



Contributions to Finance and Accounting

Gioia Arnone

# Navigating the World of Cryptocurrencies

Technology, Economics, Regulations,  
and Future Trends

*Foreword by Samrat Ray*

 Springer

# **Contributions to Finance and Accounting**

The book series 'Contributions to Finance and Accounting' features the latest research from research areas like financial management, investment, capital markets, financial institutions, FinTech and financial innovation, accounting methods and standards, reporting, and corporate governance, among others. Books published in this series are primarily monographs and edited volumes that present new research results, both theoretical and empirical, on a clearly defined topic. All books are published in print and digital formats and disseminated globally. This book series is indexed in Scopus.

Gioia Arnone

# Navigating the World of Cryptocurrencies

Technology, Economics, Regulations,  
and Future Trends

Foreword by Samrat Ray

 Springer

Gioia Arnone  
Department of Managerial and Quantitative Studies  
University of Naples Parthenope  
Napoli, Italy

Department of Private and Economic Law  
Vrije Universiteit Brussel  
Brussels, Belgium

ISSN 2730-6038                      ISSN 2730-6046 (electronic)  
Contributions to Finance and Accounting  
ISBN 978-3-031-69175-1              ISBN 978-3-031-69176-8 (eBook)  
<https://doi.org/10.1007/978-3-031-69176-8>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

# Foreword

## Introduction to Cryptocurrencies

As with so many disruptive technologies, the development of cryptocurrencies usefully maintains a respectful if not publicly positive relationship with the financial order that it challenges. Public and open source in nature, there are strong forces pushing the development of cryptocurrency technology, particularly for established activities in business and finance. Although trading plays a considerable role in the cryptocurrency communities and market viability is often cited as a necessary trait of a good cryptocurrency, the key today—as in any good platform—is the set of available applications, both present and future (Albayati et al. 2020).

Financial professionals, in both their official and non-official capacities, are actively engaging in mining, governance of the cryptocurrency networks, and evangelization. Institutions directly recognize prospects in early adoption and investment choices in cryptocurrencies or blockchain services. While the “protocol wars” and adversarial markets raging for world technology dominance during the earlier Internet era failed to materialize in all but a handful of cases, this is certainly not true for cryptocurrencies. The cause and effect are different, but the relationship is just as close (Chen 2021).

As a result, opinions and beliefs about the potential viability, or not, of cryptocurrencies are driving not only academics but also policymakers. The degree of attention is unique if not amusing—a search on the US Office of Foreign Asset Control (OFAC) website indicates only two instances of the term “blockchain,” both issued on Wednesday, November 28, 2018, almost 10 years after its formation. Finally, defenders of the status quo are responding intelligently, applying lessons from cryptography research and practice to the problem created by cryptocurrencies, insisting that they follow their rules, be scalable and usable through trusted enforcers and center operators (Campbell-Verduyn and Giumelli 2022).

Cryptocurrencies have gained an unprecedented status in the realm of tech-enabled decentralization and global finance (Omarova 2020). The field of cryptocurrencies is certainly lively and open to a fairly wide range of interpretations; defining what a

cryptocurrency is, and how it fits into the broader categories of digital, token, or asset in the realm of decentralized platforms, remains controversial. Historically, cryptocurrencies are a natural offshoot of the Internet revolution that dis-intermediated any number of trusted entities (Ghaemi et al. 2021). The hyperbolic growth of cryptocurrencies provides validation—from a part of the world that has mostly failed to embrace cutting-edge technological business models—that the disruptive threats to finance, legacy systems, and traditional intermediaries are real. Their adoption is, to a large extent, a consequence of post-2000 thinking. Not only are cryptocurrencies directly rooted in advances in practical cryptography and systems security, but the communities and markets built on cryptocurrencies, their decentralized bases, and blockchain technologies also reflect a post-2000 shift in where the wealth of the World Wide Web truly resides. These gains have not been lost in the larger financial communities, regulators, or even the US Central Intelligence Agency (Lipton and Treccani 2021).

### ***Definition and Characteristics of Cryptocurrencies***

The design features of Bitcoin have gained great interest from academics and experts in various disciplines, such as economics, finance, law, computer science, cryptography, and engineering. Cryptocurrencies possess a unique set of characteristics, specifically the absence of a central issuer, the employment of a public and immutable ledger to record all transactions, the use of cryptographic algorithms to secure the ledger itself and digital wallet, the permissions and costs to alter the ledger, the incentive design to ensure the security of the ledger, and finally, the decentralized nature of the system. These characteristics combined allow the creation of a system that records, in a secure way, all transaction agreements among individuals and groups of individuals and can thus be used as a form of money (Fosso et al. 2020).

