Brought to you by:

ORACLE

Enterprise Blockchain

for dummies

A Wiley Brand

Explore blockchain basics

Examine enterprise requirements for blockchain

Discover projects that leverage blockchain technology

Michael G. Solomon

Oracle Special Edition

About Oracle

Emerging technologies are disrupting old paradigms and unleashing new opportunities. Oracle has embedded innovative technologies in every aspect of our cloud, enabling companies to reimagine their businesses, processes, and experiences.

With the introduction of Oracle Autonomous Database, the industry's only self-driving, self-securing, and self-repairing database, Oracle is again revolutionizing how data is managed. Oracle is the #1 provider of business software, with a broad portfolio of solutions for companies of all sizes. Today, 430,000 customers in 175 countries use Oracle technologies to seize business opportunities and solve real, tangible challenges.

Businesses around the world have already reaped the benefits of blockchain applications built on Oracle Blockchain Platform. Companies using Oracle's business-ready blockchain have been able to move from experimentation to production by creating new blockchain applications from scratch or adding blockchain functionality to an existing solution.

For more information about Oracle (NYSE: ORCL), please visit us at **www.oracle.com**.

Enterprise Blockchain

Oracle Special Edition

by Michael G. Solomon

for dummies®
A Wiley Brand

Enterprise Blockchain For Dummies®, Oracle Special Edition

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

ISBN 978-1-119-59401-7 (pbk); ISBN 978-1-119-59402-4 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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.

Publisher's Acknowledgments

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

Project Editor: E. N. Kuball

Executive Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Tamilmani Varadharaj

Special Help: Mary Hall, Suzanne Blackstock

Table of Contents

Introduction

Welcome to *Enterprise Blockchain For Dummies*, your guide to leveraging blockchain benefits for the enterprise IT infrastructure. Blockchain technology has matured from its beginnings as a vehicle for Bitcoin and other cryptocurrencies. Today, blockchain can offer enterprises the ability to provide transparency, security, and automated transaction processing, all with lower costs and delays.

Blockchain is changing how enterprises conduct business with one another and their customers. Blockchain supply chain applications are one of the more common use cases, but blockchain enables enterprises and consortiums of organizations within industry groups to carry out transactions with untrusted parties. The ability to impart trust (via decentralized data), along with unprecedented transparency, has positioned blockchain technology as holding the promise to revolutionize business models.

At its core, blockchain technology is simply storing transactions in a shared chain of linked blocks in such a way that all participants agree before any new blocks get added. But its implications go far beyond a basic definition. Blockchain is disrupting business — in a very good way.

About This Book

Enterprise Blockchain For Dummies introduces blockchain technology, its history, the different types of blockchains, and how the technology works. You learn the differences in the generations of blockchain implementations and where each one shines. You examine blockchain benefits, how blockchain is similar to database storage, and most important, how it's very different. You survey blockchain benefits and how they can align with enterprise strategic goals.

After exploring blockchain and its main features, you read about best fit use cases for blockchain technology and how to integrate a blockchain into your own enterprise applications. Finally, you explore ten current enterprise blockchain projects and see how blockchain is already adding value in the enterprise space.

Foolish Assumptions

I wrote this book based on certain assumptions about you, the reader. First, I assume that whether you're coming from the technical or business side of things you're relatively new to blockchain. Regardless of your role, however, I assume that you're interested in finding out more about blockchain in the enterprise and its tremendous potential to disrupt status quo business operations. I also assume you want to know more about the steps you

need to take to start deploying enterprise blockchain-based solutions.

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:

The Tip icon guides you to faster, easier ways to perform a task or better ways to put blockchain to use in your enterprise.

The Remember icon highlights concepts worth remembering and other important topics.

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

Where to Go from Here

I can only cover so much in a book of this size. For even more information on blockchain in the enterprise, head to `www.oracle.com/blockchain`.

IN THIS CHAPTER

- Understanding what blockchain technology means
- Looking at the various types of blockchains
- Considering how blockchain is typically implemented

Chapter 1
Exploring Blockchain Basics

Blockchain is often called one of the most disruptive and promising technologies of our generation. In this chapter, you learn about blockchain technology and some of its most popular implementations. You learn what blockchain really is and how aligning this new technology's capabilities with enterprise goals can leverage new opportunities that may have been out of reach even a few years ago.

