1

WHAT IS THE BLOCKCHAIN?

"If you cannot understand it without an explanation, you cannot understand it with an explanation."

—HARUKI MURAKAMI

PAY CLOSE ATTENTION. This chapter is probably the most important in the book, because it attempts to offer a foundational explanation of the blockchain. It is the first stage of this book's promise to give you a holistic view of the blockchain's potential.

Understanding blockchains is tricky. You need to understand their message before you can appreciate their potential. In addition to their technological capabilities, blockchains carry with them philosophical, cultural, and ideological underpinnings that must also be understood.

Unless you're a software developer, blockchains are not a product that you just turn on, and use. Blockchains will enable other products that you will use, while you may not know there is a blockchain behind them, just as you do not know the complexities behind what you are currently accessing on the Web.

Once you start to imagine the blockchains' possibilities on your own, without continuously thinking about trying to understand them at the same time, you will be in a different stage of your maturity for exploiting them.

It is my belief that the knowledge transfer behind understanding the blockchain is easier than the knowledge about knowing where they will fit. It's like learning how to drive a car. I could teach you how to drive one, but cannot predict where you will take it. Only you know your particular business or situation, and only you will be able to figure out where blockchains fit, after you have learned what they can do. Of course, we will first go together on road tests and racing tracks to give you some ideas.

VISITING SATOSHI'S PAPER

When Tim Berners-Lee created the first World Wide Web page in 1990, he wrote: "When we link information in the Web, we enable ourselves to discover facts, create ideas, buy and sell things, and forge new relationships at a speed and scale that was unimaginable in the analogue era."

In that short statement, Berners-Lee predicted search, publishing, e-commerce, e-mail, and social media, all at once, by a single stroke. The Bitcoin equivalent to that type of prescience by someone who just created something spectacular can be found in Satoshi Nakamato's 2008 paper, "Bitcoin: A Peer-to-Peer Electronic Cash System,"[1] arguably the root of modern blockchain-based cryptocurrency innovation.

The paper's abstract depicts Bitcoin's foundation, and it explains its first principles:

- A purely *peer-to-peer* version of electronic cash would allow online payments to be sent *directly from one party to another without going through a financial institution*.

- A *trusted third party is not required* to prevent double-spending.

- We propose a *solution* to the double-spending problem *using a peer-to-peer network*.

- *The network timestamps transactions* by hashing them into an ongoing chain of hash-based proof-of-work, forming *a record that cannot be changed without redoing the proof-of-work.*

- The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as *a majority of CPU power is controlled by nodes that are not cooperating to attack the network,* they'll generate the longest chain and outpace attackers.

- The network itself requires minimal structure. Messages are broadcast on a best-effort basis, and *nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*

If you are a non-technical reader, and you focus on the italicized parts, you will start to get the gist of it. Please re-read the above points, until you have internalized Nakamoto's sequential logic! Seriously. You will need to believe and accept that validating peer-to-peer transactions is entirely possible by just letting the network perform a trust duty, without central interference or hand-holding.

Paraphrasing Nakamoto's paper, we should be left with these points:

- Peer-to-peer electronic transactions and interactions
- Without financial institutions
- Cryptographic proof instead of central trust
- Put trust in the network instead of in a central institution

As it turns out, the "blockchain" is that technology invention behind Bitcoin, and what makes this possible. With Satoshi's abstract still in your mind, let us dive deeper with three different but complementary definitions of the blockchain: a technical, business, and legal one.

Technically, the blockchain is a back-end database that maintains a distributed ledger that can be inspected openly.

Business-wise, the blockchain is an exchange network for moving transactions, value, assets between peers, without the assistance of intermediaries.

Legally speaking, the blockchain validates transactions, replacing previously trusted entities.

TECHNICAL Back-end database that maintains a distributed ledger, openly.

BUSINESS Exchange network for moving value between peers.

LEGAL A transaction validation mechanism, not requiring intermediary assistance.

Blockchain Capabilities = Technical + Business + Legal.

THE WEB, ALL OVER AGAIN

The past is not an accurate compass to the future, but understanding where we came from helps us gain an enlightened perspective and a better context for where we are going. The blockchain is simply part of the continuation of the history of Internet technology, represented by the Web, as it carries on its journey to infiltrate our world, businesses, society, and government, and across the several cycles and phases that often become visible only in the rearview mirror.

Whereas the Internet was first rolled out in 1983, it was the World Wide Web that gave us its watershed evolutionary moment, because it made information and information-based services openly and instantly available to anyone on earth who had access to the Web.

In the same way that billions of people around the world are currently connected to the Web, millions, and then billions of people, will be connected to blockchains. We should not be surprised if the velocity of blockchain usage propagation surpasses the historical Web users growth.

By mid-2016, 47% of the world's 7.4 billion population had an Internet connection. In 1995, that number was less than 1%. It took until 2005 to reach one billion Web users. In contrast, cellular phone usage galloped faster, passing the number of landlines in 2002, and surpassing the world's population in 2013. As for websites, in 2016, their total number hovered at around one billion. Quite possibly, blockchains will grow into several flavors, and will become as easily configurable as launching a website on Wordpress or Squarespace.

