THE BUSINESS BLOCKCHAIN
promise, practice, and application of the next Internet technology

foreword by Vitalik Buterin

WILLIAM MOUGAYAR
Author of Centerless

WILEY
THE BUSINESS BLOCKCHAIN
THE BUSINESS BLOCKCHAIN

Promise, Practice, and Application of the Next Internet Technology

WILLIAM MOUGAYAR

FOREWORD BY VITALIK BUTERIN
For my parents, who continue to be by my side.

To Maureen, with whom everything is possible.

And to our beloved dog, Pasha, the brave little Bichon Frisé. You filled my heart forever.
CONTENTS

Foreword VITALIK BUTERIN ix
Acknowledgments xiv
A Personal Preface xvi
Introduction xxi
1 What is the Blockchain? 1
2 How Blockchain Trust Infiltrates 29
3 Obstacles, Challenges, & Mental Blocks 61
4 Blockchain in Financial Services 85
5 Lighthouse Industries & New Intermediaries 109
6 Implementing Blockchain Technology 124
7 Decentralization as the Way Forward 147
   Epilogue 167
   Selected Bibliography 171
   Index 173
   Additional Resources 177
   About the Author 179
this decade is an interesting time for the development of decentralized technologies. Although cryptographers, mathematicians and coders have been working on increasingly specific and advanced protocols in order to get stronger and stronger privacy and authenticity guarantees out of various systems—from electronic cash to voting to file transfer—progress was slow for over 30 years. The innovation of the blockchain—or, more generally, the innovation of public economic consensus by Satoshi Nakamoto in 2009—proved to be the one missing piece of the puzzle that single-handedly gave the industry its next giant leap forward.

The political environment seemed to almost snap into place: the great financial crisis in 2008 spurred growing distrust in mainstream finance, including both corporations and the governments that are normally supposed to regulate them, and was the initial spark that drove many to seek out alternatives. Then Edward Snowden’s revelations in 2013, highlighting how active the government was in realms citizens once believed private, were the icing on the cake. Even though blockchain technologies specifically have not seen mainstream adoption as a result, the underlying spirit of decentralization to a substantial degree has.

Applications ranging from Apple’s phones to WhatsApp have started building in forms of encryption that are so strong that even the company writing the software and managing the servers cannot break it. For those who prefer corporations to government as
their boogeyman of choice, the advent of “sharing economy 1.0” is increasingly showing signs of failure to fulfill what many had originally seen to be its promise. Rather than simply cutting out entrenched and oligopolistic intermediaries, giants like Uber are simply replacing the middleman with themselves, and not always doing a better job of it.

Blockchains, and the umbrella of related technologies that I have collectively come to call “crypto 2.0,” provide an attractive fix. Rather than simply hoping that the parties we interact with behave honorably, we are building technological systems that inherently build the desired properties into the system, in such a way that they will keep functioning with the guarantees that we expect, even if many of the actors involved are corrupt.

All transactions under “crypto 2.0” come with auditable trails of cryptographic proofs. Decentralized peer-to-peer networks can be used to reduce reliance on any single server; public key cryptography could create a notion of portable user-controlled identities. More advanced kinds of math, including ring signatures, homomorphic encryption, and zero-knowledge proofs, guarantee privacy, allowing users to put all of their data in the open in such a way that certain properties of it can be verified, and even computed on, without actually revealing any private details.

What is most surprising to early adopters of the technology, however, is just how rapidly institutional adoption has spread in the last two years. All the way from 2011 to 2013, the blockchain scene—or, realistically, what was then just the “bitcoin” scene—was very cryptoanarchist in spirit, with colorful and idealistic revolutionaries excited about “fighting the power” (or, more precisely, routing around the power). Today in 2016, however, the most exciting announcements all have to do with some collaboration announced with IBM or Microsoft, a research paper by the Bank of England, or a banking consortium announcing yet another round of new members.
What happened? In part, I would argue that the cryptoanarchists underestimated how flexible, technologically progressive, and even idealistic large corporations and banks can be. We often forget that corporations are made up of people, and people inside of corporations often have similar values and concerns to the kinds of regular people whom you might find at meetups. It might seem as though “the trust machine,” as The Economist calls it, is purely a replacement for centralized anchors of trust, both in finance and elsewhere, that rely on real-world reputation and regulatory oversight, but the reality is much more complex. In truth, institutions do not fully trust one another either, and centralized institutions in one industry are just as concerned about centralization in other industries as regular people are. Energy companies, which are involved in producing and selling electricity, are just as happy to sell to a decentralized market as they are to a centralized one, and they may even prefer the decentralized version if it takes a smaller cut.

