O'REILLY®

Blockchain

BLUEPRINT FOR A NEW ECONOMY

Melanie Swan

O'REILLY®

Blockchain

Bitcoin is starting to come into its own as a digital currency, but the blockchain technology behind it could prove to be much more significant. This book takes you beyond the currency ("Blockchain 1.0") and smart contracts ("Blockchain 2.0") to demonstrate how the blockchain is in position to become the fifth disruptive computing paradigm after mainframes, PCs, the Internet, and mobile/social networking.

Author Melanie Swan, Founder of the Institute for Blockchain Studies, explains that the blockchain is essentially a public ledger with potential as a worldwide, decentralized record for the registration, inventory, and transfer of all assets—not just finances, but property and intangible assets such as votes, software, health data, and ideas.

Topics include:

- Concepts, features, and functionality of Bitcoin and the blockchain
- Using the blockchain for automated tracking of all digital endeavors
- Enabling censorship-resistant organizational models
- Creating a decentralized digital repository to verify identity
- Possibility of cheaper, more efficient services traditionally provided by nations
- Blockchain for science: making better use of the data-mining network
- Personal health record storage, including access to one's own genomic data
- Open access academic publishing on the blockchain

This book is part of an ongoing O'Reilly series. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* introduces Bitcoin and describes the technology behind Bitcoin and the blockchain. *Blockchain: Blueprint for a New Economy* considers the theoretical, philosophical, and societal impact of cryptocurrencies and blockchain technologies.

Melanie Swan founded and participated in new markets startups GroupPurchase and Prosper, and developed virtual world digital asset valuation and accounting principles for Deloitte. She is an instructor at Singularity University and an Affiliate Scholar at the Institute for Ethics and Emerging Technologies.

E-COMMERCE

US $34.99 CAN $46.99

ISBN: 978-1-491-92049-7

Twitter: @oreillymedia
facebook.com/oreilly

Blockchain

Blueprint for a New Economy

Melanie Swan

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo O'REILLY®

Blockchain
by Melanie Swan

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editor: Tim McGovern
Production Editor: Matthew Hacker
Copyeditor: Rachel Monaghan
Proofreader: Bob Russell, Octal Publishing, Inc.
Indexer: Wendy Catalano
Interior Designer: David Futato
Cover Designer: Ellie Volckhausen
Illustrator: Rebecca Demarest

February 2015: First Edition

Revision History for the First Edition
2015-01-22: First Release

See *http://oreilly.com/catalog/errata.csp?isbn=9781491920497* for release details.

978-1-491-92049-7

[LSI]

Table of Contents

Preface

We should think about the blockchain as another class of thing like the Internet—a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property, homes, cars); and intangible assets (votes, ideas, reputation, intention, health data, information, etc.). But the blockchain concept is even more; it is a new organizing paradigm for the discovery, valuation, and transfer of all quanta (discrete units) of anything, and potentially for the coordination of all human activity at a much larger scale than has been possible before.

We may be at the dawn of a new revolution. This revolution started with a new fringe economy on the Internet, an alternative currency called Bitcoin that was issued and backed not by a central authority, but by automated consensus among networked users. Its true uniqueness, however, lay in the fact that it did not require the users to trust each other. Through algorithmic self-policing, any malicious attempt to defraud the system would be rejected. In a precise and technical definition, Bitcoin is digital cash that is transacted via the Internet in a decentralized trustless system using a public ledger called the *blockchain*. It is a new form of money that combines BitTorrent peer-to-peer file sharing[1] with public key cryptography.[2] Since its launch in 2009, Bitcoin has spawned a group of imitators—alternative currencies using the same general approach but with different optimizations and tweaks. More important, blockchain technology could become the seamless embedded economic layer the Web has never had, serving as the technological underlay for payments, decentralized exchange, token earning and spending, digital asset invocation and transfer, and smart contract issuance and execution. Bitcoin and blockchain technology, as a mode of decentralization, could be the next major disruptive technology and worldwide computing paradigm (following the mainframe, PC, Internet, and social networking/mobile phones), with the potential for reconfiguring all human activity as pervasively as did the Web.