The blockchain's usage growth has an advantage on the Web's trajectory, because its starting point is amplified along four segments: Web users, cellular phone users, website owners, and any "thing" that gains benefits from being connected, and becoming a "smart thing." This means that blockchain usage will ride on these four categories, instead of purely seeking new users.

ONE OR SEVERAL BLOCKCHAINS?

There are no previous paradigms for the blockchain. It is not a new version of TCP/IP, the Internet network protocol. It is not another whole Internet either. In 2015, some proponents of a single Bitcoin blockchain lamented the existence of several blockchains. The blockchain was seen via a one-dimensional lens (Bitcoin maximalism[2]), by taking a similar view as the Internet. Yes, it's good there is only one Internet, as it would have never propagated as it did. But the blockchain is a different construct. It is more of a new protocol that sits on top of the Internet, just as the World Wide Web sits on top of the Internet via its own technology standards.

The blockchain is part database, part development platform, part network enabler, so we need many instances of it and variations thereof. As an overlay on top of the Internet, blockchains can take many forms of implementations. Blockchains can be seen as a trust layer, an exchange medium, a secure pipe, a set of decentralized capabilities, and even more.

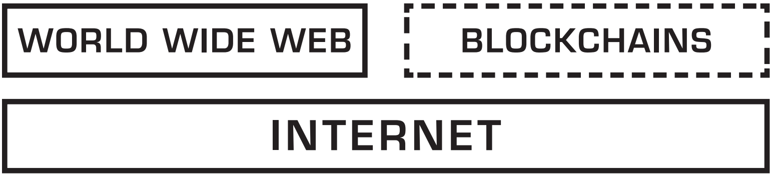
That said, there are many analogies between the Web's early years and today's blockchain's evolution, in terms of how the technology will be adopted.

Let us not forget that it took about three years for most companies to fully understand the Web's potential (1994–1997 roughly), after its initial commercialization, and it took seven years after the Internet's 1983 launch for the Web to come into play. There is no doubt the blockchain will remain a semi-mysterious, semi-complex phenomena for the period 2015–2018, just as it took Bitcoin three quiet years (2009–2012) before it became more visibly known to the general public.

INTRODUCTION TO BLOCKCHAIN APPLICATIONS

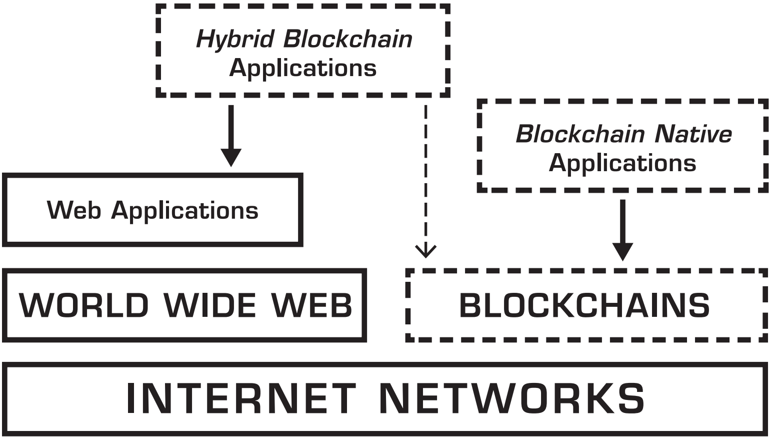
The Web could not exist without the Internet. And blockchains could not be without the Internet. The Web made the Internet more useful, because people were more interested in using the information, than figuring out how to hook up computers together. Blockchain applications need the Internet, but they can bypass the Web, and give us another version that is more decentralized, and perhaps more equitable. That is one of the biggest promises of blockchain technology.

BLOCKCHAINS, LIKE THE WEB, NEED THE INTERNET



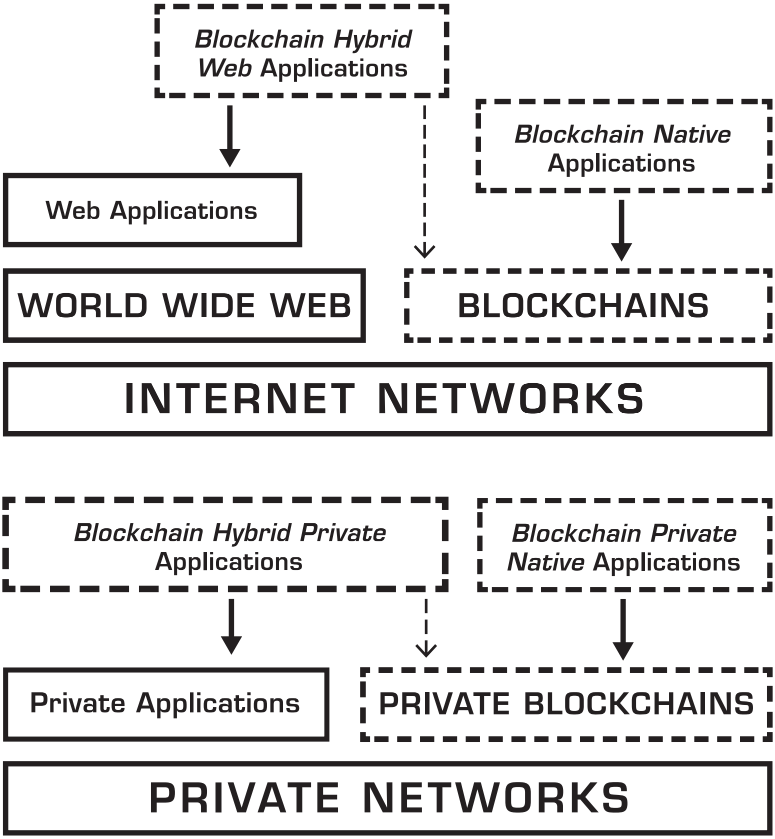
There is more than one way to build blockchain applications. You can build them natively on a blockchain, or you could mix them in an existing Web application, and we will call that flavor, "hybrid blockchain applications."