Defining Blockchain Technology

Blockchain technology is a revolutionary way to handle decentralized data. It's essentially a ledger of data that is copied to multiple locations, or nodes, that may not trust one another. The technology provides guarantees that the data stays the same on all nodes. This creates trust among parties transacting business, even if they don't know each other. The whole idea of blockchain is to provide data integrity guarantees without relying on a central authority. This notion may be called decentralized trust through reliable data.

Blockchain technology was originally proposed to support a new decentralized form of digital currency, called *cryptocurrency.* Because most data on the earliest blockchains were simple financial transactions, blockchain data is normally referred to as a *ledger.*

Examining blockchain structure

The name *blockchain* comes from the fact that all data gets stored in blocks, and each block is connected to the previous block, forming a chainlike structure. You can only add (append) new blocks to a blockchain, and you

can't modify the contents of any block or delete any block after it gets added to the blockchain.

Each block stores a cryptographic hash of the previous block as its link. A cryptographic hash function is a function that takes data as its input and returns a fixed-length string of characters that represents the input data. The returned value is called the *hash value.* If you make any changes to the input data and run the hash function again, you'll get a different hash value.

Hash values makes it easy to detect changes in blockchain blocks. Any change in a block "breaks" the chain by invalidating the link from the next block.

REMEMBER

Every block in the chain stores the original hash value of the previous block. Changes to any block cause that block's hash value to change, which means that the hash value stored in the next block no longer matches the current block's hash value. Any node can quickly determine if any block changed since it was added.

When a new full node joins the blockchain network, it downloads a copy of all the blocks currently on the chain. After the new node synchronizes with the other nodes and has the latest blockchain version, it receives any new blocks, just like other nodes.

TIP

There are different types of blockchain network nodes. Full nodes store a complete copy of the blockchain. Lightweight nodes only store the most recent blocks, and can request older blocks on demand when users need them.

Creating new blocks

A blockchain *transaction* is any action that writes information to the blockchain. Users submit transactions to blockchain nodes, and when there are enough transactions to warrant a new block, a node creates a new block that contains these pending transactions.

TIP

Unlike a traditional database system, blockchains only support *Read* and *Append* operations. You can only add new information to the blockchain and read whatever is already stored on the blockchain.

Although each blockchain implementation handles block creation and validation differently, they do agree on basic consensus. A simple majority of nodes (that is, one node more than half) agree that the newly created block is valid and should be added to the blockchain.

One of the more popular consensus protocols is called Proof of Work (PoW), which the Bitcoin and Ethereum blockchains use. In PoW, some nodes take new proposed blocks and compete among themselves to solve a very difficult mathematical puzzle. The winner receives a

reward for its effort. The process of solving the puzzle that results in a valid block is called *mining.* Nodes that participate in mining are called *miners.*

The process of mining in PoW involves calculating a hash value that meets specific complexity requirements. In Bitcoin, the requirement is a certain number of leading zeros in the hash value result. Miners calculate the hash value of the block and a special number, called a *nonce.* Miners try many different values for the nonce, or number used once, until they find one that meets the output complexity requirement. This difficult process results in a block that all nodes can agree on and accept as valid. Finding the right nonce is very hard, but verifying the block by calculating the block's hash value is very easy. Any node can quickly spot a bad block.

When a miner successfully mines the new block, it sends that block to all nodes and it becomes the last block on the chain.

Controlling computation

The power of blockchain is far more than just sharing data with untrusted nodes. You also can set rules that every node follows to control how users access the blockchain. You can limit how users create transactions, and even how they can view data. Smart contracts are the programs that are part of the blockchain and control access to it.

Suppose your enterprise is part of a supply chain consortium that uses blockchain technology to manage how products travel from producer to consumer. Every ownership transfer should occur only after the parties satisfy specific rules. In a blockchain environment, smart contracts define the rules that every blockchain node has to follow. No node can ignore the rules. The guarantee of mandatory compliance allows you to conduct business with entities you don't trust, because you do trust the technology.

