Introduction

May I consider the wise man rich, and may my pile of gold be of a size that a moderate man could bear and carry with him.

Socrates, *Phaedrus*

On the morning of February 7, 2014, the world woke up to discover that history's greatest bank robbery had taken place while it was sleeping. But the target was not Fort Knox or Goldman Sachs. The robbers did not use guns or sticks of dynamite. And the stolen assets were not gold ingots or dollar bills.

Instead, the target was an obscure company called Mt. Gox – an acronym for Magic: The Gathering Online Exchange – operating out of a small office in Tokyo. The robbers used sophisticated hacking tools to exploit a flaw in the company's software. And the stolen assets were a recently created virtual currency called bitcoin.

Bitcoin was the brainchild of a man named Satoshi Nakamoto, a shadowy figure active in cryptography circles on the internet who has yet to be identified in real life. Nakamoto viewed his creation as a kind of anti-money, a "peer-to-peer" virtual currency that would exist only on computers and would zip around the world at the speed of light. At the heart of the currency was a set of features that made it uniquely and, to some, radically democratic. Bitcoins, unlike dollars or euros, would be created and controlled by everyone. Anyone with a computer would have access to the network and could start creating new currency. People could send and receive the virtual money over the internet without ever going to a bank. Users would operate the network by consensus. Importantly, all of this would take place anonymously; the only identifying information in the system would be long strings of numbers and letters that could not be traced back to real-world individuals. For those who feared the growing power of the state and the corporation in modern society, bitcoin was the perfect antidote. It provided a way for regular people to take back control of their financial lives.

But an undertaking with the radical aspirations of bitcoin, operating on the fringes of the internet (and the law) as bitcoin did, was bound to run into

trouble at some point. It was not a question of whether. It was a question of when.

It was 2011 when Mark Karpeles became the chief executive officer of Mt. Gox. He had acquired the company from its founder, a man named Jed McCaleb who originally created the site as a way to trade Magic: The Gathering cards over the internet. Eventually, McCaleb gave up on a future in Magic and transformed the site into a bitcoin exchange. Soon after, Karpeles came calling.

Karpeles, like many of the early adopters of bitcoin, was an unlikely CEO. He was a baby-faced, twenty-six-year-old Frenchman who had a penchant for wearing graphic t-shirts and went by the name of Magical Tux. He had previously worked for a small online gaming company in Paris but was fired after being accused of stealing customer usernames and passwords. His great passion was baking – apple pie was his favorite – and he was always on the lookout for the best croissants in Tokyo, where he had relocated after acquiring Mt. Gox.[1]

Despite his apparent lack of qualifications, Karpeles oversaw a rapid expansion of Mt. Gox's business. By 2012, the company was the world's largest bitcoin exchange. At its height, it handled 80 percent of global transactions in the currency. If you owned bitcoin in 2014, you almost certainly dealt with Mt. Gox.[2]

But Karpeles struggled under the burdens of running his new corporate empire. It didn't help that he was hopelessly devoted to his cat, Tibanne, which, he claimed, required daily shots of medicine, a fact that prevented him from traveling outside the country. And as bitcoin started to gain wider notice in the investment community, and the value of bitcoin spiked, Mt. Gox became an obvious target for hackers looking for vulnerabilities in the cryptocurrency.[3]

By 2014, Karpeles was responding to "daily hacking attempts." At one point, a hacker briefly took control of the site and caused the value of bitcoin to plummet below one cent. It took Karpeles weeks to fix the problem. In another incident, Karpeles reassured users that delays they were experiencing on the site were due to overwhelming demand, not hackers. Hackers, apparently taking Karpeles' statement as a challenge, immediately launched a cyberattack on the site and forced it to shut down entirely. Eventually, Karpeles had to bring in outside help to strengthen Mt. Gox's cybersecurity systems.[4]

In January 2014, however, users of Mt. Gox again began to experience delays on the site. The delays were sporadic – some transactions went through without a glitch – but frequent. Complaints started to mount. Some investors reported that they paid for bitcoins but never received them. For an exchange, this was a definite problem. Mt. Gox marketed itself as a platform that made

the process of buying and selling virtual currencies easy. If it could not deliver on that promise, its service was useless. Panicked messages to Mt. Gox's customer service account went unanswered. Bitcoin message boards lit up with angry investors asking what was happening.