FLAVORS OF BLOCKCHAIN APPLICATIONS


Hybrid Blockchain Applications
Blockchain Native Applications
Web Applications
WORLD WIDE WEB
BLOCKCHAINS
INTERNET NETWORKS

Since the Internet is comprised of a public version and several private variations, blockchains will also follow that path. Therefore, we will have public and private blockchains. Some will be natively bolted to a blockchain, whereas others might be a hybrid implementation that is part of an existing Web or private application.

FOUR TYPES OF
BLOCKCHAIN APPLICATIONS


Blockchain Hybrid Web Applications
Blockchain Native Applications
Web Applications
WORLD WIDE WEB
BLOCKCHAINS
INTERNET NETWORKS
Blockchain Hybrid Private Applications
Blockchain Private Native Applications
Private Applications
PRIVATE BLOCKCHAINS
PRIVATE NETWORKS

THE BLOCKCHAIN'S NARRATIVE IS STRONG

A sign of strong impact for a technology or trend is whether it has a strong narrative. What's the difference between a story and a narrative? Whereas a story is usually consistent and known, a narrative creates more individual stories for whomever interacts with that trend.

John Hagel explained that difference well:[3]

> *Stories are self-contained—they have a beginning, a middle and an end. Narratives on the other hand are open-ended—the outcome is unresolved, yet to be determined. Second, stories are about me, the storyteller, or other people; they are not about you. In contrast, the resolution of narratives depends on the choice you make and the actions you take—you will determine the outcome.*

The Internet had a strong narrative. If you ask various people how they use the Internet, or what it means to them, you would undoubtedly hear different answers, because each person takes the Internet and makes it their own, depending on their own adaptation of its usages.

The blockchain has a strong narrative because it sparks our imagination.

According to Hagel, these are specific benefits that narratives provide:

DIFFERENTIATION – it helps you to stand out from the crowd
LEVERAGE – it mobilizes people outside your company
DISTRIBUTED INNOVATION – it spurs innovation in unexpected directions
ATTRACTION – it draws people by the opportunity and the challenge you have laid out
RELATIONSHIPS – it spurs sustained relationships with others that have fallen under the spell of your narrative

John Hagel goes on specifying that "it's about connecting with and mobilizing others beyond the boundaries of ...." Replace the dots by "blockchain," and you will get a powerful foundation for a strong and long lasting blockchain narrative.

A META TECHNOLOGY

The blockchain is a meta technology because it affects other technologies, and it is made up of several technologies itself. It is as an overlay of computers and networks that are built on top of the Internet. When you examine the architectural layers of a blockchain, you will find it is comprised of several pieces: a database, a software application, a number of computers connected to each other, clients to access it, a software environment to develop on it, tools to monitor it, and other pieces (that will be covered in Chapter 6).

Blockchain is not just any new technology. It is a type of technology that challenges other existing software technologies, because it has the potential to replace or supplement existing practices. In essence, it is technology that changes other technology.

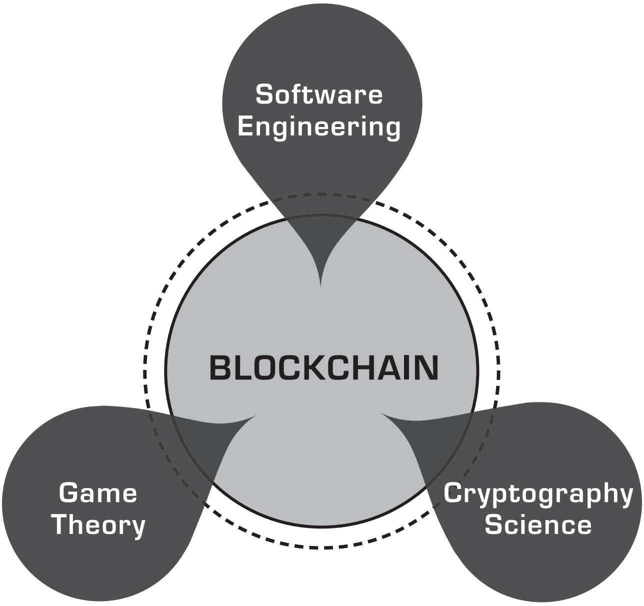
The last time we witnessed such a catalytic technology dates back to the Web's arrival. The Web also changed how we wrote software applications, and it brought along with it new software technology that challenged and replaced previous ones. In 1993, HTML, a markup language changed publishing. In 1995, Java, a Web programming language changed programming. A few years earlier, TCP/IP, a computer network protocol had started to change networking by making it fully interoperable, globally.

