

Compliments of



Blockchain

for
dummies[®]
A Wiley Brand

IBM Limited Edition



Grasp blockchain
fundamentals

—
Make blockchain real
for business

—
Get started
on blockchain

Manav Gupta



Blockchain

IBM Limited Edition

by Manav Gupta

for
dummies[®]
A Wiley Brand

Blockchain For Dummies®, IBM Limited Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2017 by John Wiley & Sons, Inc.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. IBM and the IBM logo are registered trademarks of International Business Machines Corporation. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN: 978-1-119-37123-6 (pbk); ISBN: 978-1-119-37139-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Acquisitions Editor: Steve Hayes

Business Development

Representative: Sue Blessing

Production Editor: Vasanth Koilraj

Table of Contents

INTRODUCTION	1
About This Book	1
Foolish Assumptions	2
Icons Used in This Book.....	2
CHAPTER 1: Grasping Blockchain Fundamentals	3
Tracing Blockchain's Origin	3
The shortcomings of current transaction systems.....	4
The emergence of bitcoin	5
The birth of blockchain	6
Revolutionizing the Traditional Business Network	6
Exploring a blockchain application	7
Recognizing the key business benefits.....	9
Building trust with blockchain	10
CHAPTER 2: Taking a Look at How Blockchain Works	13
Why It's Called "Blockchain"	13
What Makes a Blockchain Suitable for Business?	14
Shared ledger	15
Permissions	15
Consensus.....	16
Smart contracts.....	17
Identifying Participants and Their Roles.....	18
CHAPTER 3: Propelling Business with Blockchains	19
Recognizing Types of Market Friction	20
Information frictions.....	20
Interaction frictions	20
Innovation frictions.....	21
Moving Closer to Friction-Free Business Networks	21
Reducing information friction	22
Easing interaction friction	22
Easing innovation friction	23
Transforming Ecosystems through Increased Visibility.....	24

CHAPTER 4: Blockchain in Action: Use Cases 25

- Financial Services 25
 - Commercial financing..... 25
 - Trade finance..... 26
 - Cross-border transactions 26
- Insurance..... 27
- Government 27
- Supply Chain Management 28
- Healthcare 29
 - Electronic medical records 29
 - Healthcare payments pre-authorization..... 29
- The Internet of Things (IoT)..... 30

CHAPTER 5: Hyperledger, a Linux Foundation Project 31

- Hyperledger Vision 32
- Hyperledger Fabric..... 33
- How Can IBM Help Developers Innovate With Blockchain?..... 34
 - Offering an easily accessible cloud and development platform 34
 - Individualized attention and industry expertise 35

CHAPTER 6: Ten Steps to Your First Blockchain application 37

- Deciding Whether Blockchain Has a Place in Your Industry 37
- Identifying Speed Bumps in Business Processes 38
- Determining How Blockchain Can Help 38
- Choosing an Appropriate Use Case 39
- Determining the Goal of Your Blockchain Network 39
- Identifying Dependencies..... 39
- Choosing a Blockchain Provider and Platform 40
- Developing and Deploying Chaincode..... 40
- Testing and Fine-Tuning Your Application and Network..... 41
- Joining the Hyperledger Rocket Chat Channel..... 41

Introduction

Welcome to *Blockchain For Dummies*, IBM Limited Edition, your guide to all things blockchain for business. It has been said that blockchain will do for transactions what the Internet did for information. What that means is that it allows increased trust and efficiency in the exchange of almost anything. Blockchain can profoundly change how the world works. If you've ever bought a house, you probably had to sign a huge stack of papers from a variety of different stakeholders to make that transaction happen. If you've ever registered a vehicle, you may understand how painful that process can be. I won't even get started on how challenging it can be to track your medical records.

Blockchain, most simply defined as a shared, immutable ledger, has the potential to be the technology that redefines those processes and many others. To be clear, when I talk about blockchain, I'm not talking about bitcoin. I'm talking about the underlying digital foundation that supports applications *such as* bitcoin. But the reaches of blockchain extend far beyond bitcoin.

About This Book

Blockchain For Dummies, IBM Limited Edition, equips you with an understanding of what blockchain is, how it works, and how it can enhance your business and the industry in which it operates. You learn the fundamentals of blockchain and how this technology will revolutionize transactions and business networks. You also discover the important difference between blockchain and blockchain for business and what makes blockchain an ideal solution for streamlining business networks.

You will also discover Hyperledger, a Linux Foundation project, designed to help advance technology and thought leadership of cross-industry blockchain technologies. You learn about Hyperledger Fabric, an open source framework, and the instrumental role it plays in developing a blockchain for business. Finally, you find out everything you need to spin up a blockchain network today.

Foolish Assumptions

I wrote this book based on certain assumptions about you, the reader, to tailor the content of this book and its presentation to the proper audience. First, I assume that you're a developer who's relatively new to blockchain, although the less technical parts of this book may also be of interest to business owners and decision makers. Regardless of your role, I assume you're interested in finding out more about blockchain and its tremendous potential. I also assume you want to know more about the steps you need to take to start deploying blockchain-based business networks.

Icons Used in This Book

Every *For Dummies* book has small images, called icons, sprinkled throughout the margins. I use the following icons in this book:



TIP

This icon guides you to faster, easier ways to perform a task or better ways to put blockchain to use in your business.



REMEMBER

This icon highlights concepts worth remembering and other important topics.



WARNING

If you see this icon, proceed with caution. Here you find advice on how to avoid the most common pitfalls.



ON THE
WEB

Seek out this icon if you want to find out more about blockchain and related topics on the web.

- » Exploring the roots of the shared ledger system
- » Appreciating blockchain's business potential

Chapter **1**

Grasping Blockchain Fundamentals

Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. An *asset* can be tangible — a house, a car, cash, land — or intangible like intellectual property, such as patents, copyrights, or branding. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

That's the elevator speech for blockchain. In the rest of this chapter, I provide additional details to help you more fully appreciate this technology and its potential for streamlining business operations.

Tracing Blockchain's Origin

You can gain a deeper understanding of blockchain by exploring the context in which it was developed — the need for an efficient, cost-effective, reliable, and secure system for conducting and recording financial transactions. In this section, I provide that context and describe the characteristics of blockchain that make it such a suitable solution.

The shortcomings of current transaction systems

Throughout history, instruments of trust, such as minted coins, paper money, letters of credit, and banking systems, have emerged to facilitate the exchange of value and protect buyers and sellers. Important innovations, including telephone lines, credit card systems, the Internet, and mobile technologies have improved the convenience, speed, and efficiency of transactions while shrinking and sometimes virtually eliminating the distance between buyers and sellers.



WARNING

Still, many business transactions remain inefficient, expensive, and vulnerable, suffering from the following limitations:

- » Cash is useful only in local transactions and in relatively small amounts.
- » The time between transaction and settlement can be long.
- » Duplication of effort and the need for third-party validation and/or the presence of intermediaries add to the inefficiencies.
- » Fraud, cyberattacks, and even simple mistakes add to the cost and complexity of doing business, and they expose all participants in the network to risk if a central system, such as a bank, is compromised.
- » Credit card organizations have essentially created walled gardens with a high price of entry. Merchants must pay the high costs of onboarding, which often involves considerable paperwork and a time-consuming vetting process.
- » Half of the people in the world don't have access to a bank account and have had to develop parallel payment systems to conduct transactions.