"Where are my Bitcoins MTGOX?"[5]

"WTF GOX!"[6]

"Get your popcorn ready as the fireworks show is just beginning . . . ."[7]

"MtGox always finds a way to continue f**king everyone into oblivion, indefinitely."[8]

Karpeles, who had lately been spending much of his time designing a "Bitcoin Café" that would sell bitcoins and pastries to Tokyo patrons, finally decided to look into the complaints. Doing so was harder than it might sound. This was because Karpeles had instituted a security mechanism known as "cold storage" for keeping client accounts safe. Instead of keeping users' private keys – essentially passwords that allowed bitcoin owners to buy and sell their coins – on his company's computers, Karpeles had stored them on paper slips stashed all around Tokyo. Cold storage was thought to protect client assets from theft because hackers could not access the passwords even if they managed to break into the company's systems. Instead, they would need to physically access the paper slips. But, ironically, the very system that was designed to prevent theft now made it very hard to determine whether a theft had actually occurred. In order to find out what was wrong, Karpeles had to race around the city manually retrieving the slips of paper and then scanning them into his computer.[9]

It is remarkable that Karpeles had not thought to do this before. After all, it would have been natural for users to assume that the world's largest bitcoin exchange would perform regular audits of its accounts. If it had handled physical currency, as a normal bank does, it would have been obligated to do so by numerous laws and regulations. But bitcoin operated in a legal netherworld, where it was unclear which rules, if any, applied to it. Plus, Karpeles had another reason for not checking his clients' accounts. As he explained it, "each time you want to check the balance of a cold wallet, you're making it less cold." In other words, by storing his clients' private keys offline, he protected them from cybertheft. But every time he typed those keys into his computer to check their accounts, the chances that a hacker might be able to discover the keys increased. In other words, in order for Mt. Gox's security system to work, it was paramount that no one check that it was working.[10]

When Karpeles finally decided to check, he was in for a surprise. Wallet after wallet came back empty. Hundreds of thousands of bitcoins that were supposed to be in his accounts were gone. And despite furious efforts to locate

the missing coins, he could not track them down. They had disappeared into thin air.

Karpeles had no choice. He swiftly halted all withdrawals from the Mt. Gox exchange. He took his website offline. He filed for bankruptcy. The world's largest bitcoin exchange had just gone under.

Karpeles would eventually announce the full extent of his losses: a staggering 850,000 bitcoins had disappeared from Mt. Gox's accounts.[11] At bitcoin's height, these coins would have been worth $17 billion.[12]

***

Blockchain Democracy tells the story of the blockchain. This remarkable new technology stormed onto the stage in the last decade and quickly captured the public's imagination, as well as much of its money. Strange forms of virtual currency, entirely divorced from traditional monetary systems such as the American dollar or the Japanese yen, seemingly appeared out of nowhere to challenge existing hierarchies and power structures. Some see them as a powerful tool for good, a way of protecting individual freedom and privacy. Others see them as the greatest scam ever perpetrated, a Ponzi scheme that is doomed to collapse under its own weight. This book aims to help sort out these claims.

As such, *Blockchain Democracy* is a story about technology. Where it comes from. How it is created. And what happens when it meets the messy facts of the real world. Each Chapter of the book explores a different facet of the blockchain technology, from the underlying code and the miners that implement it to the businesses and governments that seek to control it. It is hoped that these bite-sized views of the blockchain, when put together, provide a comprehensive view into the role of this important technology in society today.

Blockchain Democracy is also a story about money. Proponents of the blockchain, after all, hoped to ignite a revolution in the way that money worked in the world. Despite the fact that people spend a great deal of time thinking about dollars and cents, it is surprisingly difficult to define precisely what money is and what purpose it serves in society. Until we know these things, it is hard to assess how we can improve on it. It turns out that the founders of bitcoin and other cryptocurrencies thought deeply about these questions and had well-worked-out answers. It is hoped that by studying money and its role in the economy, we can get a better handle on what cryptocurrencies are. But it is also hoped that by studying cryptocurrencies, we can begin to sort out our ideas about what money is and how we might change it.