From a software development point of view, one of the biggest paradigm shifts that the blockchain claims is in challenging the function and monopoly of the traditional database as we currently know it. Therefore we need to deeply understand how the blockchain makes us rethink the existing database constructs.

The blockchain is changing how we write applications via a new form of scripting languages that can program business logic as smart contracts that are enforced on the blockchain.

SOFTWARE, GAME THEORY AND CRYPTOGRAPHY

Another way to understand the blockchain is in seeing it as a triad of combustion of the known fields of 1) game theory, 2) cryptography science, and 3) software engineering. Separately, these fields have existed for a long time, but for the first time, they have together intersected harmoniously and morphed inside blockchain technology.



Game theory is 'the study of mathematical models of conflict and cooperation between intelligent rational decision-makers."[4] And this is related to the blockchain because the Bitcoin blockchain, originally conceived by Satoshi Nakamoto, had to solve a known game theory conundrum called the Byzantine Generals Problem.[5] Solving that problem consists in mitigating any attempts by a small number of unethical Generals who would otherwise become traitors, and lie about coordinating their attack to guarantee victory.

This is accomplished by enforcing a process for verifying the work that was put into crafting these messages, and time-limiting the requirement for seeing untampered messages in order to ensure their validity. Implementing a "Byzantine Fault Tolerance" is important because it starts with the assumption that you cannot trust anyone, and yet it delivers assurance that the transaction has traveled and arrived safely based on trusting the network during its journey, while surviving potential attacks.

There are fundamental implications for this new method of reaching safety in the finality of a transaction, because it questions the existence and roles of current trusted intermediaries, who held the traditional authority on validating transactions. This makes us ponder the existential question: why do we need a central authority to ensure central trust, if we can accomplish the same trustworthiness when the transaction travels from one peer to another, via a network where trust is embedded in it?

Cryptography science is used in multiple places to provide security for a blockchain network, and it rests on three basic concepts: hashing, keys, and digital signatures. A "hash" is a unique fingerprint that helps to verify that a certain piece of information has not been altered, without the need to actually see it. Keys are used in at least a combination of two: a public and a private one. For analogy, imagine a door that needs two keys to open it. In this case, the public key is used by the sender to encrypt information that can only be decrypted by the owner of the private key. You never reveal your private key. A digital signature is a mathematical computation that is used to prove the authenticity of a (digital) message or document.

Cryptography is based on the public/private hegemony, which is the yin-yang of the blockchain: public visibility, but private inspection. It's a bit like your home address. You can publish your home address publicly, but that does not give any information about what your home looks like on the inside. You'll need your private key to enter your private home, and since you have claimed that address as yours, no one else can claim a similar address as being theirs.

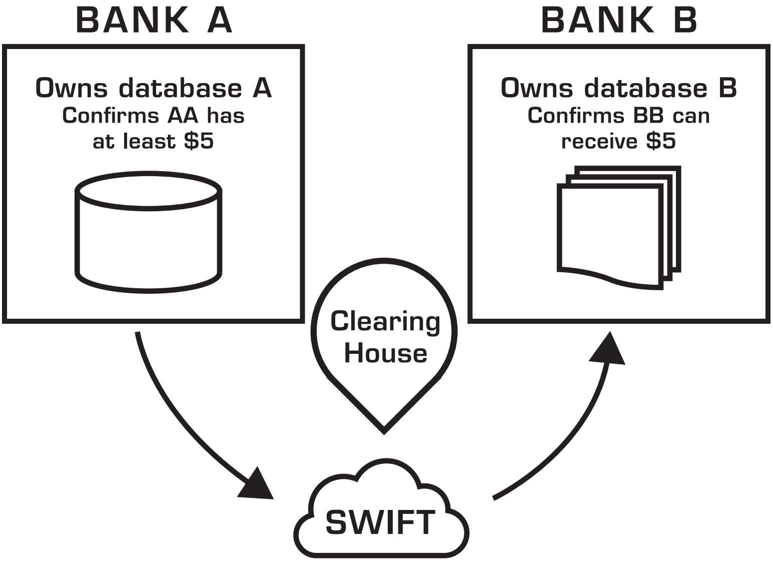
Although the concepts of cryptography have been around for a while, software engineers are feasting on combining it with game theory innovation, to produce the overall constructs of blockchains, where seeming uncertainty is mitigated with overwhelming mathematical certainty.

THE DATABASE VS. THE LEDGER

We have transactions that can get validated without a third party. Now, you're thinking—how about databases? We have always thought that databases are trusted repositories for holding assets.

In the case of the blockchain, the ledger is that irrefutable record that holds the register of transactions that have been validated by the blockchain network.