Transaction volumes worldwide are growing exponentially and will surely magnify the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems. The growth of ecommerce, online banking, and in-app purchases, and the increasing mobility of people around the world have fueled the growth of transaction volumes. And transaction volumes will explode with the rise of Internet of Things (IoT) — autonomous objects, such as refrigerators that buy groceries when supplies are

running low and cars that deliver themselves to your door, stopping for fuel along the way.

To address these challenges and others, the world needs payment networks that are fast and that provide a mechanism that establishes trust, requires no specialized equipment, has no chargebacks or monthly fees, and provides a collective bookkeeping solution for ensuring transparency and trust.

The emergence of bitcoin

One solution that has been developed to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems is *bitcoin* — a digital currency that was launched in 2009 by a mysterious person (or persons) known only by the pseudonym Satoshi Nakamoto.

Unlike traditional currencies, which are issued by central banks, bitcoin has no central monetary authority. No one controls it. Bitcoins aren't printed like dollars or euros; they're “mined” by people and increasingly by businesses, running computers all around the world, using software that solves mathematical puzzles. Rather than rely on a central monetary authority to monitor, verify, and approve transactions and manage the money supply, bitcoin is enabled by a peer-to-peer computer network made up of its users' machines, akin to the networks that underpin BitTorrent and Skype.



TIP

Bitcoin has several advantages over other current transaction systems, including the following:

- » **Cost-effective:** Bitcoin eliminates the need for intermediaries.
- » **Efficient:** Transaction information is recorded once and is available to all parties through the distributed network.
- » **Safe and secure:** The underlying ledger is tamper-evident. A transaction can't be changed; it can only be reversed with another transaction, in which case both transactions are visible.

The birth of blockchain

Bitcoin is actually built on the foundation of blockchain, which serves as bitcoin's shared ledger. Think of blockchain as an operating system, such as Microsoft Windows or MacOS, and bitcoin as only one of the many applications that can be run on that operating system. Blockchain provides the means for recording bitcoin transactions — the shared ledger — but this shared ledger can be used to record any transaction and track the movement of any asset whether tangible, intangible, or digital. For example, blockchain enables securities to be settled in minutes instead of days. It can also be used to help companies manage the flow of goods and related payments, or enable manufacturers to share production logs with original equipment manufacturers (OEMs) and regulators to reduce product recalls.



REMEMBER

The takeaway lesson: Bitcoin and blockchain are *not* the same. Blockchain provides the means to record and store bitcoin transactions, but blockchain has many uses beyond bitcoin. Bitcoin is only the first use case for blockchain.

Revolutionizing the Traditional Business Network

With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records, as shown in the picture on the left in Figure 1-1. This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services. It's clearly inefficient due to delays in executing agreements and the duplication of effort required to maintain numerous ledgers. It's also vulnerable because if a central system (for example, a bank) is compromised, due to fraud, cyberattack, or a simple mistake, the entire business network is affected.

The picture on the right in Figure 1-1 represents business networks that use blockchain. The blockchain architecture gives participants the ability to share a ledger that is updated, through peer-to-peer replication, every time a transaction occurs. *Peer-to-peer replication* means that each participant (node) in the network acts as both a publisher and a subscriber. Each node can receive or send transactions to other nodes, and the data is synchronized across the network as it is transferred.

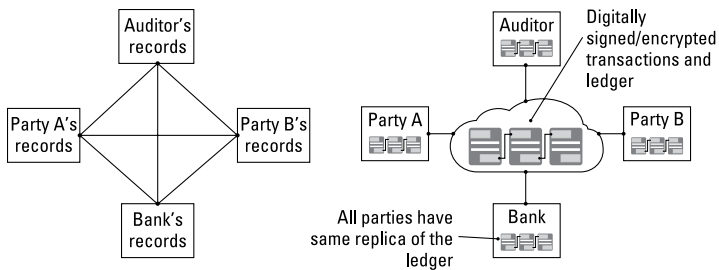


FIGURE 1-1: Business networks before and after blockchain.

The blockchain network is economical and efficient, because it eliminates duplication of effort and reduces the need for intermediaries. It's also less vulnerable because it uses consensus models to validate information. Transactions are secure, authenticated, and verifiable.



REMEMBER

The participants in both transaction systems are the same. What has changed is that the transaction record is now shared and available to all parties.

A blockchain network has the following key characteristics:

- » **Consensus:** For a transaction to be valid, all participants must agree on its validity. (See Chapter 2 for more about consensus mechanisms.)
- » **Provenance:** Participants know where the asset came from and how its ownership has changed over time.
- » **Immutability:** No participant can tamper with a transaction after it's been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible.
- » **Finality:** A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

Exploring a blockchain application

Car companies make leasing a vehicle look easy, but in reality, it can be quite complicated. A significant challenge faced by today's car leasing networks is that even though the physical supply chain is usually integrated, the supporting systems are often fragmented. Each party within the network maintains its own ledger, which can take days or weeks to synchronize (see Figure 1-2).

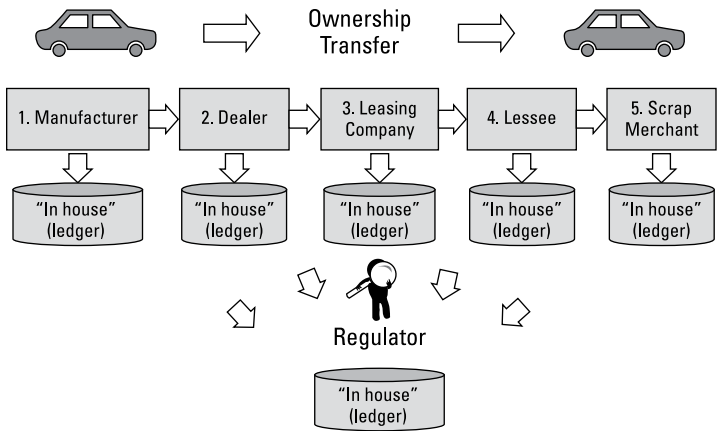


FIGURE 1-2: Tracking vehicle ownership without blockchain.

By using a shared ledger on a blockchain network, every participant can access, monitor, and analyze the state of the vehicle irrespective of where it is within its life cycle (see Figure 1-3).

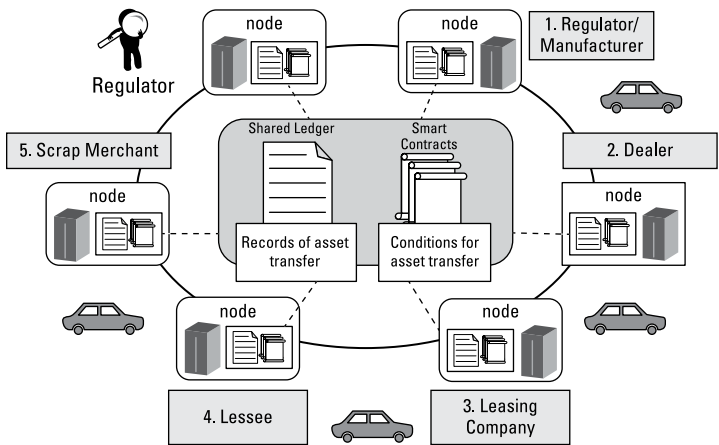


FIGURE 1-3: Tracking vehicle ownership with blockchain.