Currency, Contracts, and Applications beyond Financial Markets

The potential benefits of the blockchain are more than just economic—they extend into political, humanitarian, social, and scientific domains—and the technological capacity of the blockchain is already being harnessed by specific groups to address real-world problems. For example, to counter repressive political regimes, blockchain technology can be used to enact in a decentralized cloud functions that previously needed administration by jurisdictionally bound organizations. This is obviously useful for organizations like WikiLeaks (where national governments prevented credit card processors from accepting donations in the sensitive Edward Snowden situation) as well as organizations that are transnational in scope and neutral in political outlook, like Internet standards group ICANN and DNS services. Beyond these situations in which a public interest must transcend governmental power structures, other industry sectors and classes can be freed from skewed regulatory and licensing schemes subject to the hierarchical power structures and influence of strongly backed special interest groups on governments, enabling new disintermediated business models. Even though regulation spurred by the institutional lobby has effectively crippled consumer genome services,[3] newer sharing economy models like Airbnb and Uber have been standing up strongly in legal attacks from incumbents.[4]

In addition to economic and political benefits, the coordination, record keeping, and irrevocability of transactions using blockchain technology are features that could be as fundamental for forward progress in society as the Magna Carta or the Rosetta Stone. In this case, the blockchain can serve as the public records repository for whole societies, including the registry of all documents, events, identities, and assets. In this system, all property could become *smart property*; this is the notion of encoding every asset to the blockchain with a unique identifier such that the asset can be tracked, controlled, and exchanged (bought or sold) on the blockchain. This means that all manner of tangible assets (houses, cars) and digital assets could be registered and transacted on the blockchain.

As an example (we'll see more over the course of this book), we can see the world-changing potential of the blockchain in its use for registering and protecting intellectual property (IP). The emerging digital art industry offers services for privately registering the exact contents of any digital asset (any file, image, health record, software, etc.) to the blockchain. The blockchain could replace or supplement all existing IP management systems. How it works is that a standard algorithm is run over a file (any file) to compress it into a short 64-character code (called a *hash*) that is unique to that document.[5] No matter how large the file (e.g., a 9-GB genome file), it is compressed into a 64-character secure hash that cannot be computed backward. The hash is then included in a blockchain transaction, which adds the timestamp—the proof of that digital asset existing at that moment. The hash can be recalculated from the

underlying file (stored privately on the owner's computer, not on the blockchain), confirming that the original contents have not changed. Standardized mechanisms such as contract law have been revolutionary steps forward for society, and blockchain IP (digital art) could be exactly one of these inflection points for the smoother coordination of large-scale societies, as more and more economic activity is driven by the creation of ideas.

Blockchain 1.0, 2.0, and 3.0

The economic, political, humanitarian, and legal system benefits of Bitcoin and blockchain technology start to make it clear that this is potentially an extremely disruptive technology that could have the capacity for reconfiguring all aspects of society and its operations. For organization and convenience, the different kinds of existing and potential activities in the blockchain revolution are broken down into three categories: Blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 is *currency*, the deployment of cryptocurrencies in applications related to cash, such as currency transfer, remittance, and digital payment systems. Blockchain 2.0 is *contracts*, the entire slate of economic, market, and financial applications using the blockchain that are more extensive than simple cash transactions: stocks, bonds, futures, loans, mortgages, titles, smart property, and smart contracts. Blockchain 3.0 is blockchain *applications* beyond currency, finance, and markets—particularly in the areas of government, health, science, literacy, culture, and art.

What Is Bitcoin?

Bitcoin is digital cash. It is a digital currency and online payment system in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. The terminology can be confusing because the words *Bitcoin* and *blockchain* may be used to refer to any three parts of the concept: the underlying blockchain *technology*, the *protocol* and *client* through which transactions are effected, and the actual *cryptocurrency* (money); or also more broadly to refer to the whole concept of cryptocurrencies. It is as if PayPal had called the Internet "PayPal," upon which the PayPal protocol was run, to transfer the PayPal currency. The blockchain industry is using these terms interchangeably sometimes because it is still in the process of shaping itself into what could likely become established layers in a technology stack.

Bitcoin was created in 2009 (released on January 9, 2009[6]) by an unknown person or entity using the name Satoshi Nakamoto. The concept and operational details are described in a concise and readable white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System."[7] Payments using the decentralized virtual currency are recorded in a public ledger that is stored on many—potentially all—Bitcoin users' computers, and continuously viewable on the Internet. Bitcoin is the first and largest decentralized

cryptocurrency. There are hundreds of other "altcoin" (alternative coin) cryptocurrencies, like Litecoin and Dogecoin, but Bitcoin comprises 90 percent of the market capitalization of all cryptocurrencies and is the de facto standard. Bitcoin is pseudonymous (not anonymous) in the sense that public key addresses (27–32 alphanumeric character strings; similar in function to an email address) are used to send and receive Bitcoins and record transactions, as opposed to personally identifying information.