TIP

If any node breaks the rules, the data that node writes to the blockchain would be different from what other nodes would write, creating a block inconsistency. Nodes vote on which version is correct, and the majority wins.

Because smart contract code is part of the blockchain, you can trust that the code you published is the code that everyone is running. Plus, each node guarantees that smart contract code executes the same way on all nodes. You never have to worry that one node gets a different answer from another node. All smart contract code is deterministic — you can count on the result being the same everywhere.

Describing Types of Blockchains

Blockchains are not all the same. Some blockchains are designed to be open repositories. Others store data that shouldn't be available to everyone. Different needs have given rise to different blockchain visibility models.

Public blockchains: Sharing data with the whole world

The original blockchain proposal was for a blockchain that would be shared without restriction with any node that wanted to participate in the network. Nodes do not need permission to join the blockchain network. This type of blockchain is called a *public* or *permissionless* blockchain; it's the kind of blockchain used for most types of cryptocurrencies.

Because anyone can join, there is a very low level of trust. That's why the complex consensus algorithms, such as PoW, are so important. The consensus algorithms provide trust at the technology level when no trust exists between nodes.

Private blockchains: Protecting sensitive data

It didn't take long for organizations to recognize the value of blockchains within their IT infrastructure. Blockchains provide the ability to share data that was previously locked away in silos. Although there is some level of trust among users within the organization, separate organizational units may not completely trust one another. A *private* or *permissioned* blockchain allows organizations to apply access controls to the blockchain and still provide the ability to share data in a semi-trusted environment. A permissioned blockchain provides a way to limit access only to users who have been granted access to the data.

Hybrid blockchains: Striking a balance between public and private

Some applications that are good fits for blockchain technology are neither completely public nor private. In a supply chain, a group of unrelated participants work together to get products from a producer to a consumer. There may be many participants in the supply chain that are not part of the same organization. Shared supply chain data has value to participants and competitors.

This type of use case benefits from a *hybrid* or *consortium* blockchain. A hybrid blockchain is one that is semi-private, in that some meta-organization manages access controls to limit which organizations can participate. Only members of the supply chain consortium can gain access to the blockchain. Authorized participants can access data much like accessing a public blockchain.

Comparing Popular Blockchain Implementations

Blockchain technology is in its third generation. Each generation evolved to address rapidly expanding demands. From cryptocurrency to enterprise-scale applications, blockchain can offer a wide range of benefits.

Making digital currency work

The first generation of blockchain technology started in October 2008, when Satoshi Nakamoto published a paper titled "Bitcoin: A Peer-to-peer Electronic Cash System." The paper proposed the Bitcoin cryptocurrency and the blockchain technology to make it possible.

No one really knows who Satoshi Nakamoto is. The name is either a pseudonym for one person, or possibly a group of people.

The first generation of blockchain specifically supported cryptocurrency. It had limited functionality beyond managing cryptocurrency transfer transactions.

Providing computation control

In late 2013, Vitalik Buterin published an updated blockchain implementation proposal. Buterin's blockchain, Ethereum, extended the features of the Bitcoin blockchain by extending Bitcoin's limited scripting capability.

Ethereum is an open-source blockchain project that supports a complete language that allows for complex programs, called *smart contracts.* Smart contracts support comprehensive controls that govern transactions. The addition of smart contracts, along with the availability of the Ethereum code, launched the second generation of blockchain — the computation control generation.

Scaling to meet enterprise needs

From the very beginning of the blockchain boom, forward-thinking enterprises recognized the potential of blockchain but also saw scaling issues. One of the foundational design features of blockchain is its transparency and consensus algorithms. Making all data available to all users is good for public data sharing, but it makes placing an organization's sensitive data on a blockchain

problematic. For example, how can an organization comply with privacy regulations if it places private data on a public blockchain?

In late 2015, the Linux Foundation launched the Hyperledger project, with support from high-profile technology and software companies, as well as academic institutions. The main purpose of the Hyperledger project is to develop open-source blockchain implementations that address enterprise goals and scale to meet enterprise operational requirements.