With blockchain, network participants can interact as follows:

- 1. The government regulator creates and populates the registration for the new vehicle on the blockchain and transfers the ownership of the vehicle to the manufacturer.**

2. **The manufacturer adds the make, model, and vehicle identification number to the vehicle template within the parameters allowed by the *smart contract* (a digital agreement or set of rules that govern a transaction — see Chapter 2 for details).**
3. **The dealer can see the new stock availability, and ownership of the vehicle can be transferred from the manufacturer to the dealership after a smart contract is executed to validate the sale.**
4. **The leasing company can see the dealer's inventory.**
Ownership of the vehicle can be transferred from the dealer to the leasing company after a smart contract is executed to validate the transfer.
5. **The lessee can see the cars available for lease and complete any form required to execute the lease agreement.**
6. **The leasing process continues between various lessees and the leasing company until the leasing company is ready to retire the vehicle.**

At this point, ownership of the asset is transferred to the scrap merchant, who, according to another smart contract, has permission to dispose of the vehicle.

Recognizing the key business benefits

For business, blockchain has the following specific benefits:

- » **Time savings:** Transaction times for complex, multi-party interactions are slashed from days to minutes. Transaction settlement is faster, because it doesn't require verification by a central authority.
- » **Cost savings:** A blockchain network reduces expenses in several ways:
 - Less oversight is needed because the network is self-policed by network participants, all of whom are known on the network.
 - Intermediaries are reduced because participants can exchange items of value directly.
 - Duplication of effort is eliminated because all participants have access to the shared ledger.

» **Tighter security:** Blockchain's security features protect against tampering, fraud, and cybercrime. If a network is permissioned, it enables the creation of a members-only network with proof that members are who they say they are and that goods or assets traded are exactly as represented.



TIP

Not all blockchains are built for business. Some are permissioned while others aren't. A permissioned network is critical for a blockchain for business, especially within a regulated industry. It offers

- » **Enhanced privacy:** Through the use of IDs and permissions, users can specify which transaction details they want other participants to be permitted to view. Permissions can be expanded for special users, such as auditors, who may need access to more transaction detail.
- » **Improved auditability:** Having a shared ledger that serves as a single source of truth improves the ability to monitor and audit transactions.
- » **Increased operational efficiency:** Pure digitization of assets streamlines transfer of ownership, so transactions can be conducted at a speed more in line with the pace of doing business.

Chapter 2 goes into more detail on what makes a blockchain network ideal for business.

Building trust with blockchain

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with; it's that you don't need to when operating on a blockchain network.

Blockchain is particularly valuable at increasing the level of trust among network participants. Because every transaction builds on every other transaction, any corruption is readily apparent, and everyone is made aware of it. This self-policing can mitigate the need to depend on the current level of legal or government safeguards and sanctions to monitor and control the flow of business transactions. The community of participants does that.

Where third-party oversight is required, blockchain reduces the burden on the regulatory system by making it easier for auditors and regulators to review relevant transaction details and verify compliance.

Blockchain builds trust through the following five attributes:

- » **Distributed and sustainable:** The ledger is shared, updated with every transaction, and selectively replicated among participants in near real time. Because it's not owned or controlled by any single organization, the blockchain platform's continued existence isn't dependent on any individual entity.
- » **Secure, private, and indelible:** Permissions and cryptography prevent unauthorized access to the network and ensure that participants are who they claim to be. Privacy is maintained through cryptographic techniques and/or data partitioning techniques to give participants selective visibility into the ledger; both transactions and the identity of transacting parties can be masked. After conditions are agreed to, participants can't tamper with a record of the transaction; errors can be reversed only with new transactions.
- » **Transparent and auditable:** Because participants in a transaction have access to the same records, they can validate transactions and verify identities or ownership without the need for third-party intermediaries. Transactions are time-stamped and can be verified in near real time.
- » **Consensus-based and transactional:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms. Each blockchain network can establish the conditions under which a transaction or asset exchange can occur.
- » **Orchestrated and flexible:** Because business rules and smart contracts (that execute based on one or more conditions) can be built into the platform, blockchain business networks can evolve as they mature to support end-to-end business processes and a wide range of activities.

IN THIS CHAPTER

- » Breaking down the “blockchain” concept
- » Understanding what makes a blockchain network suitable for business
- » Checking out the network participants and the roles they play

Chapter 2

Taking a Look at How Blockchain Works

While Chapter 1 gives you a general understanding of what blockchain is and an appreciation of what it can do, you may be wondering how it works. In this chapter, I tackle that topic by taking you behind the scenes of a blockchain network without getting overly technical.

Here, you get a glimpse of how blockchain stores transactions in a way that prevents recorded transactions from being changed. You discover the four concepts that form the foundation of a blockchain for business, and you meet the network participants and find out about the various roles they play.

Why It’s Called “Blockchain”

Blockchain owes its name to the way it stores transaction data — in *blocks* that are linked together to form a *chain* (see Figure 2-1). As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed on by the network participants.

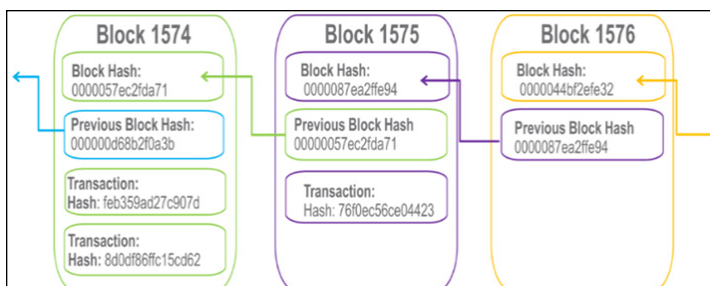


FIGURE 2-1: Blockchain stores transaction records in a series of connected blocks.

Each block contains a *hash* (a digital fingerprint or unique identifier), timestamped batches of recent valid transactions, and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain. The method renders the blockchain tamper-evident, lending to the key attribute of immutability.



To be clear, while the blockchain contains transaction data, it's *not* a replacement for databases, messaging technology, transaction processing, or business processes. The blockchain contains verified proof of transactions. However, while blockchain essentially serves as a database for recording transactions, its benefits extend far beyond those of a traditional database.

What Makes a Blockchain Suitable for Business?

Instead of having a blockchain that relies on the exchange of cryptocurrencies with anonymous users on a public network (as is the case with bitcoin), a blockchain for business is a private, permissioned network with known identities and without the need for cryptocurrencies.

To further understand how a blockchain for business works, and to appreciate its potential for revolutionizing business networks, you need to understand the four key concepts of blockchain for business, shown in Figure 2-2.