Let us illustrate the impact of this situation: the database versus the (blockchain) ledger.

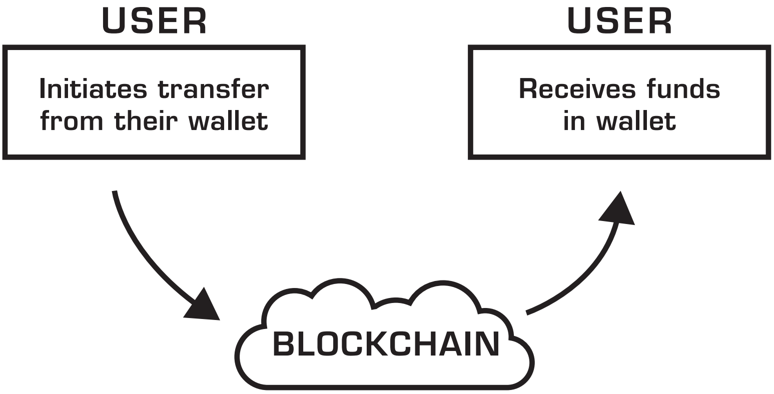


When you open a bank account, you have really abdicated authority to your bank on that "account." In reality, they provided you the illusion of access and activity visibility on it. Every time you want to move money, pay someone or deposit money, the bank is giving you explicit access because you gave them implicit trust over your affairs. But that "access" is also another illusion. It is really an access to a database record that says you have such amount of money. Again, they fooled you by giving you the illusion that you "own" that money. But they hold the higher authority because they own the database that points to that entry that says that you have the money, and you assume that you have your money.

Banking is complex, but I tried to simplify the above illustration to emphasize the fact that a given bank owns the control hierarchy for granting or denying access to money they hold. The same concept applies for any digital assets (stocks, bonds, securities) that a financial institution might hold on your behalf.

Enter the blockchain.

In its most basic form, that same scenario can happen without the complexities depicted above. A user can send money to another, via a special wallet, and the blockchain network does the authentication, validation and transfer, typically within 10 minutes, with or without a cryptocurrency exchange in the middle.



That is the magic of the blockchain in its simplest form. That is why I suggest to anyone who is going to get involved in implementing the blockchain to experience performing this type of transaction with their own wallet, by either downloading one of the many available versions, or by signing-up to a local Bitcoin exchange that exists wherever you live. Once you do, you will realize the true meaning of "no intermediaries," and you will start to question why we still need the current intermediaries.

LOOKING BACK SO WE CAN LOOK FORWARD

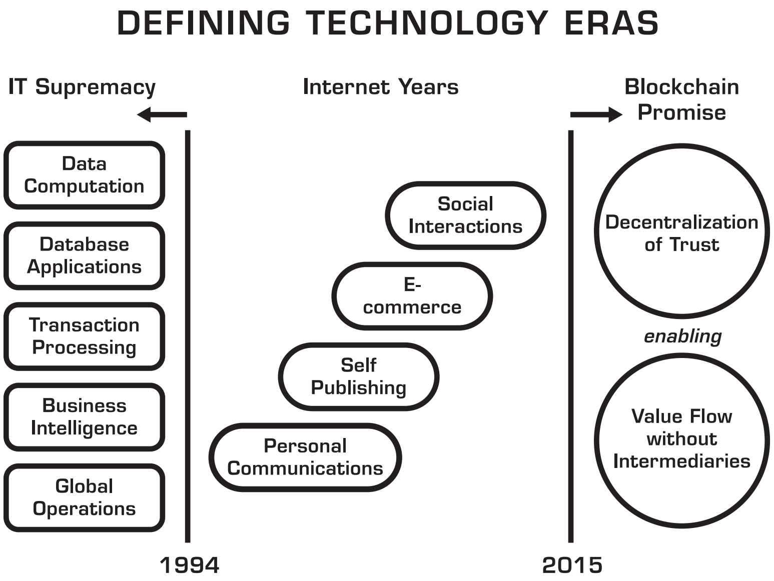
So, where does the blockchain fit in the overall context of the various eras of technology evolution?

In 2003, Nicholas G. Carr dropped a seminal article[6] in the *Harvard Business Review*, "IT Does not Matter," that shook the Information Technologies corporate circles and questioned their strategic relevance. He wrote:

> *What makes a resource truly strategic—what gives it the capacity to be the basis for a sustained competitive advantage—is not ubiquity but scarcity. You only gain an edge over rivals by having or doing something that they cannot have or do. By now, the core functions of IT—data storage, data processing, and data transport—have become available and affordable to all.*

Although Carr was vigorously debated for another two years following that article, the writing was already on the wall, coinciding with the advent of the Web as a powerful new computing platform. The Web caught CIOs by surprise, and put most of them in disarray for at least three years, especially that many of them were more focused on the year 2000 date compliance issue. In reality, IT's decline had started when the Web arrived, because the Web provided some competitive advantages to those who mastered it early.

As depicted in this chart, the end of IT supremacy was followed by the Internet years, which in turn will be followed by the Blockchain's promise.



