The Bitcoin Standard Prologue

By Saifedean Ammous

On November 1, 2008, a computer programmer going by the pseudonym Satoshi Nakamoto sent an email to a cryptography mailing list to announce that he had produced a “new electronic cash system that’s fully peer-to-peer, with no trusted third party.”1 He copied the abstract of the paper explaining the design, and a link to it online. In essence, Bitcoin offered a payment network with its own native currency, and used a sophisticated method for members to verify all transactions without having to trust in any single member of the network. The currency was issued at a predetermined rate to reward the members who spent their processing power on verifying the transactions, thus providing a reward for their work. The startling thing about this invention was that, contrary to many other previous attempts at setting up a digital cash, it actually worked.

While a clever and neat design, there wasn’t much to suggest that such a quirky experiment would interest anyone outside the circles of cryptography geeks. For months this was the case, as barely a few dozen users worldwide were joining the network and engaging in mining and sending each other coins that began to acquire the status of collectibles, albeit in digital form.

But in October 2009, an Internet exchange2 sold 5,050 bitcoins for $5.02, at a price of $1 for 1,006 bitcoins, to register the first purchase of a bitcoin with money.3 The price was calculated by measuring the value of the electricity needed to produce a bitcoin. In economic terms, this seminal moment was arguably the most significant in Bitcoin’s life. Bitcoin was no longer just a digital game being played within a fringe community of programmers; it had now become a market good with a price, indicating that someone somewhere had developed a positive valuation for it. On May 22, 2010, someone else paid 10,000 bitcoins to buy two pizza pies worth $25, representing the first time that bitcoin was used as a medium of exchange. The token had needed seven months to transition from being a market good to being a medium of exchange.

Since then, the Bitcoin network has grown in the number of users and transactions, and the processing power dedicated to it, while the value of its currency has risen quickly, exceeding $7,000 per bitcoin as of November 2017.4 After eight years, it is clear that this invention is no longer just an online game, but a technology that has passed the market test and is being used by many for real-world purposes, with its exchange rate being regularly featured on TV, in newspapers, and on websites along with the exchange rates of national currencies.

Bitcoin can be best understood as distributed software that allows for transfer of value using a currency protected from unexpected inflation without relying on trusted third parties. In other words, Bitcoin automates the functions of a modern central bank and makes them predictable and virtually immutable by programming them into code decentralized among thousands of network members, none of whom can alter the code without the consent of the rest. This makes Bitcoin the first demonstrably reliable operational example of digital cash and

digital hard money. While Bitcoin is a new invention of the digital age, the problems it purports to solve—namely, providing a form of money that is under the full command of its owner and likely to hold its value in the long run—are as old as human society itself. This book presents a conception of these problems based on years of studying this technology and the economic problems it solves, and how societies have previously found solutions for them throughout history. My conclusion may surprise those who label Bitcoin a scam or ruse of speculators and promoters out to make a quick buck. Indeed, Bitcoin improves on earlier "store of value" solutions, and Bitcoin's suitability as the sound money of a digital age may catch naysayers by surprise.

History can foreshadow what's to come, particularly when examined closely. And time will tell just how sound the case made in this book is. As it must, the first part of the book explains money, its function and properties. As an economist with an engineering background, I have always sought to understand a technology in terms of the problems it purports to solve, which allows for the identification of its functional essence and its separation from incidental, cosmetic, and insignificant characteristics. By understanding the problems money attempts to solve, it becomes possible to elucidate what makes for sound and unsound money, and to apply that conceptual framework to understand how and why various goods, such as seashells, beads, metals, and government money, have served the function of money, and how and why they may have failed at it or served society's purposes to store value and exchange it.

The second part of the book discusses the individual, social, and global implications of sound and unsound forms of money throughout history. Sound money allows people to think about the long term and to save and invest more for the future. Saving and investing for the long run are the key to capital accumulation and the advance of human civilization. Money is the information and measurement system of an economy, and sound money is what allows trade, investment, and entrepreneurship to proceed on a solid basis, whereas unsound money throws these processes into disarray. Sound money is also an essential element of a free society as it provides for an effective bulwark against despotic government.

The third section of the book explains the operation of the Bitcoin network and its most salient economic characteristics, and analyzes the possible uses of Bitcoin as a form of sound money, discussing some use cases which Bitcoin does not serve well, as well as addressing some of the most common misunderstandings and misconceptions surrounding it. This book is written to help the reader understand the economics of Bitcoin and how it serves as the digital iteration of the many technologies used to fulfill the functions of money throughout history.

This book is not an advertisement or invitation to buy into the bitcoin currency. Far from it. The value of bitcoin is likely to remain volatile, at least for a while; the Bitcoin network may yet succeed or fail, for whatever foreseeable or unforeseeable reasons; and using it requires technical competence and carries risks that make it unsuited for many people. This book does not offer investment advice, but aims at helping elucidate the economic properties of the network and its operation, to allow readers an informed understanding before deciding whether they want to use it.

Only with such an understanding, and only after extensive and thorough research into the practical operational aspects of owning and storing bitcoins, should anyone consider holding value in Bitcoin. While bitcoin's rise in market value may make it appear like a no-brainer as an

investment, a closer look at the myriad hacks, attacks, scams, and security failures that have cost people their bitcoins provides a sobering warning to anyone who thinks that owning bitcoins provides a guaranteed profit. Should you come out of reading this book thinking that the bitcoin currency is something worth owning, your first investment should not be in buying bitcoins, but in time spent understanding how to buy, store, and own bitcoins securely. It is the inherent nature of Bitcoin that such knowledge cannot be delegated or outsourced. There is no alternative to personal responsibility for anyone interested in using this network, and that is the real investment that needs to be made to get into Bitcoin.