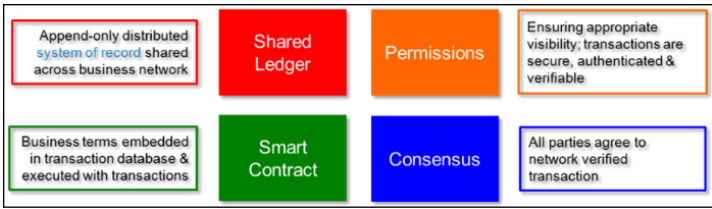


FIGURE 2-2: The key concepts of blockchain for business.

These four concepts are explained in this section.

Shared ledger

Ledgers are nothing new; they've been used in double-entry bookkeeping since the 13th century. What is new is the concept of a shared, distributed ledger — an immutable record of all transactions on the network, a record that all network participants can access. With a shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks. The shared ledger has the following characteristics:

- » Records all transactions across the business network; the shared ledger is *the* system of record, the single source of truth.
- » Is shared among all participants in the network; through replication, each participant has a duplicate copy of the ledger.
- » Is permissioned, so participants see only those transactions they're authorized to view. Participants have identities that link them to transactions, but they can choose the transaction information that other participants are authorized to view.

Permissions

Blockchains can be permissioned or permissionless. With a permissioned blockchain, each participant has a unique identity, which enables the use of policies to constrain network participation and access to transaction details. With the ability to constrain network participation, organizations can more easily comply with data protection regulations, such as those stipulated in the Health Insurance Portability and Accountability Act (HIPAA). Permissioned blockchains are also more effective at controlling the consistency of the data that gets appended to the blockchain.

With the ability to restrict access to transaction details, more transaction detail can be stored in the blockchain, and participants can specify the transaction information they're willing to allow others to view. In addition, some participants may be authorized to view only certain transactions, while others, such as auditors, may be given access to a broader range of transactions. (With a public blockchain, the level of transaction detail may be limited to protect confidentiality and anonymity.)

For example, if Party A transfers an asset to Party B, both Party A and Party B can see the details of the transaction. Party C can see that A and B have transacted but can't see the details of the asset transfer. If an auditor or regulator joins the network, privacy services can ensure that they see full details of all transactions on the network. Cryptographic technology — this time through the use of *digital certificates* — makes this possible.

Just like a passport, a digital certificate provides identifying information, is forgery resistant, and can be verified because it was issued by a trusted agency. The blockchain network will include a certification authority who issues the digital certificate.

Consensus

In a business network where participants are known and trusted, transactions can be verified and committed to the ledger through various means of *consensus* (agreement), including the following:

- » **Proof of stake:** To validate transactions, validators must hold a certain percentage of the network's total value. Proof-of-stake might provide increased protection from a malicious attack on the network by reducing incentives for attack and making it very expensive to execute attacks.
- » **Multi-signature:** A majority of validators (for example, three out of five) must agree that a transaction is valid.
- » **Practical Byzantine Fault Tolerance (PBFT):** An algorithm designed to settle disputes among computing *nodes* (network participants) when one node in a set of nodes generates different output from the others in the set.



REMEMBER

Blockchain for business features *pluggable consensus* — a way to implement whichever consensus mechanism is deemed best for any given industry segment.

PROOF OF WORK: AN UNNECESSARY EXPENSE FOR A BLOCKCHAIN FOR BUSINESS

When participants are anonymous (such as in the bitcoin world), commitment is expensive. On the bitcoin network, consensus is reached through *proof of work*. The network challenges every machine that stores a copy of the ledger to solve a complex puzzle based on its version of the ledger. Machines with identical copies of the ledger “team up” to solve the puzzle they’ve been given. The first team to solve the puzzle wins, and all other machines update their ledgers to match that of the winning team. The idea is that the majority wins because it has the most computing power to solve its puzzle first.

Proof of work is useful on a public blockchain, such as the one used for bitcoin, but it consumes considerable computing power and electricity, making it an expensive way to reach consensus. Such an expense is unnecessary on a private business network where all participants are known.

Smart contracts

A *smart contract* is an agreement or set of rules that govern a business transaction; it’s stored on the blockchain and is executed automatically as part of a transaction. Smart contracts may have many contractual clauses that could be made partially or fully self-executing, self-enforcing, or both. Their purpose is to provide security superior to traditional contract law while reducing the costs and delays associated with traditional contracts.

For example, a smart contract may define contractual conditions under which corporate bond transfer occurs or it may encapsulate the terms and conditions of travel insurance, which may be executed automatically when, for example, a flight is delayed by more than six hours.

Identifying Participants and Their Roles

Various participants on a blockchain network play a role in its operation. Following are descriptions of each of the participants:

- » **Blockchain user:** A participant (typically a business user) with permissions to join the blockchain network and conduct transactions with other network participants. Blockchain technology operates in the background, so the blockchain user has no awareness of it. There are typically multiple users on any one business network.
- » **Regulator:** A blockchain user with special permissions to oversee the transactions happening within the network. Regulators may be prohibited from conducting transactions.
- » **Blockchain developer:** Programmers who create the applications and smart contracts that enable blockchain users to conduct transactions on the blockchain network. Applications serve as a conduit between users and the blockchain.
- » **Blockchain network operator:** Individuals who have special permissions and authority to define, create, manage, and monitor the blockchain network. Each business on a blockchain network has a blockchain network operator.
- » **Traditional processing platforms:** Existing computer systems that may be used by the blockchain to augment processing. This system may also need to initiate requests into the blockchain.
- » **Traditional data sources:** Existing data systems that may provide data to influence the behavior of smart contracts and help to define how communications and data transfer will occur between traditional applications/data and the blockchain — via API calls, thru MQ style cloud messaging, or both.
- » **Certificate authority:** An individual who issues and manages the different types of certificates required to run a permissioned blockchain. For example, certificates may need to be issued to blockchain users or to individual transactions.

IN THIS CHAPTER

- » Recognizing blockchain's potential for eliminating market friction
- » Working toward friction-free business networks
- » Harnessing the transformative power of increased visibility

Chapter 3

Propelling Business with Blockchains

Global trade has been the single greatest creator of wealth in human history, and market friction the greatest obstacle to wealth. Over the years, businesses have overcome multiple sources of friction. Institutions and instruments of trust emerged to reduce risk in business transactions. Technology innovations helped overcome distances and inefficiencies. Still, many business transactions remain inefficient, expensive, and vulnerable.

Blockchain technology has the potential to remove much of the remaining *market friction* — the speed bumps that throttle the pace of business. As friction dissipates, a new science of organization will emerge, revolutionizing the way industries and enterprises are structured. With transparency the norm, a robust foundation for trust can become the springboard for further ecosystem evolution. Participants and assets once shut out of markets can join in, unleashing an accelerated flow of capital and unprecedented opportunities to create wealth.

Recognizing Types of Market Friction

Market friction is anything that impedes the exchange of assets — anything that adds costs or delays, such as taxes, regulations, bureaucracy, fraud, the involvement of intermediaries, delays in executing contracts, and so on. Various types of market friction impact different industries in different ways and to varying degrees, and they remain a drag on global business and trade, slowing business or even stopping it cold. In this section, you find out about the common types of market friction that blockchain is capable of alleviating.