This third generation of blockchain technology means blockchain is no longer just a cryptocurrency or small-scale solution. Blockchain technology has matured in a very short span of time to take its place in the enterprise IT infrastructure to address strategic goals.

IN THIS CHAPTER

- Processing and storing data with blockchain technology
- Mapping blockchain benefits to business goals
- Building modular blockchain solutions

Chapter 2
Evaluating How Well Blockchain Fits Your Needs

Blockchain technology offers some impressive benefits, including transparency, security, resilience, traceability, and potentially reduced overall operational costs. But, contrary to the hype, blockchain technology doesn't solve every problem enterprises encounter.

One of the most important factors when considering blockchain technology is whether it's a good solution for the problems your organization faces. When it is a good fit, blockchain technology offers benefits that are difficult or impossible to realize in other ways. When it isn't a good fit, blockchain technology can end up costing time and money that may be better invested in traditional approaches. It's important to plan carefully for blockchain and really consider if you have the resources and skills in house or if additional help will be needed.

In this chapter, you determine whether blockchain technology is a good fit or whether another approach would be more prudent. This determination alone can be the difference between a project's success or its failure.

Summarizing Blockchain Benefits for Processing and Storing Data

A blockchain solution is often considered to be an alternative to a database. In the simplest comparison, both technologies store persistent data that multiple users can access. Although there are features that both technologies provide, don't consider one to be a direct replacement for the other. Each technology has its own benefits and drawbacks. A blockchain solution may be a good fit if its benefits address problems that other technology just can't.

Describing blockchain benefits

One of the primary benefits of blockchain technology is transparency. Many existing technology solutions require data isolation. To ensure data integrity and confidentiality, access to the data is limited. This approach to limiting access to data does provide security, but at the expense of transparency.

Blockchains rely on consensus protocols and the blockchain design itself to provide data integrity. Removing some of the access restrictions means that persistent data can be used by more people, which leads to more fully leveraging data's value to the organization. Converting data's potential value into kinetic value through transparency can decrease administrative workflow and costs, and can support more fine-grained revenue-producing activities.

Enterprises can protect data confidentiality on a blockchain environment as well. Public blockchains rely on encryption and key management to protect confidentiality. On the other hand, private blockchains have more options. Because private blockchains have a governing authority, they can implement sophisticated fine-grained access controls and key management for encrypted data.

Another benefit of blockchain technology is the property that existing blocks are not allowed to change. Assurance that every block's initial state is maintained makes auditing and investigations easier and more reliable. If you

need to access and trust historical data, a blockchain will do that very well.

TIP

Many people say that blockchains are immutable, but that isn't technically accurate. Any user that can access the physical blocks in a blockchain can change its data. Of course, that would change the hash of the block, which invalidates the link from the previous block and every successive block. Blockchains are tamper-resistant and tamper-evident, but not technically immutable.

Comparing blockchain to database storage

Database management systems have been around for several decades, and have matured a lot in that time. If your only goal is to provide the highest performance with respect to transaction processing, a database solution may be the right choice. However, today's databases rely on a central authority to ensure proper access control. Only users to which the central authority grants access can read from or write to the database.

However, even with centrally governed access control, there is no consensus for database modifications. Any single bad actor that acquires access authority can corrupt database data. That means the entire database's

confidentiality and integrity depends on the central access granting authority being right 100 percent of the time.

A key feature of blockchain technology is a consensus mechanism that requires more than just a simple yes/no decision of a central authority. Consensus basically means that participants cannot arbitrarily add data to the blockchain. All participating parties must agree that any new data is valid before it's allowed on the blockchain. A consensus mechanism is a set of rules that all participants agree to which means that it's very hard for a malicious actor to put bad data on a blockchain.

Leveraging blockchain trust and transparency

One of the general application domains with which blockchain tends to fit well is environments that track changes of ownership among participants with limited trust. One of the classic blockchain example use cases is supply chain. A supply chain application tracks products as they travel from producer to consumer. The Oracle Blockchain App for Intelligent Track and Trace securely records business transactions across the supply chain. The Oracle Blockchain App uses fine-grained access control to provide track-and-trace reporting, insights, and analytics based on the trading partner's privileges on the network.

