various problems; the prevalence of fraudulent practices and unsavoury characters in cryptocurrencies, and then explaining blockchains and smart contracts, and their various criticisms.

In the introductory section Gerard does an excellent job of explaining the technology without the usual techno-jargon that surrounds the subject, and goes through the main reasons that proponents advocate the use of Bitcoin. Cryptocurrencies are often offered as a decentralised solution to the excesses incurred by financial institutions and governments. "Be your own bank" is cited as one of the advantages of Bitcoin, but Gerard accurately describes the various problems that this presents. Being your own bank means requiring security fit for a bank, which most people do not have. Moreover, some of the characteristics present in Bitcoin make it particularly unsuitable as a means of payment. Bitcoin is based on scarcity; only 21 million coins will ever be mined, so there is a strong incentive to hoard coins and hold. Similarly, cryptocurrency transactions are irreversible; if you lose coins in a hack, or make a transaction mistake, the coins are gone forever.

In the chapters dealing with fraud, Gerard does an excellent job of going through the dark side of cryptocurrencies. Cryptocurrencies rely on intermediaries, either exchanges that will accept your "fiat" currency and exchange it into digital currency, or "wallets", where people can store their coins. The problem is that this unregulated space attracted fraudsters and amateurs in equal measure, and during its short history the space has been filled with Ponzi schemes, con-men, and manipulators. Gerard also describes the use of Bitcoin in the Dark Web, where it is the currency of choice of various illegal businesses.

But it is in his criticism of the blockchain technology where the book really shines. Even vocal Bitcoin critics used to think that that even if cryptocurrencies fail, the underlying blockchain technology would

remain and become an important contribution to the way in which online transactions are made. Gerard became one of the first critics of the blockchain itself.

The blockchain is an immutable and decentralised record of all of the transactions that requires no trust in an intermediary. This is supposed to prove useful in any situation where a trustless system is required. But as Gerard points out, there are not a lot of situations when this is even the case, and most instances presented by blockchain advocates are not necessary. The book describes two main issues with using blockchain in a business environment. Firstly, decentralization is always expensive; there is a reason why many companies have been moving towards centralization of network services through the hiring of cloud providers. Decentralization means that you have to make sure that everyone is using the same protocols and compatible systems, but also you have to account for redundancies as you have to rely on services that are not always available, this results in slower and more cumbersome networks that spend more energy to produce a similar result. Secondly, if data management is a problem in your business, then adding a blockchain won't make the problem go away. On the contrary, he sets out a number of questions that must be asked whenever anyone is thinking of implementing a blockchain to existing business models, including whether the technology can scale, and whether a centralised system will work just as well.

Finally, the book analyses smart contracts, which are contracts conducted digitally through a combination of cryptocurrencies and tokens recorded on a blockchain. The idea is that the parties to a contract code terms and conditions into an immutable token written in computer code which defines the parameters of the contract (conditions, payment, operational parameters), and those who want to transact with each other will write another token that will meet those parameters, at which point the payment is made and the electronic contract concluded. This contract is immutable and irrevocable.

Gerard accurately points out that this combination of immutability and irrevocability are toxic in a legal environment, as any error in the code can lead to nefarious legal consequences. Traditional contracts rely on human intent, and if a mistake is made or a conflict arises, the parties can go to court. But in a smart contract, the code is the last word, and there is no recourse in case of an error or a conflict other than trying to re-write the blockchain, which is not possible unless a majority of participants in the scheme agree to change the code.

This book is a must-read for anyone interested in an easy-to-read and enjoyable criticism of cryptocurrencies and the blockchain. It is a testament of the strength of the ideas presented that we are just now starting to undergo a much-needed check on the blockchain hype from various quarters. Even if cryptocurrencies manage to get past this early stage unscathed, it will be books like this one that will help to narrow the focus away from the narrative of bubbles and easy gains.

Cite as: Andres Guadamuz, *New Kids on the Blockchain*, JOTWELL (April 3, 2018) (reviewing David Gerard, *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts* (2017)), https://cyber.jotwell.com/new-kids-on-the-blockchain/.