Furthermore, many industries are decentralized already, to an extent that many people outside of these industries do not appreciate, but they are decentralized in an inefficient way—a way that requires each company to maintain its own infrastructure around managing users, transactions, and data, and to reconcile with the systems of other companies every time it needs to interact. Consolidation around a single market leader would, in fact, make these industries more efficient. But neither the competitors of the likely leader nor antitrust regulators are willing to accept that outcome, leading to a stalemate. Until now. With the advent of decentralized databases that can technologically replicate the network effect gains of a single monopoly, everyone can join and align for their benefit, without actually creating a monopoly with all the negative consequences that it brings.

This is the story that arguably drives the interest in consortium chains in finance, blockchain applications in the supply chain industry, and blockchain-based identity systems. They all use
decentralized databases to replicate the gains of everyone being on one platform without the costs of having to agree on who gets to control that platform and then put up with them if they choose to try to abuse their monopoly position.

In the first four years after Satoshi’s launch of Bitcoin in January 2009, much attention focused on the currency, including its payment aspects and its function as an alternative store of value. In 2013, attention started to shift to the “blockchain 2.0” applications: uses of the same technology that underlies Bitcoin’s decentralization and security to other applications, ranging from domain name registration to financial contracts to crowdfunding and even games. The core insight behind my own platform, Ethereum, was that a Turing-complete programming language, embedded into the protocol at the base layer, could be used as the ultimate abstraction, allowing developers to build applications with any kind of business logic or purpose while benefiting from the blockchain’s core properties. Around the same time, systems such as the decentralized storage platform InterPlanetary File System (IPFS) began to emerge, and cryptographers came out with powerful new tools that could be used in combination with blockchain technology to add privacy, particularly zk-SNARKs, or zero-knowledge Succinct Non-Interactive ARgument Knowledge. The combination of Turing-complete blockchain computing, non-blockchain decentralized networks using similar cryptographic technologies, and the integration of blockchains with advanced cryptography was what I chose to call “crypto 2.0”—a title that may be ambitious, but which I feel best captures the spirit of the movement in its widest form.

What is crypto 3.0? In part, the continuation of some of the trends in crypto 2.0, and particularly generalized protocols that provide both computational abstraction and privacy. But equally important is the current technological elephant in the room in the blockchain sphere: scalability. Currently, all existing blockchain
protocols have the property that every computer in the network must process every transaction—a property that provides extreme degrees of fault tolerance and security, but at the cost of ensuring that the network’s processing power is effectively bounded by the processing power of a single node.

Crypto 3.0—at least in my mind—consists of approaches that move beyond this limitation, in one of various ways to create systems that break through this limitation and actually achieve the scale needed to support mainstream adoption (technically astute readers may have heard of “lightning networks,” “state channels,” and “sharding”).

And then, there is also the question of adoption. Aside from the simple currency use case, “crypto 2.0” in 2015 saw a lot of people talking about it, developers releasing base platforms, but not yet any substantial applications. In 2016, we are seeing both startups and institutional players develop proof of concepts. Of course, the vast majority of these will never get anywhere and slowly wither away and die. That is inevitable in any field. It is a truism of entrepreneurship generally that 90% of all new businesses fail. But the 10% that succeed will likely at some point be scaled up into full-on products that reach millions of people—and that’s where the fun really begins.

Perhaps William’s book will inspire you to understand and, perhaps, join in refining the business blockchain.

Vitalik Buterin

Ethereum inventor and Chief Scientist,
Ethereum Foundation

APRIL 2, 2016