Finally, *Blockchain Democracy* is a story about democracy. How it works. How it doesn't. And whether it can withstand the powerful forces unleashed by

those other great mechanisms: money and technology. The blockchain was founded on the idea of wresting control of our lives back from the government. Giving power to the people sounds a lot like democracy. But it is not necessarily so. Modern democracies have struggled for centuries to find a proper balance between popular sovereignty and individual rights, between freedom and equality, between government regulation and self-determination. The blockchain has been around for only a decade and, in many ways, rejects many of the precepts of modern democracy. Can a democratic system of government coexist with a technology of the likes of the blockchain? Can governments harness the power of decentralized networks without losing control over those they govern? These are the questions that this book seeks to answer.

At the root of all of these grand themes lies a central question: Where should power reside in modern society? Should it be centralized and concentrated? Or should it be decentralized and dispersed? The blockchain was founded on the concept of decentralization; it was purposely designed so that everyone could have a say in its future. For its founders and original programmers, decentralized networks offered a set of benefits to the community that no other form of organization could offer. They were secure and stable and democratic. But decentralized networks also have a set of costs that are hard-wired into them and that are difficult to avoid. And, just as importantly, the invisible hand of the market may lead to centralization even when the system itself begins in a decentralized state. The internet, after all, bred Facebook, Google and Amazon. People like one-stop shops, coherent ecosystems and easy-to-use interfaces. Companies like monopolies. All of which suggests that market forces may end up pushing even the most decentralized and democratic technologies in a centralized, antidemocratic direction.

Technology. Money. Democracy. These ideas are the great challenges facing our world today. They permeate our lives in ways that are hard to overstate, but they are also the source of much anxiety and controversy. Tech companies like Apple, Google and Facebook have come under criticism for their addictive effects and their hoarding of private data. Soaring levels of debt, from mortgages to student loans, have been blamed for a variety of ills, and the gap between the rich and the poor grows wider every day. Democracy itself is under attack by nationalists and populists around the globe. It is hard not to think that somehow these troubling trends are linked.

At the same time, technology, money and democracy seem more important than they have ever been. We need democracy to define our common values and our common goals. We need technology to pursue those values and to

reach those goals. And we need money to make this all possible. Resolving society's ills requires us to confront these great challenges.

The blockchain lies squarely at the intersection of these great leitmotifs of modern society. It has led to advances in technology by pioneering new uses of encryption and peer-to-peer networks. It has harnessed these tools to create new forms of money. And it uses lessons from democracy to inform its decision-making processes. In many ways, its achievements warrant celebration. They have shown how decentralized networks can be used to replace a wide variety of outdated systems, from financial recordkeeping to the tracking of election results. They have also shone a light on the many flaws of our current monetary system. The founders of bitcoin and other cryptocurrencies saw the contradictions and failings of the modern economy and decided to fashion a new one, using technology to refine and improve on old models. What they created was revolutionary and new. It challenged powerful incumbents. And it broke all the rules.

But if the blockchain has ushered in a revolution in finance and politics, it has also created opportunities for the unprincipled and the immoral to flourish. Criminals and terrorists have rushed into the industry, and their actions have threatened to undermine the accomplishments, and indeed the continued existence, of cryptocurrencies. Governments have watched these developments with a wary eye and, in some cases, have gone further, stepping in to limit or even ban the currencies. The life of the blockchain, thus, in many ways resembles Plato's description of life in a democracy: "It will be an agreeable kind of regime – anarchic, colourful, and granting equality of a sort to equals and unequals alike."[13]

***

The story of Mt. Gox is meant to be a cautionary tale. It highlights the challenges of democratizing technologies, particularly in an area as fundamental to our economy as money is. Mistakes will be made. Unintended consequences are to be expected. Technology magnifies these consequences by making them instantaneous and infinitely repeatable.

But the failure of Mt. Gox also shows something else. It shows that millions of people were willing to put their trust in an algorithm. That this algorithm had become the repository for billions of dollars of real-world money. And that, somehow, through this algorithm, people across the globe were able to communicate and make decisions as if they were a single community.

This book will tell the story of what made that possible.