1

Introduction

WE HAVE SEEN many amazing technological revolutions throughout human history. The Guttenberg press helped bring books to the masses. The telegraph has enabled crude but rapid communication across great distances. More recently, personal computers have vastly increased human productivity, leading to the creation of the Internet, digital communications, and the advent of citizen journalism as photos of major events are almost instantly uploaded to Twitter and other social networks via smartphone, which are small computers in their own right. Until fairly recently, however, the monetary system has remained somewhat untouched by a major breakthrough.

Bitcoin is run by software whose blueprint (source code) is freely available for anyone to see and even adapt for his or her own use. It currently runs on multiple computers connected over the Internet via a common networking protocol defined by this same software.

Existing within this software and existing because of it is a digital currency known as *bitcoin*, spelled with a lower case b and abbreviated BTC.

Bitcoin, both a virtual currency and a payment system, represents a revolutionary concept whose significance quickly becomes apparent with a first transaction. A buyer making a purchase in BTCs has only to provide the merchant with personal information relevant to the purchase, for example, the shipping or email address, to pay. Compare this with a credit card purchase, which necessitates the buyer giving enough personal information to enable another party bent on fraud, a hacker or dishonest employee, to make fraudulent purchases with it.

Bitcoin's significance is not limited to the simplicity of the payment system, however. The supply of Bitcoin currency is defined by the software and its underlying protocol. Only 21 million bitcoins will ever come into existence, with about 12 million so far having been created. The last bitcoin is expected to be created around the year 2140. This very specific, limited money supply has led to many controversies, some of which have more to do with lack of understanding of the protocol or the economics than with the software itself. Although 21 million BTC might seem insufficient with a global population of 7 billion people, the bitcoin currency is highly divisible. The smallest denomination allowed by the current software is 0.00000001 BTC (10^{-8} BTC), which has been defined as 1 *satoshi* and was named after the software's putative creator, Satoshi Nakamoto. There are therefore 100 million satoshis in a single bitcoin, and thus the maximum supply of 21 million BTC will be equal to 2.1 quadrillion satoshis or, if you prefer, 2,100 trillion satoshis.

Bitcoin was created by an anonymous person (or group of persons) known as Satoshi Nakamoto. At the time Nakamoto made his first public post announcing his paper on Bitcoin, he was just another anonymous user like millions of others posting on Internet forums. His new software was then still in the early phase of development, and

Bitcoin was only an experiment in its early stages. Satoshi's interaction was limited to email exchanges only and for a brief duration of a little over 2 years. Since then, we haven't heard from him. Around the time of his last post, Bitcoin's value was soaring, and the media were starting to take notice. Just when Bitcoin appeared poised to take off and was beginning to attract serious interest, Satoshi Nakamoto retreated from the public eye.

A few years later, Satoshi has become something of an iconic figure, and his retreat has only served to amplify the mystery surrounding him. His identity is irrelevant to the well-being of Bitcoin, as the code is open source and is, in fact, being constantly upgraded and improved upon even as we speak. However, gaining an understanding of the mindset of the mysterious person (or group of persons) behind this marvelous new technology would certainly prove interesting.

Satoshi's two-year "public life" overlapping Bitcoin's development and launch began with the publication of his paper "Bitcoin: A Peer-to-Peer Electronic Cash System", which he announced on November 1st, 2008, on the Cryptography Mailing List. At that time, this paper could be downloaded at domain name *bitcoin.org,* which had been registered a few months earlier on August 18th, 2008, through *anonymousspeech.com*. On November 9th, 2008, the Bitcoin project was registered on *SourceForge.net* and, at the beginning of 2009, the genesis block was created. To understand the genesis block, imagine a bookkeeping ledger that adds new pages (blocks) daily and contains a record of all bitcoin transactions ever made. The very first page of this book is called the genesis block, which will be explained in more detail in the following chapter. Satoshi incorporated this interesting quote into the genesis block in reference to the bank bailouts occurring at the time:

The Times 03/Jan/2009
Chancellor on brink of second bailout for banks

Bank bailouts were and still are extremely unwelcome occurrences, particular to libertarians, who caricaturized our political and economic environment with this quote: "Privatize the gains and socialize the losses".

Six days later, on January 9th, 2009, Nakamoto published the source code of Bitcoin version 0.01 on *SourceForge.net*. As of this writing (March 2014), Bitcoin v. 0.8.6 is the latest version.

Satoshi's last post was published on the *bitcointalk.org* forum on December 12th, 2010. His last known communication is a private email sent a few months later to Gavin Andresen, current Lead Core Developer of the Bitcoin project.

Below is a chart of the public trade data from *bitcoinmarket.com*, the first Bitcoin exchange, which is no longer in business. As can be seen, the value of one bitcoin went from 10 cents to a dollar in a very short time. At the time of Satoshi's last post on the forum, it was trading around 25 cents and was approaching 30 cents per bitcoin.