Bitcoin and its derivatives and competitors that have emerged in recent years have raised significant attention not only in the financial industry but in many other fields. Cryptocurrencies offer an alternative to traditional currencies and other financial assets, as they provide unique technological features, a flexible and proxy form of peer-to-peer transactions, and are expected to be more robust compared to traditional money. Bitcoin and other cryptocurrencies operate without central authorities and are operated by the people using them and by the incentives they find to keep participating in the transactions, which are mainly given by the release of the cryptocurrencies when new blocks of transactions are recorded in the blockchain (Giudici et al. 2020).

### ***Brief History and Evolution***

The network came into global prominence, and Nakamoto disappeared from the Internet in 2010 (Ducrée 2022). Hal Finney was an early supporter of Bitcoin and received the first Bitcoin transaction. Bitcoin was first described by an unknown

person—a group, a male individual, or a female individual—under the pseudonym Satoshi Nakamoto in 2008 in a paper posted to the cryptography mailing list. Nakamoto implemented the first blockchain and a proof-of-work scheme illustrating some of Bitcoin’s operations (Centobelli et al. 2021).

Many cryptographic researchers authored papers and proposed systems that moved the field forward. However, they were unsuccessful in coming up with a solution that gained commercial acceptance. In 1998, Wei Dai proposed b-money, an anonymous, distributed electronic money that created the ground for subsequent developments. In 1998, Nick Szabo proposed Bit gold, a decentralized digital currency that shares many similarities with modern cryptocurrencies, using a solving-puzzles scheme similar to Bitcoin’s proposal. Cryptocurrency dates back to the work of David Chaum, a pioneer in modern cryptography. In 1983, Chaum unmasked numerous capabilities and limitations of cryptographic techniques, and after several breakthroughs, he started DigiCash in 1989. Unfortunately, the company went bankrupt in 1996 (Panda et al. 2023).

## **Cryptocurrency Technology**

Cryptocurrency uses a distributed database, or blockchain, to record the transactions. These transactions are performed by computers solving cryptographic puzzles for which they are rewarded. The rewards come in the form of a new digital asset. By design, these assets are deflationary in nature. That is, either the supply is finite or can expand only at a predictable rate. There are numerous types of cryptocurrencies. In this work, we restrict our study to proof-of-work cryptocurrencies which are popular. The two most widely discussed types of cryptocurrencies are Bitcoin and Litecoin. Bitcoin was the first cryptocurrency which was created in 2009 by a person using the alias of Satoshi Nakamoto. Since then, several cryptocurrencies have been developed in the last few years. A cryptocurrency (or crypto-currency) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the asset. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies. Bitcoin, created in 2009, was the first decentralized cryptocurrency in the world. Since then, many other cryptocurrencies have been created using the blockchain, which is a public distributed ledger used to record the transactions across the network (Chowdhary 2020).

## ***Blockchain Technology***

By providing a public registry of all transactions, the blockchain also provides the solution to the “Byzantine General Problem,” hence allowing for a decentralized trust mechanism. Even though the invention of the blockchain is largely credited to

Satoshi Nakamoto, there is prior research work that described similar concepts with different nomenclature. The blockchain is actually a chain of blocks stored in a shared database that maintains an individual history for each coin and updates the database based on a “Proof-of-Work,” a time-bound computation that grows linearly with the number of transactions in the system. The actual transaction is composed by one originating coin, a list of destination coins, and a signature from its owner, such that users can receive future transactions. This structure ensures that any user who knows the public key corresponding to a coin can verify it, and anybody who wants to transfer it needs to possess the private key associated with that coin. The use of public–private key encryption creates a way of ensuring both authenticity and anonymity (Ducrée 2022; Magnuson 2020).

Among the technological innovations that stood out in the world of IT in the last few years, the blockchain technology arguably is one of the most appealing for its potential to revolutionize a vast array of industries. Originally, the blockchain was developed to work as a public transaction ledger for the cryptocurrency Bitcoin, to solve the issue of double spending of digital currencies. Another attempt at developing a digital currency (eCash) would rely on a single institution’s control and issuance, whereas a digital currency should work under a peer-to-peer logic, where any individual would be able to trust total strangers, without the need of an intermediary institution. The algorithm behind the blockchain solves this issue by working on a public ledger that is virtually impossible to tamper with. Hence the concept, the term blockchain, with new transactions stored in blocks and each block pointing back to the previous one through a hash code, providing a verification of the transactions order (Alshaikhli et al. 2021).

### *Consensus Mechanisms*

The concept of decentralized consensus is simple: it is the creation of an unforgeable financial database—a ledger—that nobody can change. It seems impossible to do without having a single trusted authority, but the essence of Bitcoin has showed us that this is possible. The blockchain—the best-known implementation of a consensus mechanism—is one such cryptographic ledger: it’s just a series of blocks of data, each one referring to the previous one using a hash. The blockchain can’t be easily modified as it would require the alteration of all subsequent blocks and all subsequent work. And given that the blockchain is run by a decentralized peer-to-peer network working under a protocol, trust continues to be distributed among many parties. In a sense, the protocol coordinates the network by providing a set of rules and stipulations that must be obeyed, an element of each block, and a technique for reaching an agreement about which block is next (Hariguna et al. 2021).