Blockchain technology's hallmark benefit of providing trust in an untrusted environment provides value to many types of applications, including supply chain, retail, and finance. Each participant in the blockchain network can rely on the technology to trust transactions, instead of having to trust other participants. Every participant accepts and enforces the same rules for adding data to the blockchain, and also agrees that consensus among a majority of participants results in confidence that all new blockchain data is valid.

A further boost of trust among all participants lies in the fact that all blockchain data persists in its original state. Any blockchain network node that can access blockchain data can also verify the validity of all historical data. If a rogue node were able to corrupt a block, that malicious act would be almost immediately known and quickly rectified.

Aligning Blockchain Features to Business Needs

Blockchain benefits can be great, but they don't mean much if they don't align with your organization's needs. The best indicator of whether your organization really needs a blockchain solution is determining if blockchain can solve your key business challenges.

Looking at a transparent blockchain

Blockchain data is available to all authorized users. For public blockchains, that means anyone can access blockchain data. For private blockchains, only authorized users can access blockchain data.

Regardless of the permission model, blockchain generally exposes data to more users than traditional database systems do. This transparency empowers more checks and balances among participants. And it generally allows more users to access the data, making it available for more uses.

Trusting blockchain data

A central design feature of blockchain technology is that the nodes all participate in the process of determining when new blocks get added to the chain. All nodes on a blockchain network agree on the consensus algorithm in use, and a majority of nodes must agree before any new block gets added to the chain. Majority consensus results in a higher level of confidence that all blockchain data is verifiably legitimate. Unless all participants agree and provide consent, blockchain data never changes. In the absence of consent to change, which can be difficult to obtain, data can only be appended to the blockchain.

Another central design feature of blockchains is the ease of block verification. After a block is added to the chain, nodes routinely verify that blocks remain valid. This provides an unmatched level of confidence in data integrity and validity. Blockchain trust is a core feature that aligns with any enterprise need for positive data consistency. Use cases that require consistency include any auditable transactions and record of compliance.

Tracing blockchain data history

Beyond trusting data, blockchain design requires that blocks remain unchanged, automatically providing an audit trail of data history. Traditional database management systems support updating data in place. That means you can overwrite any data record and essentially lose any previous data values. Auditors often place requirements on apps to keep a record of all previous data values. Blockchains automatically do this. Tracing the history of data involves simply traversing the blockchain.

This design feature makes it easy to audit transaction history. Because any changes to data require a new block with the modified data, auditors and investigators can trace the progression of data updates with ease. This benefit makes it easy to track behavior changes over time for any entity that blockchain data represents, and makes blockchain an attractive technology for regulatory compliance.

Ensuring blockchain resilience

Many of today's enterprise database application environments must resort to external measures to provide redundancy. Because databases rely on centrally stored data, enterprises commonly employ high-throughput mechanisms to replicate their databases. Replicated database data provides secondary copies of mission-critical data to protect an organization if the primary copy becomes unavailable.

Blockchain technology relies on the distribution of the entire verified blockchain among multiple nodes in the network. This basic design feature means that there is never a single copy of the blockchain. Plus, there is no single point of failure. If any node in the blockchain network fails or is unable to access the blockchain, other nodes in the network can continue to operate normally. This assurance guarantees that the blockchain data is available as long as at least one node in the blockchain network remains operational.

Determining If Blockchain Technology Makes Sense

With a better understanding of blockchain technology's benefits, you're better positioned to decide if blockchain is right for your enterprise. But how do you make that decision? Blockchain technology isn't a simple technology

that fits some scenarios and doesn't fit others. Enterprise blockchain is a system of components tightly integrated to satisfy the design goals of transparency, trust, traceability, and resilience.

Deciding whether a blockchain makes sense for your enterprise is a process, not a single question. In 2017, Karl Wust and Aurther Gervais published a paper titled "Do you need a blockchain?" (`https://eprint.iacr.org/2017/375.pdf`), which succinctly describes the characteristics to determine if blockchain is a fit for your organization by asking six questions. Each question helps to focus on whether the use case in question is better served by traditional solutions or a blockchain.