Another way to see continuity in technology's evolution is by depicting the various phases of the Web's evolution, and seeing that the blockchain is yet another new phase, focused on peer-to-peer, trust-based asset transactions. Let us remember the key mini-revolutions that the Internet brought us since 1994: Personal Communications, Self-Publishing, E-Commerce, and the Social Web. In hindsight, each of these four phases was defined by the functions they disrupted: the post-office, print media, supply chains/physical stores, and the real world.

PHASE	GOAL	DISRUPTING	OUTCOME
Communications	Reach anyone in the world	Post office	Personal Communications
Publishing	Spread ideas	Print media	Self-publishing
Commerce	Trade	Supply chains and physical stores	E-Commerce
Social Interactions	Connect with friends	Real world	Social Web
Asset Transactions	Manage what you own	Existing custodians	Trust-based Services

The irony of this situation is that blockchain-based applications can replace any Web application. Although we think the Web brought us information publishing, communications and e-commerce, those very functions will be threatened by new versions that rest on peer-to-peer protocols that are anchored by blockchain technologies.

UNPACKING THE BLOCKCHAIN

Let us continue revealing the many layers of the blockchain! If there is one main point that I will keep drilling upon, it is to emphasize that the blockchain is not one item, thing, trend, or feature. It is many pieces all at once, some of them working together, and others independently.

When the Internet started to get commercialized around 1995, we often described it as multi-purpose kind of phenomenon. In my previous book, *Opening Digital Markets*, in 1997, I described the Internet as having "five multiple identities," and added that "each one must be taken advantage of by developing a different strategy." The Web was simultaneously a Network, a Development Platform, a Transaction Platform, a Medium, and a Marketplace. (We didn't see the Community / Social Network aspect then, as it surfaced later.)

The blockchain takes that multiplicity of functions further. It exhibits simultaneously the following ten properties:

1. Cryptocurrency
2. Computing Infrastructure
3. Transaction Platform
4. Decentralized Database
5. Distributed Accounting Ledger
6. Development Platform
7. Open Source Software
8. Financial Services Marketplace
9. Peer-to-Peer Network
10. Trust Services Layer

Let us dive into each one of them, as the first step in establishing a foundational understanding of the blockchain.

1. Digital Cryptocurrency

The digital currency function is probably the most "visible" element in a blockchain, especially if the blockchain is a public one, for example, Bitcoin (BTC) or Ethereum (ETH). Cryptocurrency is generally an economic proxy to the viable operations and security of a blockchain. Sometimes it is represented by a token, which is another form of related representation of an underlying cryptocurrency.

One of the challenging issues with cryptocurrencies is their price volatility, which is enough to keep most consumers away. In a 2014 paper describing a method for stabilizing cryptocurrency, Robert Sams quoted Nick Szabo: "The main volatility in bitcoin comes from variability in speculation, which in turn is due to the genuine uncertainty about its future. More efficient liquidity mechanisms do not help reduce genuine uncertainty." As cryptocurrency gains more acceptance and understanding, its future will be less uncertain, resulting in a more stable and gradual adoption curve.

Cryptocurrency can have a "production" role for compensating miners who win rewards when they successfully validate transactions. Cryptocurrency can also have a "consumption" role when paying a small fee for running a smart contract (e.g., Ethereum's ETH), or as a transaction fee equivalent (e.g., Ripple's XRP or Bitcoin's BTC). These economic incentives and costs are put in place to prevent abuse of the blockchain. In a more advanced usage case, the token can be used as a unit of internal value, for example in Distributed Autonomous Organizations (DAOs), a subject that will be covered later in Chapters 5 and 7 of this book.

Outside of the blockchain's operations proper, cryptocurrency is just like any other currency. It can be traded on exchanges, and it can be used to buy or sell goods and services. Cryptocurrency is very efficient inside blockchain networks, but there is friction every time it crosses into the real world of traditional currency (also called "fiat currency").

2. Decentralized Computing Infrastructure

The blockchain can also be seen as a software design approach that binds a number of computers together that commonly obey the same "consensus" process for releasing or recording what information they hold, and where all related interactions are verified by cryptography.

From a physical perspective, networked computer servers are what really powers blockchains. But developers do not need to set up these servers, and that is part of the magic of a blockchain. As contrasted with the Web where an HTTP (Hypertext Transfer Protocol) request is sent to the server, with blockchain apps, the network makes a request to the blockchain.

3. Transaction Platform

A blockchain network can validate a variety of value-related transactions relating to digital money or assets that have been digitized.

Every time a consensus is reached, a transaction is recorded on a "block" which is a storage space. The blockchain keeps track of these transactions that can be later verified as having taken place. The blockchain is therefore this giant transaction processing platform, capable of handling microtransactions and large value transactions alike.