Bitcoins are created as a reward for computational processing work, known as *mining*, in which users offer their computing power to verify and record payments into the public ledger. Individuals or companies engage in mining in exchange for transaction fees and newly created Bitcoins. Besides mining, Bitcoins can, like any currency, be obtained in exchange for fiat money, products, and services. Users can send and receive Bitcoins electronically for an optional transaction fee using *wallet software* on a personal computer, mobile device, or web application.

What Is the Blockchain?

The blockchain is the public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as miners add new blocks to it (every 10 minutes) to record the most recent transactions. The blocks are added to the blockchain in a linear, chronological order. Each full node (i.e., every computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) has a copy of the blockchain, which is downloaded automatically when the miner joins the Bitcoin network. The blockchain has complete information about addresses and balances from the genesis block (the very first transactions ever executed) to the most recently completed block. The blockchain as a public ledger means that it is easy to query any block explorer (such as *https://blockchain.info/*) for transactions associated with a particular Bitcoin address—for example, you can look up your own wallet address to see the transaction in which you received your first Bitcoin.

The blockchain is seen as the main technological innovation of Bitcoin because it stands as a "trustless" proof mechanism of all the transactions on the network. Users can trust the system of the public ledger stored worldwide on many different decentralized nodes maintained by "miner-accountants," as opposed to having to establish and maintain trust with the transaction counterparty (another person) or a third-party intermediary (like a bank). The blockchain as the architecture for a new system of *decentralized trustless transactions* is the key innovation. The blockchain allows the disintermediation and decentralization of all transactions of any type between all parties on a global basis.

The blockchain is like another application layer to run on the existing stack of Internet protocols, adding an entire new tier to the Internet to enable economic transactions, both immediate digital currency payments (in a universally usable

cryptocurrency) and longer-term, more complicated financial contracts. Any currency, financial contract, or hard or soft asset may be transacted with a system like a blockchain. Further, the blockchain may be used not just for transactions, but also as a registry and inventory system for the recording, tracking, monitoring, and transacting of all assets. A blockchain is quite literally like a giant spreadsheet for registering all assets, and an accounting system for transacting them on a global scale that can include all forms of assets held by all parties worldwide. Thus, the blockchain can be used for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property); and intangible assets (votes, ideas, reputation, intention, health data, etc.).

The Connected World and Blockchain: The Fifth Disruptive Computing Paradigm

One model of understanding the modern world is through computing paradigms, with a new paradigm arising on the order of one per decade (Figure P-1). First, there were the mainframe and PC (personal computer) paradigms, and then the Internet revolutionized everything. Mobile and social networking was the most recent paradigm. The current emerging paradigm for this decade could be the *connected world of computing* relying on blockchain cryptography. The connected world could usefully include blockchain technology as the economic overlay to what is increasingly becoming a seamlessly connected world of multidevice computing that includes wearable computing, Internet-of-Things (IoT) sensors, smartphones, tablets, laptops, quantified self-tracking devices (i.e., Fitbit), smart home, smart car, and smart city. The economy that the blockchain enables is not merely the movement of money, however; it is the transfer of information and the effective allocation of resources that money has enabled in the human- and corporate-scale economy.

With revolutionary potential equal to that of the Internet, blockchain technology could be deployed and adopted much more quickly than the Internet was, given the network effects of current widespread global Internet and cellular connectivity.

Just as the social-mobile functionality of Paradigm 4 has become an expected feature of technology properties, with mobile apps for everything and sociality as a website property (liking, commenting, friending, forum participation), so too could the blockchain of Paradigm 5 bring the pervasive expectation of value exchange functionality. Paradigm 5 functionality could be the experience of a continuously connected, seamless, physical-world, multidevice computing layer, with a blockchain technology overlay for payments—not just basic payments, but micropayments, decentralized exchange, token earning and spending, digital asset invocation and transfer, and smart contract issuance and execution—as the economic layer the Web never had. The world is already being prepared for more pervasive Internet-based money: Apple Pay (Apple's token-based ewallet mobile app) and its competitors could

be a critical intermediary step in moving to a full-fledged cryptocurrency world in which the blockchain becomes the seamless economic layer of the Web.