Storing state data

The first qualifying question is whether the application needs to store state data. Blockchain supports storing attributes that define each state of a system. That differs from traditional databases that just store the latest copy of data. If your application doesn't need to store the system's state and the history of state changes, you may not need to use a blockchain. If you do require the ability to store the current state of a system and all changes to that state, a blockchain does that.

Supporting multiple writers

One of the advantages of blockchain is that it allows users of multiple nodes to submit transactions that are stored in blocks. If your application requires a centralized writing agent, as opposed to multiple users who can write data, a blockchain is probably not the best choice. One of the strengths of blockchain is its ability to allow multiple users to submit transaction data to be added to the chain.

Eliminating a centralized access admin

Traditional database applications often rely on a trusted third party (TTP) to manage access rights. The TTP not only grants access permission, but also determines if data submitted for storage is valid. Blockchain was specifically designed to allow multiple nodes to write data to the blockchain, without trusting other nodes.

The blockchain technology design provides trust in the validity of all data, without trusting the node that submitted it. And, this trust in technology occurs without the need for a TTP. If your application requires a TTP to manage data access, a blockchain may not be a good fit. On the other hand, if eliminating a TTP is a design goal for your application, blockchain may be a good choice.

Allowing untrusted writers

Some applications require knowledge of user identities, but those users don't trust each other. For example, many enterprises maintain separate databases and applications for distinct business units. Human resources users may not trust manufacturing shop floor users with their data. Blockchain supports applications that engage users who lack complete trust in one another.


TIP

If your application requires that known but untrusted users work together, a private blockchain may be a good solution.

A private blockchain does have a TTP, but the TTP in this role serves to associate identities with addresses and limit access to the blockchain to authorized identities. The TTP in this scenario doesn't impose granular access controls — it only determines which identities can write to the blockchain. The blockchain's consensus protocol ensures that any write provides valid data for the blockchain, and the TTP can manage encryption keys to provide confidentiality.

Allowing unknown writers

One drawback of moving away from a TTP is a loss of trust and awareness of other participants' identities. Each participant in a blockchain network has an address,

but that's just a truncated public key. An address reveals nothing about the true identity of the address owner.

Allowing untrusted writers is one thing, but allowing unknown writers raises a whole new set of concerns. In traditional applications, writers would be required to register their identity with a TTP. That registration would provide the association between actions and an identity. That association would allow controls to limit and record actions.

In a blockchain environment, any user that a blockchain node allows can write to the blockchain. The consensus algorithm provides the assurance of data validity, instead of the TTP attestation. If your application goal is to allow unknown writers, a public blockchain may be a good choice.

Requiring public verifiability

The last requirement in determining blockchain applicability is whether your application requires public verifiability. In other words, does the data on your blockchain need to be available for public scrutiny? One example of such an application would be a blockchain of government spending. Having the entire blockchain available for verification and analysis would be desirable. In these cases, a public blockchain may be a good fit. If you still need to restrict who can access the blockchain, a hybrid blockchain may be the right choice.

IN THIS CHAPTER

- Exploring popular blockchain use cases
- Examining common strengths of blockchain
- Discovering unique blockchain features

Chapter 3
Describing Use Cases Where Blockchain Fits Well

Blockchain is an emerging technology that has captured attention around the world, and in many domains. Blockchain promises to disrupt and revolutionize the way we all interact and conduct business.

In the midst of all the hype, it's difficult to tell the difference between an interesting concept and a legitimate project with true profit potential. One of the best places to start when trying to determine how blockchain technology may fit in your organization is to look at other successful projects.

In this chapter, you learn about some use cases that leverage blockchain's strengths. You explore a few application categories, identify common traits of blockchain-friendly use cases, and see how blockchain's unique features make emerging enterprise applications possible.

Describing Top Blockchain Uses

Enterprises are exploring blockchain solutions for a wide range of applications. In spite of the variety of creative blockchain uses, several recurring use cases appear to be the most popular entry points into enterprise blockchain applications.