If we are to equate blockchains to other transactions processing networks, what comes to mind is their processing throughput, which is measured in transactions per second (TPS). As a reference, in 2015, VISA handled an average of 2,000 TPS on their VisaNet, with a peak rate of 4,000 TPS, and a peak capacity of 56,000 TPS. During 2015, PayPal processed a total 4.9 billion payments,[7] equivalent to 155 TPS. As of 2016, the Bitcoin blockchain was far from these numbers, hovering at 5–7 TPS, but with prospects of largely exceeding it due to advances in sidechain technology and expected increases in the Bitcoin block size. Some other blockchains are faster than Bitcoin's. For example, Ethereum started with 10 TPS in 2015, edging towards 50–100 TPS in 2017, and targeting 50,000–100,000 TPS by 2019.[8] Private blockchains are even faster because they have less security requirements, and we are seeing 1,000–10,000 TPS in 2016, going up to 2,000–15,000 TPS in 2017, and potentially an unlimited ceiling beyond 2019. Finally, linking blockchain's output to clustered database technology might push these transactional throughput limits even higher, leading to a positive development.

4. Decentralized Database

The blockchain shatters the database/transaction processing paradigm. In 2014, I made the strong assertion that the blockchain is the new database, and warned developers to get ready to rewrite everything.

A blockchain is like a place where you store any data semipublicly in a linear container space (the block). Anyone can verify that you've placed that information, because the container has your signature on it, but only you (or a program) can unlock what's inside the container, because only you hold the private keys to that data, securely.

So the blockchain behaves almost like a database, except that part of the information stored, its "header," is public. Admittedly, blockchains are not very efficient databases, but that's OK. Their job is not to replace large databases, but rather, it is the job of software developers to figure out how they can re-write their applications to take advantage of the blockchain's state transitions capabilities.

5. Shared, Distributed Accounting Ledger

The blockchain is also a distributed, public, time-stamped asset ledger that keeps track of every transaction ever processed on its network, allowing a user's computer to verify the validity of each transaction such that there can never be any double-counting. This ledger can be shared across multiple parties, and it can be private, public, or semi-private.

Although being a distributed ledger of transactions is a popular way to describe blockchains, and some see it as the killer app, it is only one of its characteristics.

6. Software Development Platform

For developers, a blockchain is first and foremost a set of software technologies. Yes, they have an underlying political and societal underpinning (decentralization), but they bring with them technological novelties. This new set of development tools is an exciting event for software engineers. The blockchain includes technologies for building a new breed of applications, ones that are decentralized and cryptographically secure.

Also, blockchains can have a variety of APIs, including a transaction scripting language, a P2P nodes communications API, and a client API to check transactions on the network. I will cover the software development aspect in more details in Chapter 6 of this book.

7. Open Source Software

Most robust blockchains are open sourced, which not only means that the source of the software is public, it also means that innovation can happen in a collaborative way, on top of the core software.

For example, the core Bitcoin protocol is open source. Since its initial development by its creator Satoshi Nakamoto, it has been maintained by a group of "core developers," who continue to enhance it over time. In addition, thousands of independent developers innovate with complementary products, services, and applications that take advantage of the Bitcoin protocol robustness.

The fact that blockchain software is open source is a powerful feature. The more open the core of a blockchain is, the stronger the ecosystem around it will become.

8. Financial Services Marketplace

Money is at the heart of cryptocurrency-based blockchains. When cryptocurrency is treated like any currency, it can become part of a financial instrument, leading to the development of a variety of new financial products.

Blockchains offer an incredible innovation environment for the next generation of financial services. As cryptocurrency volatilities subside, these will become popular. Derivatives, options, swaps, synthetic instruments, investments, loans, and many other traditional instruments will have their cryptocurrency version, therefore creating a new financial services trading marketplace.

9. Peer-to-Peer Network

There is nothing "central" about blockchains. Architecturally, the base layer of the blockchain is a peer-to-peer network. A blockchain pushes for decentralization via peer processing at its node locations. The network is really the computer. You verify each other transaction at the peer-to-peer level. In essence, a blockchain could be regarded as a thin computing cloud that is truly decentralized.

Any user can reach and transact with another user instantly, no matter where they are in the universe, and regardless of business hours. No intermediary is needed to filter, block, or delay a transaction between any two or more users, or between nodes that are consuming a transaction. Any node on the network is allowed to offer services based on their knowledge of transactions everywhere else in that network.

In addition to creating a technical P2P network, blockchains also create a marketplace of users. Blockchain networks and applications on top of them create their own (distributed) economies, with a variety of sizes and vibrancy. So, blockchains bring with them an economic model, and that is a key feature that will be expanded upon later in this book.

10. Trust Services Layer

All blockchains commonly hold trust as an atomic unit of service. In essence, it is a function and a service that is delivered. But trust does not apply only to transactions. It is extended to data, services, processes, identity, business logic, terms of an agreement, or physical objects. It applies to almost anything that can be digitized as a (smart) asset with an inherent or related value attached to it.

Now, imagine the possible mashup of innovations that will spring out on top of these 10 powerful features and characteristics. By combining them together, you'll start to imagine the incredible enabling powers of blockchains.

STATE TRANSITIONS AND STATE MACHINES—WHAT ARE THEY?

The blockchain is not for everything. And not everything fits the blockchain paradigm. The blockchain is a "state machine," which is another concept that needs to be understood.

