SATOSHI'S GIFT

The Past, Present and Future of Bitcoin

By Michael Hollomon Jr.

Contents

To Satoshi:

Thank you.

"The first requisite of a sound monetary system is that it shall not be subject to the whim of politicians."

—Ludwig von Mises

Preface

Something is wrong with your money. You know it, even if you can't quite put your finger on why. We constantly work harder, but our money buys less. We save, and still fall behind for some reason. The standard of living of our parents' generation feels hopelessly out of reach to ours. Most of us can sense that the system is rigged somehow, but the full picture is hidden behind complicated words, confusing charts, and empty promises.

This book is not about investing. It's not about getting rich quick. It's about something bigger—something deeper: the right of free people to work, save, build, and plan for the future without having their time and energy stolen from them through hidden inflation, systemic exploitation and the obscure wranglings of powerful governments and too-big-to-fail banks.

Bitcoin offers us a solution. It's not a perfect solution, perhaps. It's not an easy solution. But it's the first real solution we've seen in generations—a system of money built on truth, scarcity, and freedom, not government control, ever-expanding national debt, and layers of deceit. *Satoshi's Gift* is my attempt to explain where we've been, where we find ourselves today, and where we might go tomorrow—if we choose something better. You don't need to be an economist, a computer programmer, or a cypherpunk to understand this book. You just need to be curious about what's really going on and to want a future where your money, your work, and your time belong to you again. If that sounds like the kind of world you want to live in, then this book was written for you.

Let's begin.

Chapter 1

The Money Problem (What is Money?)

In this book, we will explore the history, nature and potential of Bitcoin. But Bitcoin is only one of many attempts by people to solve the money problem. So it makes sense to first briefly discuss the problem and our earlier attempts to solve it, to better see how those attempts compare with the Bitcoin solution.

Money is the tool we use to measure, store, and exchange value. Without it, people would have to rely on barter. Barter can work for small, close-knit groups trading subsistence-level goods, where we're more likely to find the necessary "coincidence of wants"—when two parties each have goods or services that the other party desires, making a direct exchange possible. The coincidence of wants can be a real challenge in barter because it's not always easy to find someone who wants exactly what you have and who also has something that you want. This is why barter often fails in larger, more complex trading networks where trust is limited, and trade extends beyond basic needs.

Also, without some common unit of measurement, it can be difficult to determine whether you're receiving fair value in exchange for your goods or services. How many cupcakes, for instance, is an iPhone worth? And even if Apple was interested in trading phones for baked goods, imagine the hassle of carting 200 cupcakes to your local Apple Store to exchange for the latest phone. These are some of the problems money was invented to solve. And to solve these problems, money needs to serve three basic functions. It needs to work as: (1) a store of value; (2) a unit of account; and (3) a medium of exchange.

What exactly is a "store of value?" Value, in simple terms, is a measure of the usefulness, or desirability of a thing. The more value something has, the more people will want it. If you have a valuable object, you could likely exchange it for something else you might want. And the more value your object has, the more things you'll probably be able to trade it for. Thus, for money to serve its purposes, people have to want it. In other words, it needs to be "valuable." If I don't value your money, I won't exchange my goods or services for it. In which case, your money is not good money.

So what makes money valuable? Subjective Value Theory (SVT) is a foundational concept in Austrian economics, which holds that the value of a good or service is not objective or inherent in the good itself, but instead is determined by the personal preferences, needs, and circumstances of the consumer. In other words, value only exists in the mind of each individual. The same object might have different values to different people, or even to the same person at different times. However, despite the fundamentally subjective nature of value, certain goods stand out as especially "salable" because they consistently meet key monetary properties (i.e., fungibility, durability, divisibility, portability, verifiability, and—critically—scarcity). And goods that satisfy these criteria tend to be widely accepted as valuable, even across different societies and time periods. In this sense, good money can exhibit a kind of universal utility.

Also, as often as not, we are motivated by the desires of other people. If everyone else really wants a thing, it will have value. And that alone is usually enough to influence us to want that thing too. This helps to explain the various crazes we have been through, from tulips to pet rocks, Beanie Babies and stock in internet companies like AOL and Yahoo. When a critical mass of people shows a strong enough desire for anything, that will very often increase the desire other people feel for that same thing. FOMO[1] is real. Things that are inherently useful (arrowheads, for example)

[1] Fear of missing out.

will have some value based on their utility. But even things with zero inherent utility (Beanie Babies, for instance) can be valuable simply for the reason that enough other people see value in them. And, of course, anything that holds enough value can be exchanged for other things of value. In other words, it can function as money. So if your money (regardless what it's made of) is desired by enough other people, it is *ipso facto* valuable; it can function as a "store of value" and is, therefore, a potential candidate for good money.

Money also needs to function as a unit of account. A "unit of account" simply refers to the use of money as a standard measurement of value. It allows people to compare the worth of different kinds of goods and services and provides a consistent way to express prices, making economic calculations and transactions easier to understand and conduct.

For example, if I'm a shoemaker who needs some arrowheads, and you're an arrowhead-maker in need of shoes, we can be said to have coincidental wants and can probably do business together. However, without a common unit of account, how would we determine the number of arrowheads that a pair of shoes is worth? We might have to resort to some degree of guesswork, posturing, haggling or disagreement before finally coming to terms, or walking away in frustration from the deal. But if we both do business using the same kind of money, and I've been selling my shoes for, say, 5 cowrie shells per pair, and the going rate for arrowheads in our community is known to be 1 cowrie shell a piece. It's a simple matter to determine that 5 of your arrowheads are probably a fair trade for my pair of shoes. In other words, when things can be measured in a common unit of account (whether U.S. dollars, gold coins or cowrie shells), it becomes much easier to determine the fair price of exchange for pretty much any goods and services. This is one of the functions that money serves.

Lastly, money serves as a "medium of exchange." This means that when I need to do business in a distant locale, rather than carrying my entire inventory of shoes with me to trade, I can instead travel with a pocketful of money (U.S. dollars, gold coins, cowrie shells, or whatever), and use this money, rather than the immediate products of my labor, to trade with. The advantages of traveling with—and trading in—a portable form of money as opposed to an inventory of shoes should be pretty obvious. This is another function that money serves.

Sound Money vs. Unsound Money

Sound money is a term used to describe money that maintains its value, is stable, and cannot be easily manipulated. Sound money tends to retain its purchasing power (i.e., value) over time, and therefore it protects savers from things like devaluation, debasement and monetary inflation. It is often contrasted with unsound "fiat money," which is issued by governments and can easily be inflated or debased. In this book, I will use the terms "sound money" and "good money" interchangeably. In my view, they are one and the same thing. While the terms "unsound money" and "fiat money" are not exactly the same thing, I think they are analogous enough to also be used interchangeably. But I won't be offended if some linguistic or economic sticklers take issue with that.

Now that we have a basic understanding of what money is and the functions it serves, let's consider the properties that money should have in order to be considered sound. Sound money should be fungible, durable, divisible, portable, verifiable and scarce. I'll discuss each of these monetary characteristics below.