The key to any reliable monetary system is consensus: whether and how to increase the money supply has been at the heart of most discussions around central banking throughout history. As we would expect, consensus is also integral to the

cryptocurrency protocol. After all, what is money but a shared concept—a widely accepted metric? And if the quantity of money is determined by tradition, instead of a top-down imposition of fiat, how do people coalesce around a decision? In today’s traditional models, macroeconomists argue that a single authority (the central bank of a country or a basket of countries under the Euro) is the ultimate decider of these rules. However, Bitcoin (the first and most well-known cryptocurrency) was designed as a solution to the central trust problem: instead of passing along the responsibility to a single organization, who gains such power by lucky birth into the country that defines the money supply, the Bitcoin protocol allows us to apply game theory in a more horizontal manner to come to a consensus over a set of rules, that is, *concordia discors* (Judmayer et al. 2022).

### ***Smart Contracts***

While they have advantages over traditional contracts, smart contracts also have limitations. Due to their digital nature, they cannot handle off-chain and real-world events such as exchange rates, the temperature of assets, and real-world identities. Conversely, with traditional contracts, real-world events are traceable while their resolution and enforcement are limited. Smart contracts also depend on the quality of their code and potential errors are difficult to fix after deployment. They may also have problems with encroachments and loopholes which generate litigation costs. The notion of a DOJ (Decentralized Autonomous Organization) gone wrong serves as a cautionary tale in these cases (Solaiman et al. 2021).

In 1994, Nick Szabo, a cryptographer, advanced the idea of smart contracts. Smart contracts are contracts with the terms of the agreement directly written into code. The contract is enforced and executed based on the outcomes of specific actions and events. Ethereum translated the theoretical smart contract concept into reality in 2015. In Ethereum, smart contracts are self-executing code (programs) that perform specific tasks when their conditions are met. For example, a simple smart contract can be written to transfer money to someone once he/she completes a certain task. Smart contracts can interact with distributed applications (dApps) and have use cases in many industries such as voting systems, investment banks, and supply chains. In financial services, for example, smart contracts can automate various processes, reduce paperwork, and reduce litigation risks (Zheng et al. 2020).

### **Cryptocurrency Economics**

We provide a taxonomy of cryptocurrencies that, we argue, relies more on economics and less on technology. We are going to argue that cryptocurrencies present different trade-offs between decentralization, transaction costs, informational

asymmetry, financial intermediary frictions, and security, quite similar to the ones of privately issued monies and banknotes, even if cryptocurrencies are distinct in that they allow us to make this trade-off more ex post than any other financial innovation in history. Our contribution is a dissection of the structure of cryptocurrencies and the identification and characterization of the stylized effects that each type of structure will necessarily have on different types of users—consumers, savers, investors, and entrepreneurs—and on the economy as a whole (Kannengießer et al. 2020).

One of the most common questions that seem to puzzle many newcomers to the cryptocurrency world is the following: What is the value of cryptocurrencies? The comparable sizes of the cryptocurrency market to the money market and the prevalence of several speculative bubbles in the price of cryptocurrencies seemingly erode public belief in the standard efficient market theories that advocate rational behavior and consistent beliefs. In this section, we attempt to answer this question by examining the economics of cryptocurrencies. We provide a way of shedding light into the matter without resorting to the question of being an asset class or simply another form of money (Wątorrek et al. 2021).

### *Supply and Demand Dynamics*

The creation usually slows with predefined demand at specific prices. To minimize their downside risk, transactors must be willing to accept slightly lower prices to sell, while buyers must be willing to pay slightly higher prices to purchase. Actors barter in-kind advantages such as anonymity in order to justify their market participation. By the same logic, the existence of transaction fees suggests that units of cryptocurrency as a medium can exhibit positive value. Some features of cryptocurrencies, such as their scarcity, can affect their demand and supply dynamic independently from their use as a medium of exchange. Specifically, a higher perceived future value of a product results in a higher current market price, and a lower level of supply typically leads to an expected positive effect on the market price. Additionally, expectations regarding potential speculators influencing expectations of future supply, such as thought about mining costs, new coin creation, and rules for existing coin destruction, will affect the supply and demand dynamic (Giudici et al. 2020).

Supply and demand are the fundamental forces determining prices and the success of alternative cryptocurrencies. The price of a cryptocurrency, just like any other asset, is determined by supply and demand forces. Supply is the amount of cryptocurrency coins that exist and are potentially available for trade in a given period and at a given price. Demand is the amount of coins that buyers are willing to buy in a given period and at a given price. New coin creation requires decisions. This is typically done as a fair lottery process called proof of work or proof of stake in which randomly selected nodes are chosen to solve cryptographic puzzles and receive new coins as rewards (Gandal et al. 2021).