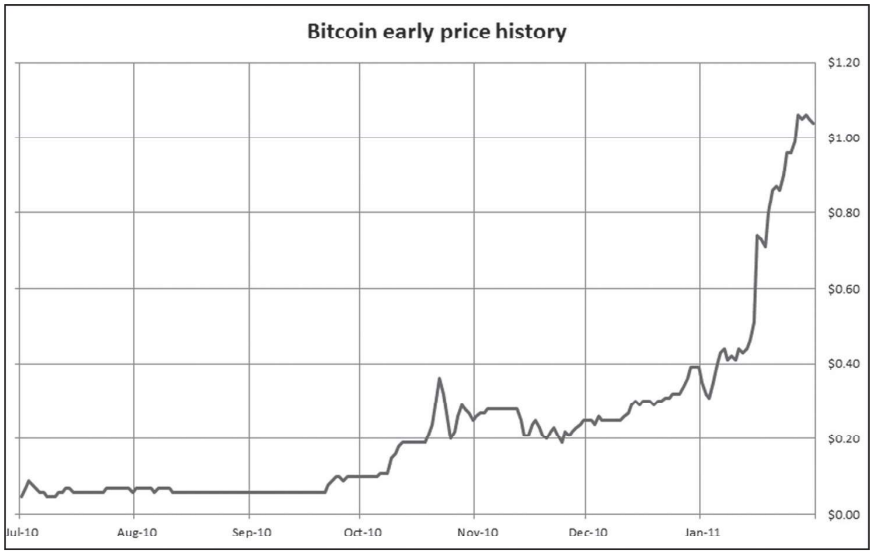

FIGURE 1 - EARLY CHART OF BITCOIN PRICED IN USD

This book is a collection of the postings and writings published under Satoshi's name on various forums and included in email exchanges. I have chosen to exclude posts of a technical nature, such as those related to coding, software compilation, and the detailed technical operation of the Bitcoin software. You will notice a few interesting subjects are discussed; one in particular involves the Byzantine Generals Problem, heretofore considered unsolvable, which describes the challenge of communicating in an unreliable environment. Some of Satoshi's comments relate to the news coverage that developed as Bitcoin started to attract media attention. One such event was when PayPal stopped processing payments for WikiLeaks, a journalistic non-profit organization dedicated to publishing selected secret and classified information provided by anonymous sources. A subsequent article published in *PC World* magazine conjectured how WikiLeaks could benefit from Bitcoin.

Satoshi's post seems to indicate that he was not comfortable with Bitcoin getting this kind of attention and was not ready for such a relationship, at least not yet:

> It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us.

How much this event influenced his decision to "retire" from Bitcoin's development is unknown, but the timing is interesting, to say the least. Significantly, this post was written just nineteen hours before his last post on the forum, the announcement of the release of Bitcoin version 0.3.19.

Many journalists and researchers have tried to identify who could be the person behind Satoshi Nakamoto. So far, at least three attempts at identifying him have been made. Typical choices have been known scientists in the field of cryptography, none of whose real names are

Satoshi Nakamoto. All have been proven false, and all denied being Satoshi Nakamoto as well. However, very recently, a newspaper claimed to have identified a Californian, an engineer with actual name Dorian Satoshi Nakamoto, as the Bitcoin Satoshi Nakamoto. Dorian Nakamoto has denied this, and I tend to believe him. For one thing, Dorian Nakamoto does not demonstrate the proficiency in English that the Bitcoin Satoshi Nakamoto has shown through his writing. What is most relevant to this book concerning this episode is that it apparently caused Bitcoin's Satoshi Nakamoto to break his silence and post this message on the *p2pfoundation* forum on Friday March 7th, 2014:

I am not Dorian Nakamoto.

As you will see in the book, Satoshi's replies addressed many of the most commonly asked questions and criticisms regarding Bitcoin and are still pertinent. I suspect that, were he still involved in Bitcoin's development and were he to be interviewed, the writings contained in this book would reflect the type of answers Satoshi would give.

Whatever eventually happens to Bitcoin itself, that the software has opened the mind of the world to a new concept is indisputable. As an open source code, it allowed a myriad of other distributed digital currencies to enter the scene. While most of them do not represent any significant innovations—only varying the number of coins, the transaction confirmation speed (in Bitcoin termed *block creation*), or the computer encryption algorithm—a few new ones which incorporate significant new features or new concepts are being developed. One such is "Truthcoin", described as a trustless, decentralized, censorship-proof, incentive-compatible, scalable bitcoin prediction marketplace. Ethereum (see *ethereum.org*) is another digital currency that, according to its creator, will allow users to encode advanced transaction types, smart contracts, and decentralized applications into the block chain (Bitcoin's large public ledger which grows in size daily).

Innovative thinkers are seeking to use some of the concepts introduced by Bitcoin in a truly open voting system, where voters can confirm that their votes have been properly counted and can, at any time, view a complete vote count, thus ensuring transparency. Bitcoin has therefore clearly sparked a new technological revolution that capitalizes on the Internet, another innovation that changed the world.

I am quite open to suggestions and corrections with respect to this book and its contents. Also, if you have private email exchanges with Satoshi that you feel can be made public, I will be glad to consider them for inclusion. Please feel free to contact me at BookOfSatoshi@gmail.com.