Information frictions

Information frictions result from the following limitations:

- » **Imperfect information:** Participants in a transaction don't have access to the same information, giving one party an unfair advantage. Information may also be incorrect or inconsistent, leading to bad decisions or delays while reconciling it.
- » **Inaccessible information:** The potential value of abundant data and information is greatly constrained by the technical challenges of storing, processing, sharing and analyzing it. As a result, much information is not collected or remains inaccessible.
- » **Information risks:** Technological risks to information, from hacking to cybercrime and privacy concerns to identity theft are on the rise. These incur growing costs, as well as damage to brand reputations.

Interaction frictions

Interaction frictions arise when either the cost of transaction is too high or the degree of separation (physical or otherwise) between parties is too great. Business transactions that take days and are costly to manage via intermediaries are prime candidates for disruption by nimbler competitors.



REMEMBER

Interaction frictions are often magnified by the number of interactions required. Blockchain's peer-to-peer architecture can often reduce the number of interactions or parties required to execute a transaction, thus reducing the number of potential sources of interaction friction.

Innovation frictions

Innovation frictions are any conditions, internal or external, that compromise an organization's ability to respond to market changes, such as the following:

- » **Institutional inertia:** Internal bureaucracy and legacy systems along with the natural human resistance to change can impede a company's responsiveness.
- » **Restrictive regulations:** While regulations may be required to control industry behavior, they have the side effect of introducing costs and delays.
- » **Invisible threats:** New competitive business models made possible by new technologies are threats for which organizations can't plan. For many, this growing uncertainty will disrupt continued business success. Both small organizations and nimble larger ones will try new approaches, and though many will fail, some will redefine entire industries.

Moving Closer to Friction-Free Business Networks

In every century, innovations have chipped away at the sources of friction — the inefficiencies stifling progress. The first letters of credit established a new basis for trust in the 14th century. The telephone delivered real-time voice communication over great distances. The Internet threw into hyper-drive what was once a slow march to dissipate friction. Technologists and economists alike began to anticipate a world that was friction-free. Friction, in theory, could be “digitized away.”

The Internet did flatten some frictions, such as transaction costs. And while it has ameliorated some forms of imperfect information, it has not resolved the issue completely. The frictions that

remain are consequential. Indeed, they have become the basis for competition as start-ups race to capitalize on their destruction.

At the same time, other frictions have grown. Conflicting cross-border regulations throttle globalization. New threats such as cyber-attacks are costly to prevent and even more expensive to recover from. Ecosystems are choked by intermediaries ready to take their cuts. The good news is that a new technology — blockchain — holds the promise of eliminating or at least significantly reducing these remaining frictions.

Reducing information friction

Uncertainty over the information needed to make business decisions often acts as a barrier to business. Blockchain has several properties that reduce information friction, including the following:

- » **Shared ledger:** Blockchains shift the paradigm from information held by a single owner to a shared lifetime history of an asset or transaction. Participants can validate transactions and verify identities and ownership without the need for third-party intermediaries. All relevant information can be shared with others based on their roles and access privileges.
- » **Permissions:** A blockchain for business network can be set up as a members-only club, where every participant has a unique identity, and participants must meet certain criteria to conduct transactions. Participants can conduct transactions confident that the person they're dealing with is who she claims to be.
- » **Cryptography:** Advanced encryption, along with permissions, ensures privacy on the network, preventing unauthorized access to transaction details and deterring fraudulent activity.
- » **Consensus:** Ensures that all transactions are validated before being appended to the blockchain, and the blockchain itself is highly tamper-resistant.

Easing interaction friction

Blockchain is particularly well-equipped to reduce interaction friction because it removes the barriers between participants in a transaction. Blockchain properties that reduce interaction friction include the following:

- » **Shared ledger:** Asset ownership can be transferred between any two participants on the network, and the transaction recorded to the shared ledger.
- » **State-based communication:** Today, banks communicate via secure messaging architecture, such as SWIFT, to accomplish tasks, with each bank maintaining its state of the task locally. With blockchain, banks can send messages that represent the shared state of the task on the blockchain, with each message moving the task to the next state in its life cycle.
- » **Peer-to-peer (P2P) transactions:** On a blockchain for business network, participants exchange assets directly, without having to process the transaction through intermediaries or a central point of control, thus reducing the costs and delays associated with the use of intermediaries.
- » **Consensus:** In place of intermediaries, blockchain uses consensus algorithms to validate and authorize transactions. Participants can conduct business at a pace that is more in-line with the pace of their business decisions.
- » **Smart contracts:** Smart contracts eliminate the hassles and delays inherent in contracts by building the contract into the transaction. Through smart contracts, the blockchain establishes the conditions under which a transaction or asset exchange can occur. No more faxing or emailing documents back and forth for review, revision, and signatures.

Easing innovation friction

Innovation friction is possibly the most difficult to overcome through technology alone, but blockchain can help in the following ways:

- » **Eliminate the cost of complexity:** As an organization's operations become increasingly complex, its growth results in diminishing returns. Blockchains have the potential to eradicate the cost of complexity and ultimately redefine the traditional boundaries of an organization.
- » **Reduce costs and delays of regulatory processes:** Automation can't entirely eliminate governance through regulation, but it can lower the costs and reduce delays inherent in regulatory processes.

» **Expand opportunities:** Blockchain can be both good and bad for businesses by providing the technology that enables businesses to develop new competitive business models. Some businesses will fail, while others redefine entire industries.

For more insight into how market frictions can be reduced or eliminated, read the study from the IBM Institute of Business Value at ibm.biz/blockchainstudy.

Transforming Ecosystems through Increased Visibility

By improving visibility, blockchain has the potential to transform entire ecosystems. Supply chains are prime examples of blockchain's potential for transformation that spans industries. Initial blockchain efforts could have quick impact by transforming even a small portion of the supply chain, such as the information used during importing. If import terminals received data from bills of lading earlier in the process, terminals could plan and execute more efficiently and without privacy concerns. Blockchain technology could make appropriate data visible in near real-time (for example, the departure time and weight of containers) without sharing information about the owners or value of the cargo. Costly delays and losses due to missing paperwork would be avoided.

On a grander scale, blockchains could enable a robust and secure exchange for shared logistics, coordinating a vast array of activities from sharing spare space in a warehouse to optimizing truck fleets and shipping containers. Retailers and manufacturers could greatly improve demand forecasting and stock replenishment. Financial institutions, armed with a detailed track record of a supplier's reliability, could extend much needed credit to fuel growth. Regulators could trace the origin of goods from raw materials, making it easier to identify counterfeit items, as well as sources of tainted materials.

Chapter 4 provides examples of more specific use cases in which you can utilize blockchain technology.