In technical terms, a state just means "stored information" at a specific point in time. A state machine is a computer or device that remembers the status of something at a given instant in time. Based on some inputs, that status might change, and it provides a resulting output for these implemented changes. Keeping track of transitions of these states is important and that's what the blockchain does well, and in a way that is immutable. In contrast, a database's record is mutable, because it can be re-written many times over. Not all databases have audit trails, and even if they do, an audit trail could be destroyed or lost, because it is not tamper proof. In the blockchain, the transition history is a persistent part of the information about that state. In the Ethereum blockchain, a distinct "state tree" is stored, representing the current balance of each address, and a "transaction list" representing the transactions between the current block and previous blocks in each block.

State machines are a good fit for implementing distributed systems that have to be fault-tolerant.

THE CONSENSUS ALGORITHMS

At the heart of understanding the severity of the blockchain paradigm shift lies the basic understanding of the concept of "decentralized consensus," a key tenet of the cryptography-based computing revolution.

Decentralized consensus breaks the old paradigm of centralized consensus, that is, when one central database used to rule transaction validity. A decentralized scheme (which blockchain protocols are based on), transfers authority and trust to a decentralized virtual network, and enables its nodes to continuously and sequentially record transactions on a public "block," creating a unique "chain," the blockchain. Each successive block contains a "hash" (a unique fingerprint) of the previous code, therefore cryptography (via hash codes) is used to secure the authentication of the transaction source and removes the need for a central intermediary. The combination of cryptography and blockchain technology ensures there is never a duplicate recording of the same transaction. What's important here is that with this degree of unbundling, the consensus logic is separate from the application itself, therefore applications can be written to be organically decentralized, and that is the spark for a variety of system-changing innovations in the software architecture of applications, whether they are money or non-money related.

You could think of consensus as the first layer of a decentralized architecture. It is the basis for the underlying protocol governing a blockchain's operation.

A consensus algorithm is the nucleus of a blockchain representing the method or protocol that commits the transaction. It is important, because we need to trust these transactions. As a business user, you do not need to understand the exact ways that these algorithms work, as long as you believe in their security and reliability.

Bitcoin initiated the Proof-of-Work (POW) consensus method, and it can be regarded as the granddaddy of these algorithms. POW rests on the popular Practical Byzantine Fault Tolerant[9] algorithm that allows transactions to be safely committed according to a given state. An alternative to POW for achieving consensus is Proof-of-Stake.[10] There are other consensus protocols such as RAFT, DPOS, and Paxos, but we are not going into that slippery slope of comparing them to each other, because they will be seen as standard plumbing over time. What will matter more is the robustness of the tools and middleware technologies that are being built on top of the algorithms, as well as the ecosystem of value-added players that surround them.

One of the drawbacks of the Proof-of-Work algorithm is that it is not environmentally friendly, because it requires large amounts of processing power from specialized machines that generate excessive energy. A strong contender to POW will be the Proof-of-Stake (POS) algorithm which relies on the concept of virtual mining and token-based voting, a process that does not require the intensity of computer processing as the POW, and one that promises to reach security in a more cost-effective manner.

Finally, when discussing consensus algorithm, you need to consider the "permissioning" method, which determines who gets to control and participate in the consensus process. The three popular choices for the type of permissioning are:

1. Public (e.g., POW, POS, Delegated POS)
2. Private (uses secret keys to establish authority within a confined blockchain)
3. Semi-private (e.g., consortium-based, uses traditional Byzantine Fault Tolerance in a federated manner)

KEY IDEAS FROM CHAPTER ONE

1. The blockchain is a layer of technology on top of the Internet, just like the World Wide Web.

2. A blockchain has technical, business and legal definitions.

3. Cryptographic proof is the trusted method that blockchains utilize to confirm the validity and finality of transactions between parties.

4. The blockchain will redefine the role of existing intermediaries (if they accept to change), while creating new intermediaries, therefore it will disrupt the traditional boundaries of value.

5. The blockchain has ten characteristics, and they all need to be understood in a holistic manner.

NOTES

1. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/en/bitcoin-paper.
2. Bitcoin "maximalism" refers to the opinion that solely supports Bitcoin at the expense of all other blockchain or cryptocurrency related projects, because maximalists believe we only a need a single blockchain, and single currency in order to achieve desired network effects benefits.
3. The Untapped Potential of Corporate Narratives. http://edgeperspectives.typepad.com/edge_perspectives/2013/10/the-untapped-potential-of-corporate-narratives.html.
4. Myerson, Roger B. (1991). *Game Theory: Analysis of Conflict,* Harvard University Press.
5. Leslie Lamport, Robert Shostak, and Marshall Pease, *The Byzantine Generals Problem.* http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf.
6. *IT Does not Matter*, https://hbr.org/2003/05/it-doesnt-matter.
7. PayPal website, https://www.paypal.com/webapps/mpp/about.
8. Personal communication with Vitalik Buterin, February 2016.
9. Byzantine fault tolerance, https://en.wikipedia.org/wiki/Byzantine_fault_tolerance.
10. Proof-of-stake, https://en.wikipedia.org/wiki/Proof-of-stake.