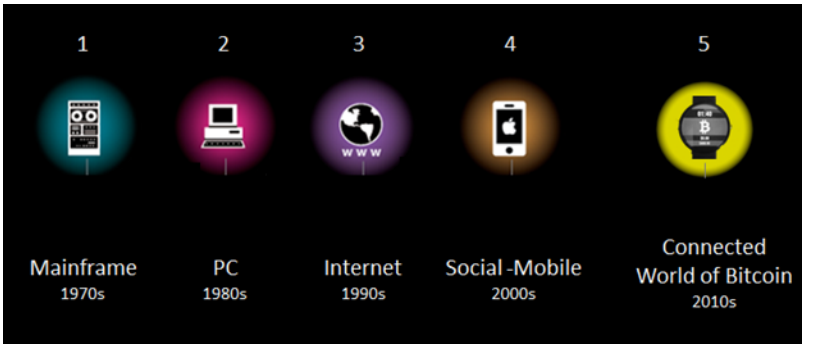

Figure P-1. Disruptive computing paradigms: Mainframe, PC, Internet, Social-Mobile, Blockchain[8]

M2M/IoT Bitcoin Payment Network to Enable the Machine Economy

Blockchain is a revolutionary paradigm for the human world, the "Internet of Individuals," and it could also be the enabling currency of the machine economy. Gartner estimates the Internet of Things will comprise 26 billion devices and a $1.9 trillion economy by 2020.[9] A corresponding "Internet of Money" cryptocurrency is needed to manage the transactions between these devices,[10] and micropayments between connected devices could develop into a new layer of the economy.[11] Cisco estimates that M2M (machine-to-machine) connections are growing faster than any other category (84 percent), and that not only is global IP traffic forecast to grow threefold from 2012 to 2018, but the composition is shifting in favor of mobile, WiFi, and M2M traffic.[12] Just as a money economy allows for better, faster, and more efficient allocation of resources on a human scale, a machine economy can provide a robust and decentralized system of handling these same issues on a machine scale.

Some examples of interdevice micropayments could be connected automobiles automatically negotiating higher-speed highway passage if they are in a hurry, microcompensating road peers on a more relaxed schedule. Coordinating personal air delivery drones is another potential use case for device-to-device micropayment networks where individual priorities can be balanced. Agricultural sensors are an example of another type of system that can use economic principles to filter out routine irrelevant data but escalate priority data when environmental threshold conditions (e.g., for humidity) have been met by a large enough group of sensors in a deployed swarm.

Blockchain technology's decentralized model of trustless peer-to-peer transactions means, at its most basic level, intermediary-free transactions. However, the potential shift to decentralized trustless transactions on a large-scale global basis for every sort

of interaction and transaction (human-to-human, human-to-machine, machine-to-machine) could imply a dramatically different structure and operation of society in ways that cannot yet be foreseen but where current established power relationships and hierarchies could easily lose their utility.

Mainstream Adoption: Trust, Usability, Ease of Use

Because many of the ideas and concepts behind Bitcoin and blockchain technology are new and technically intricate, one complaint has been that perhaps cryptocurrencies are too complicated for mainstream adoption. However, the same was true of the Internet, and more generally at the beginning of any new technology era, the technical details of "what it is" and "how it works" are of interest to a popular audience. This is not a real barrier; it is not necessary to know how TCP/IP works in order to send an email, and new technology applications pass into public use without much further consideration of the technical details as long as appropriate, usable, trustable frontend applications are developed. For example, not all users need to see (much less manually type) the gory detail of a 32-character alphanumeric public address. Already "mainstream wallet" companies such as Circle Internet Financial and Xapo are developing frontend applications specifically targeted at the mainstream adoption of Bitcoin (with the goal of being the "Gmail of Bitcoin" in terms of frontend usability—and market share). Because Bitcoin and ewallets are related to money, there is obvious additional sensitivity in end-user applications and consumer trust that services need to establish. There are many cryptocurrency security issues to address to engender a crypto-literate public with usable customer wallets, including how to back up your money, what to do if you lose your private key, and what to do if you received a proscribed (i.e., previously stolen) coin in a transaction and now cannot get rid of it. However, these issues are being addressed by the blockchain industry, and alternative currencies can take advantage of being just another node in the ongoing progression of financial technology (fintech) that includes ATMs, online banking, and now Apple Pay.

Currency application adoption could be straightforward with trustable usable frontends, but the successful mainstream adoption of beyond-currency blockchain applications could be subtler. For example, virtual notary services seem like a no-brainer for the easy, low-cost, secure, permanent, findable registration of IP, contracts, wills, and similar documents. There will doubtlessly remain social reasons that people prefer to interact with a lawyer about certain matters (perhaps the human-based advice, psychoanalysis, or validation function that attorneys may provide), and for these kinds of reasons, technology adoption based exclusively on efficiency arguments could falter. Overall, however, if Bitcoin and the blockchain industry are to mature, it will most likely be in phases, similar to the adoption pattern of the Internet for which a clear value proposition resonated with different potential audiences, and then they came online with the new technology. Initially, the Internet solved