IN THIS CHAPTER

- » Considering various implementations of blockchain in business
- » Appreciating blockchain's transformative power across industries
- » Envisioning how blockchain may streamline business in your industry

Chapter 4

Blockchain in Action: Use Cases

One of the best ways to understand blockchain, appreciate its potential, and determine whether blockchain may be able to improve the way your organization conducts business is to look at potential use cases for blockchain. In this chapter, I present a number of use cases across a wide variety of industries.



REMEMBER

The use cases in this chapter only scratch the surface of the potential for blockchain technology. As the technology matures, this list will grow. You can find the latest use case examples at www.ibm.com/blockchain/for-business.html.

Financial Services

The financial services industry has several exemplary use cases for blockchain.

Commercial financing

Businesses need to purchase goods and services on credit with end-to-end visibility to avoid and resolve transaction disputes.

For example, IBM Global Financing (IGF) provides financing to its global partners, which enables them to purchase goods and services from suppliers with credit approved by IBM. With over 4,000 partners and suppliers all using different and often incompatible systems, IBM moved all the information to the blockchain and presented it to users as a distributed ledger.



TIP

The benefits of implementation are

- » Complete visibility of the order-to-delivery pipeline
- » Reduction in number of disputes filed
- » Reduction in the time required to resolve disputes

Trade finance

Businesses need a way to streamline the process of obtaining approvals from multiple legal entities (customs, port authorities, trucking or rail transportation firms, and so on) for the movement of goods across borders. The blockchain can be used by the legal entities to sign all approvals, and it keeps all parties informed regarding the approval status, when goods are received, and when payment is transferred from the importer's to the exporter's bank.



TIP

The benefits for trade finance include the following:

- » Complex processes simplified into a single process, all accessing a shadow ledger
- » Increased access to capital, because it's not caught up in long settlement times or errors and disputes
- » Increased trust and accountability among enterprises, regulators, and consumers

Cross-border transactions

Banks need a way to manage *nostro/vostro* accounts. *Nostro* (ours) refers to an account a domestic bank holds in a foreign bank in the foreign country's currency. *Vostro* (yours) is how the foreign bank refers to that account. Such accounts are used to facilitate and simplify trade and foreign exchange transactions through reconciliation. *Nostro/vostro* accounts can become stored account transactions on a blockchain to dramatically improve transparency and efficiency through automated reconciliation of accounts.



TIP

The benefits include

- » The ability to manage transactions across all of a bank's vostro/nostro accounts through a single interface
- » Greater visibility of transaction status, current balance, and tracking over time
- » Consistent, timely, and accurate picture across all nostro/vostro accounts

Insurance

The insurance industry can also use blockchain.

Insurance providers need an efficient way to process claims, verify that an insurable event (such as an accident) actually occurred, and provide customers with fair and timely payouts. With automated insurance claim processing, policy conditions are written into a smart contract stored on the blockchain and connected to publicly available data via the Internet. Whenever an insurable event occurs and is reported by a trusted source, the insurance policy is automatically triggered, the claim is processed according to the terms of the policy specified in the smart contract, and the customer is paid.



TIP

The benefits for insurance are as follows:

- » Eliminates the cost of processing insurance claims
- » Reduces the opportunity for insurance fraud
- » Improves customer satisfaction

Government

A considerable amount of government involves recording transactions and tracking ownership of assets, all of which can be made more efficient and transparent through the use of blockchain.

Establishing trusted identity remains a problem due to forgery and expensive background checks required in verification. Millions of people worldwide may have forged their identity documentation

and may not be exactly who they say they are. Millions upon millions of refugees and their children go undocumented. People in the poorer parts of the world may not have sufficient proof to establish identity as required by certain service providers; for example, banks typically require proof of residence or utility bills to establish identity, neither of which may exist in the developing country.

Organizations can apply blockchain by issuing digitally authenticated birth certificates that are unforgeable, time-stamped, and accessible to anyone in the world. The benefits to this include

- » Reduced costs and time in identity verification
- » Reduction in human trafficking
- » Transparency in grant allocations

Supply Chain Management

When something goes wrong with a complex “system of systems,” such as an aircraft, it’s important to know the provenance, through supply chain management, of each component, down to the manufacturer, production date, batch, and even the manufacturing machine program.

Blockchain holds complete provenance details of each component part, accessible by each manufacturer in the production process, the aircraft owners, maintainers, and government regulators.



TIP

Benefits in this category include

- » Increased trust because no single authority “owns” the provenance information
- » Increased efficiencies lead to reductions in time taken to diagnose and remedy a fault improving system utilization
- » Specific recalls rather than cross fleet/generic



ON THE
WEB

Provenance is also important in the food supply chain. To find out how blockchain can be leveraged to improve food supply chain traceability, see <http://ibm.biz/FoodSupplyChain>.

Healthcare

The healthcare industry needs a more efficient and secure system for managing medical records, pre-authorizing payments, settling insurance claims, and performing and recording other complex transactions. Blockchain promises to provide much needed relief.

Electronic medical records

Electronic medical records are currently maintained in data centers (in a cloud-like environment), and access is limited to hospital and care provider networks. Centralization of such information makes it vulnerable to security breach and can be expensive.

Blockchain holds the complete medical history for each patient, with multiple granularities of control by the patient, doctors, regulators, hospitals, insurers, and so on, providing a secure mechanism to record and maintain a comprehensive medical history for every patient.



TIP

With this in mind, the following benefits are realized:

- » Tamper-resistant means of storing medical history
- » Reduced time in resolution of insurance claims and increased efficiency in providing insurance quotes
- » Complete medical history of the patient for use by physicians for precise drug recommendations

Healthcare payments pre-authorization

The term “clinical attachments” is a concept surrounding the need for additional clinical information when a payer is adjudicating a healthcare claim. Claims are often submitted without all the required supporting detail, so payer(s) need to request additional detail, which adds costs and delays to the settlement process. Further, matching up the claims with the supporting information is challenging for all parties involved.



TIP

Blockchain can simplify this complicated and time-consuming process and automate the collection and sharing of information. Additional benefits include

- » Claims can be reviewed and paid more efficiently and quickly.
- » The system can suggest alternative services that have better coverage.

The Internet of Things (IoT)

As machines interact with one another, any relevant interactions can be reported by the machines and recorded in the blockchain to increase efficiency and accuracy and reduce costs. The trade logistics use case applies blockchain to automate IoT processes.

Currently, freight logistics involve many different parties: manufacturers, forwarders, shippers, custom agents, and insurers. Although parties often interact and depend on one another, they may have different goals and use different systems to track shipments. An IoT-enabled blockchain is used as a shared ledger to record shipping containers as they move through system. Smart contracts can be automatically updated through the IoT Foundation and can be optimized to exploit IoT-enabled international trade on blockchain.



TIP

The following benefits can be realized:

- » Greater transparency of shipment progress improves efficiency.
- » Trust grows, as all transactions are indelibly recorded.
- » Accuracy is improved and costs are cut through IoT participation.
- » Participants gain the ability to optimize and automate business processes through IoT.
- » Future vision allows for “freight autonomy.”