## ***Monetary Policy and Inflation***

The money that Bitcoin supplies itself influences the currency's monetary policy. Consequentialism of money management has been inhibited through contractual agreements, such as the promise not to overissue 21 million. From the perspective of jurisprudence, the asset's rate of growth is one reason that impacts the asset's holding into the future. Seigniorage, which is the difference between the actual cost of the currency manufacturing and the money's nominal value, will be used to finance the issuer's other activities in the era of Keynes until receiving the banknotes with insignificant or zero costs. Shilla Friedrich proposed that the severe danger of hyperinflation is undercut. Seigniorage, however, relates to the policy of individual countries, the development of fiat money, corruption of public officials, and collusion with the low tax base under despotic governments (Yang and Zhou 2022).

In this section, we evaluate how Bitcoin behaves as a currency regarding monetary policy and inflation. Specifically, we investigate the supply and demand of Bitcoin, as well as the prediction that the supply of Bitcoin should be perfectly inelastic. We review the empirical performance in various market environments of the seigniorage due to Bitcoin's money issuance. The discussion of Bitcoin's ignore mechanic, limited capacity of money production, and real rate of money growth is slightly redundant with the topic of economic regulation. There is some potential inconsistency with a perfectly inelastic supply of Bitcoin in the near future. Monetary policy is a concern that is very important in many countries. Moreover, the creation and management of money will also have a subtle influence on currency exchanges (Pagnotta 2022).

## **Regulatory Frameworks and Compliance**

The recent decision by the US Securities and Exchange Commission (SEC) was a welcome development in moving the cryptocurrencies toward the financial mainstream. Cryptocurrencies are now treated as an investment option with close resemblance to gold or a commodity, and the exchanges and traders need to be licensed if they have to legally trade in bitcoins. The proposals are also to adopt appropriate standards for disclosures and insurance, which can ensure added protection for all stakeholders. It is important that potential clarity is required on the taxation treatment, which would apply to any gains from cryptocurrency trades. Regulatory compliance is necessary to enhance the reputational image of cryptocurrencies. They would ensure that legitimate business is attracted to a sound, transparent, and safe operating environment. There would be many challenges in arriving at a standard toward regulation, including divergent interests of stakeholders and privacy and ethical policy considerations (Luchkin et al. 2020).

Regulatory authorities in most countries maintain varying degrees of skepticism about cryptocurrencies. Over time, tolerance toward cryptocurrencies is seen to be

changing to regulation. Over the past few years, countries have started proposing guidelines and rules, and some are beginning to regulate the use of bitcoins. However, comprehensive and consistent regulations, which can lead to responsible, stable, and enduring use of cryptocurrencies, are still in the making. Few cryptocurrencies have already taken the initiative to adopt a clear regulatory regime of anti-money laundering policy. While this self-regulation helps them to stay above any legal scrutiny, it is also an admission that their transactions can be misused (Hairudin et al. 2022).

## ***Global Regulatory Landscape***

We then investigate which fundamental and cyclical factors drive the introduction of stricter regulations. For fundamental factors, we consider a combination of economic factors (GDP per capita, world gross product, and bank concentration ratio), institutional and political factors, financial development, the level of technology, and the level of welfare. Finally, we add a set of cyclical variables to capture the links between crypto expansion and regulation. These measures include the macroeconomic and financial context, such as market volatility and the financial stress index. We provide evidence suggesting that a more positive economic and financial environment is associated with stricter regulation regarding the use of cryptocurrencies and the services associated with them. In addition, we find little, if any, evidence of increased anti-money laundering and tax evasion concerns associated with the introduction of stricter regulations (Morton 2020).

Investment in cryptocurrencies has soared in recent years. While most studies examine the investment perspective or financial stability concerns related to cryptocurrencies, little attention has been devoted to the effects of regulation on crypto prices and volumes, or to the factors that drive the evolution of regulations in this space. In this chapter, we try to fill this gap. We first construct a regulatory database counting and categorizing regulatory news in the crypto-space for several jurisdictions. We then examine the impact of regulations on the price and volume of Bitcoin, which always represent the lion's share of the activity and capitalization in the crypto-universe. We find that, while both stricter regulations and news regarding a ban on crypto activities have negative effects on the Bitcoin price, they do not have a significant impact on trading flows (Tetiana et al. 2022).

## ***AML/KYC Requirements***

The verification and identification of the client is a central part of the financial understanding and initiation process, benefiting the customer by avoiding unlawful treatments and activities. Despite the fact that this seems self-evident, there are significant discords with the execution of AML/KYC processes within financial