- » Looking at the Hyperledger vision
- » Differentiating Hyperledger and Hyperledger Fabric
- » Understanding how IBM can help developers innovate on blockchain

Chapter 5

Hyperledger, a Linux Foundation Project

Hyperledger, a Linux Foundation project, is an open source community to help advance technology and thought leadership. It is deemed an “umbrella” for developer communities building open-source blockchain and related technologies. Hyperledger was announced and formally named in December 2015 by 17 companies in a collaborative effort created to advance blockchain technology for cross-industry use in business. Now with over 130 members across the world, it is the fastest growing project in Linux Foundation history.



REMEMBER

Hyperledger is curated by the Linux Foundation, which provides tools, training, and events to scale any open source project. IBM initially contributed what was then called *Open Blockchain* and is now called *Fabric*, and arguably that is the biggest/highest profile project. Intel has contributed “Sawtooth Lake,” which is its blockchain technology that introduces Proof of Elapsed Time (PoET) consensus. Other noteworthy projects include “Iroha” (a C++ blockchain platform) and “Cello” (rapid blockchain deployment to cloud platforms). The idea is that Hyperledger rather than being a single platform (a la Ethereum) will be more akin to the Apache Project, with multiple projects under one umbrella that will be open source, freely available, and ideally have some measure of

interoperability. Read more about the theory behind Hyperledger umbrella brand at <http://ibm.biz/UmbrellaHyperledger>.

Hyperledger Vision

The vision of Hyperledger is to provide robust and efficient standards for blockchain ledger technology to facilitate mainstream commercial adoption. Future applications will involve a world with many interconnected distributed databases and blockchains, each of which will be specialized to suit the purpose of its users and will have the potential to communicate with other ledgers, as necessary.

Another goal for Hyperledger is to provide a modular blockchain technology that contains a rich, easy-to-use application programming interface (API) and numerous core modules that enable easy development and interoperability. The API must be flexible enough to allow blockchains built outside core Hyperledger to easily interact with their components and blockchains.

HYPERLEDGER AND HYPERLEDGER FABRIC: WHAT'S THE DIFFERENCE?

Hyperledger is a Linux Foundation open-source, collaborative effort to create blockchain technology suitable for the enterprise. *Hyperledger Fabric* is a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation with a modular architecture and pluggable, interchangeable services using container technology.

- Support a wide variety of industry use cases with different requirements
- Comply with statutes and regulations that exist today
- Support verified identities and private and confidential transactions
- Support permissioned, shared ledgers
- Support performance, scaling, auditability, identity, security, and privacy
- Reduce costly computations involved in proof of work

Further, Hyperledger believes that identity and patterns of behavior of any party on a network must be difficult for unauthorized parties to ascertain by inspecting the ledger. Blockchain users must be able to make certain business logic and parameters of a transaction confidential, rendering them inaccessible to anyone other than the stakeholders.

Hyperledger Fabric

Hyperledger Fabric provides a framework for developing blockchain solutions with a modular architecture, pluggable implementations, and container technology. While leveraging open-source best practices, Hyperledger Fabric enables confidentiality, scalability, and security in business environments.

Unlike other blockchain implementations like Bitcoin or Ethereum, Hyperledger Fabric fulfills all four key elements of a blockchain for business:

- » **Permissioned network:** Collectively defined membership and access rights within your business network
- » **Confidential transactions:** Gives businesses the flexibility and security to make transactions visible to select parties with the correct encryption keys
- » **Doesn't rely on cryptocurrencies:** Doesn't require mining and expensive computations to assure transactions
- » **Programmable:** Leverages the embedded logic in smart contracts to automate business processes across your network

IBM is a founding member of Hyperledger, and has donated 44k lines of blockchain code under what was originally Hyperledger Fabric. In addition to donating code, IBM

- » Supports a broad, cross-industry, and open-source approach to advance the potential for blockchain and make it mainstream
- » Believes Hyperledger will free developers across all industries to focus on building robust applications and platforms to support many different types of business transactions over the Internet

» Has invested considerable research and development efforts exploring blockchain applications for industry and has offered its code and intellectual property



REMEMBER

For blockchain to fulfill its true potential, an open-standards approach is critical so blockchain can be widely adopted, allowing innovation to flourish.



TIP

Tune in to the Hyperledger Rocket Chat Channel at chat.hyperledger.org to join the growing community of 5,000+ developers already building with Hyperledger technologies.

How Can IBM Help Developers Innovate With Blockchain?

IBM is unlocking the potential of blockchain by making it more accessible and more open. As one of the world's leading research organizations, IBM's goal is to explore new ways to advance the science of blockchain by helping remove some of the complexity, making it more accessible and open.

Offering an easily accessible cloud and development platform

Implementing blockchain solutions on IBM Cloud is the quickest way to get started. IBM has a number of cloud-based solutions to enable you to easily develop applications while testing the security, availability, and performance of a permissioned blockchain network.



REMEMBER

IBM blockchain networks are built to benefit from decentralized control, but some cloud environments are open to vulnerabilities. Working with teams of security experts, cryptographers, hardware experts, and researchers, IBM has created essential cloud services for tamper-resistant, trusted blockchain networks.

IBM Blockchain on Bluemix

With the blockchain service on Bluemix, you can create and deploy a blockchain network based on Hyperledger Fabric. IBM Blockchain on Bluemix offers a high-security plan that provides an isolated environment for business networks. The plan extends

the starter features within an isolated environment that runs in a secure infrastructure. This plan offers high levels of security that close any back doors to unauthorized access and tampering. Key features of the plan include:

- » The blockchain operating environment protects host administrators and provides proof to ensure the blockchain executes in the agreed-upon manner.
- » High evaluation assurance level enables protection across environments where blockchain peers run in isolation from other peers and parties. This prevents leaks into another party's environment.
- » Crypto-optimization supports an environment that moves hashing and the creation of digital signatures to optimized accelerators that don't drain CPU performance.
- » FIPS 140-2 (the highest Federal Information Processing Standard) supports the use of blockchain in regulated industries such as government, financial services, and healthcare.)



ON THE
WEB

For more about IBM Blockchain on Bluemix options, visit www.ibm.com/blockchain/offerings.html.

Hyperledger Fabric images on DockerHub

Alternatively, you can pull Hyperledger Fabric images directly from Docker Hub to create and manage your own local blockchain network. Set up and run a blockchain network with IBM-certified Docker Compose script and images. For more detailed instructions on how to get started, visit <http://ibm.biz/QuickStartGuide>.



TIP

After you've deployed a network, you're ready to build your first chaincode! To earn your chaincode badge, take this course: <http://ibm.biz/BlockchainChaincodeCourse>.

Individualized attention and industry expertise



TIP

If you've been reading through to this point, you may be getting excited to build on blockchain, so now you may need some help getting other members of your organization onboard. This section should help.

IBM is developing a number of blockchain solutions for clients in varied industries. IBM Bluemix Garage for Blockchain is a collaborative workshop in which you can explore blockchain use cases relevant to your business and determine your best first pilot of the technology.

The engagement model of IBM Bluemix Garage for Blockchain consists of the following three stages:

- » **Conversation and demonstration:** A 90-minute interactive session between the IBM Bluemix Garage for Blockchain team member and the client. This session is conducted preferably face to face, but web conference, videoconference, or telephone call can also work. IBM explains its blockchain point of view in business terms avoiding technical jargon; discusses what blockchain can do for business; and presents a brief, live, interactive demonstration of a use case (see Chapter 4 for some example use cases).
- » **Technology hands-on:** This one day, highly interactive face-to-face workshop dives deeper into blockchain technology. Through a combination of presentations and guided, hands-on lab exercises, IBM takes you as deep as you want to delve into blockchain technology.
- » **First project:** The first project starts with a two-day IBM Design Thinking workshop where you, together with IBM, explore the use case from an end-user viewpoint. IBM then plans an iterative agile development of a deliverable, finite-scale solution to the business challenge (use case), which is then realized through a number of short, agile development sprints. These sprints are normally conducted by a small, joint (IBM Bluemix Garage for Blockchain + Customer) team to combine our expertise on blockchain and agile with the customer's knowledge of the use case and business scenario.

As businesses start to work through blockchain strategy, planning, and implementation, IBM Global Business Services (GBS) also provides teams of trained consultants around the globe to answer your questions and begin mapping out first projects.

IN THIS CHAPTER

- » Deciding where blockchain can deliver the biggest returns
- » Choosing a representative use case and setting goals
- » Identifying a platform to build your first application
- » Engaging with your peers in a robust community

Chapter 6

Ten Steps to Your First Blockchain application

After discovering the potential transformative power of blockchain for business, you're probably eager to find out what steps you need to take toward implementing it in your business and industry. Well, you've come to the right place. Here, I present ten steps to your first blockchain application.

Deciding Whether Blockchain Has a Place in Your Industry

As you find out more about blockchain, you may discover how it's already impacting your industry, or certain applications of blockchain may seem obvious to you as solutions for addressing current challenges. If you're uncertain of whether blockchain has a place in your industry, answer the following questions:

- » Does my business network need to manage contractual relationships?

- » Do we need to track transactions that involve more than two parties?
- » Is the current system overly complex or costly, possibly due to the need for intermediaries or a central point of control?
- » Can the network benefit from increased trust, transparency, and accountability in recordkeeping?
- » Is the current system prone to errors due to manual processes or duplication of effort?
- » Is the current transaction system vulnerable to fraud, cyber-attack, and human error?

If you answered “yes” to any of these questions, blockchain is likely to benefit your industry.

Identifying Speed Bumps in Business Processes

Examine your current business processes for inefficiencies, particularly steps in the process that are prone to delays, frustration, errors, and duplication of effort. The questions in the preceding section are likely to point you in the right direction.



TIP

A more general question to ask is this: “What challenges do I currently face in my transaction networks?”

Determining How Blockchain Can Help

After identifying challenges in your transaction network, consider various attributes of blockchain that can address the inefficiencies, costs, and other issues. For example, if a lack of trust is causing friction, blockchain’s shared ledger can provide increased visibility into transaction and asset histories to improve trust. If business agreements or rules cause delays, smart contracts may be the solution. The goal here is to determine how blockchain can help overcome specific challenges.

Choosing an Appropriate Use Case

When choosing a use case, make sure it's a good fit for what you're trying to accomplish — something that adds real value as opposed to something that could be achieved just as well using a mature technology. Your use case needs to pass the following four acid tests:

- » **Consensus:** Does agreement across the business network that each transaction is valid provide some benefit?
- » **Provenance:** Is the maintenance of a complete audit trail important?
- » **Immutability:** Is it important that the train of transactions is tamper-evident?
- » **Finality:** Is there a need for an agreed “system of record” across the business network?



TIP

Try to choose a use case that is organizationally less complex, so you're not overwhelmed with complexity during your maiden voyage with blockchain.

Determining the Goal of Your Blockchain Network

After choosing an appropriate use case, outline a clear and measurable goal for your first project. What do you hope to solve or improve using blockchain technology? What can you use to measure the success of your first project in meeting that goal?

Do you want to reduce resolution times of disputes? Speed up claims processing? Free up capital flow? Reduce fraud in your network? These are just a few possible objectives a blockchain network could help achieve.

Identifying Dependencies

When you have an appropriate use case in mind, consider what else you need, in addition to internal resources you already have, to start on your first blockchain project. Do you need a services

partner to help deploy the first project? Do you need a platform or fabric that enables you to meet certain regulatory or compliance objectives? Since transaction processing is becoming a team sport, a blockchain network is most successful when multiple parties are involved and becomes even more valuable and efficient as the blockchain grows. Enterprises need to learn a new model of ecosystem-based processes so it's important to start now.

Choosing a Blockchain Provider and Platform

Choose a provider and platform that are the best fit for your industry and business needs. As you compare the suitability of different providers and platforms, seek answers to the following questions:

- » Do you require a permissioned network?
- » Do you need to know the identities in your business network? For example, to adhere to regulations such as anti-money laundering (AML) or know your customer (KYC)?
- » Do you have frequent exchanges with others that could be automated and pre-programmed, freeing up valuable time and resource?
- » Would you benefit from transaction resolution in minutes rather than days or weeks?

For help in identifying a platform that suits your needs, refer to the options in Chapter 5.

Developing and Deploying Chaincode

The next step in your first blockchain project is to develop and deploy a blockchain application and network.



For guidance on how to set up a blockchain network and start coding, see “IBM Blockchain 101: Quick-start guide for developers” at <http://ibm.biz/QuickStartGuide>.

Testing and Fine-Tuning Your Application and Network

The final stage in creating and deploying your first blockchain application is actually an ongoing process. Monitor your application and network and capture learnings to make improvements and expand into a wider deployment.



For details and documentation on how to test your blockchain network, visit <http://ibm.biz/TestNetwork>. As you deploy and test your blockchain network, the dashboard monitor is a valuable tool; for more about the dashboard monitor, visit <http://ibm.biz/DashboardMonitor>.

Joining the Hyperledger Rocket Chat Channel



Tune in to the Hyperledger Rocket.Chat Channel at chat.hyperledger.org to join the growing community already building with Hyperledger technologies. Get answers to all your questions as you build your network, discuss what you're working on with your peers, and become an integral part of the community as Hyperledger business blockchain technologies continue to evolve.

Notes

Notes

Notes

Redefine your business networks with blockchain

Blockchain For Dummies, IBM Limited Edition, helps you understand what blockchain is, how it works, and how it can enhance your business networks. Understand how this innovative technology can apply to your industry and how you can get started building on blockchain today.

Inside...

- Understand what blockchain is (and is not)
- See blockchain's business potential
- Apply blockchain to various industries
- Learn about the Hyperledger project and Fabric
- Build your first application



Manav Gupta is the CTO for IBM Cloud Canada, a published author, IBM Master Inventor, member of IBM Academy of Technology, and IBM Senior Certified IT Architect. Manav has led several first-of-a-kind projects across North America in the areas of Cloud, Big Data, and, more recently, blockchain.

Go to **Dummies.com**[®]
for videos, step-by-step photos,
how-to articles, or to shop!

for
dummies[®]
A Wiley Brand

ISBN: 978-1-119-37123-6
Part #: XIM12354USEN-00
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.