This section introduces some of the top blockchain uses. Learning more about how other enterprises apply blockchain technology in their environments can help you identify similar opportunities in your own organization.

Empowering commerce

Blockchain technology caught the attention of businesses from the very beginning. Even when blockchain's primary offering was to support decentralized cryptocurrency, many saw its potential to transform commerce. Today, with the extensive support of smart contracts and enterprise infrastructure, blockchain is even more able to transform commerce as we know it.

Blockchain solutions empower a wide range of consumers and increase market accessibility. Producers can use blockchain solutions to reach consumers who may have no other financial connection to render payment. Likewise, consumers can buy goods and services from a large pool of producers, without having to build trust with them first. And all participants in transactions can safely exchange money for goods or services without exposing themselves to risk.

Blockchain offers the ability to strictly define the terms of a transaction, and then enforce those terms based on performance in the real world. These transaction terms are stored in computer programs that are also part of the blockchain, called *smart contracts.* All participants agree to run smart contract code to create blockchain transactions, and smart contract code is guaranteed to produce the same results for all participants. For example, a blockchain app can put an agreed-upon amount into escrow when a consumer sets an appointment with a service provider. If the consumer doesn't show up, the

smart contract would automatically refund the consumer's payment, less an agreed-upon no-show fee. The transaction occurs without any human interaction or conflict.

One of the benefits of blockchain is its unique protections. Blockchain technology provides protection for all parties that engage in commerce transactions, offers predictable exchanges of money for goods or services, and reduces transaction costs and settlement time by eliminating middlemen.

Managing product movement throughout the supply chain

Much of today's commerce involves transferring goods and services from a producer to one or more intermediaries, until they finally reach the consumer. This commerce structure is commonly called a *supply chain.* Supply chains generally consist of multiple separate commercial organizations that work as partners.

For supply chain tracking, blockchain technology offers some unique benefits:

ility: Full audit tail of data throughout the supply chain

nce: Single, time-stamped, tamper-proof source of data

- **Flexibility:** Real-time rule-based verification of multi-party confirmations
- **Reliable transactions:** Trusted digital-signature-based peer-to-peer interactions

Each supply chain partner normally maintains separate information systems that share limited data with predecessors and successors in the chain. The segmented nature of supply chain data makes tracing goods or products back to their origin difficult. The desire to standardize supply chain data has resulted in more than 400 global standardization initiatives.

Early blockchain adopters realized that blockchain technology allows supply chain partners to participate in a shared private blockchain, called a hybrid blockchain, to expose data as goods and services move along the supply chain. Blockchain technology provides a secure platform for partners that do not completely trust all other partners to seamlessly interact as goods and services move from producer to consumer.


TIP

For example, Oracle's Blockchain Supply Chain app provides end users with business-ready technology, built on a leading blockchain platform, that makes it fast and easy to realize results.

Smart contracts provide the rules that govern every aspect of an item's life on the supply chain. Transfer of

ownership, export and import requirements, and transport quality regulations can all be codified and validated automatically. And any user of the blockchain network can track an item's movement and trace it back to its origin. This auditability eases the workload when investigations or recalls become necessary.

Providing a secure digital identity

Each blockchain use case requires some notion of identity. Each entity that interacts with a blockchain relates to a real-world identity. That identity may refer to a human, or even a device.

TIP

Consider a supply chain solution. Participants can be humans who handle the goods, as well as smart vehicles that transport the goods. Items that require refrigeration during transport may spoil if a threshold temperature is exceeded. Smart sensors in trucks can report current temperature and smart contracts can take action if thresholds are exceeded. Oracle is developing four blockchain applications to help organizations manage supply-chain issues such as Intelligent Track and Trace, Product Lineage and Provenance, Intelligent Cold Chain, and Warranty and Usage Tracking.

A digital identity on the blockchain is a permanent claim to be associated with some real-world entity along with a set of attestations. An *attestation* is some form of evidence that the claimed identity is legitimate. For humans, this could include biometrics attributes (like fingerprints). For devices, this could be physical attributes and network addresses.

When enough attestations have been provided, the identity is permanently recorded. This could have a huge impact on proving a user's identity in the face of an emergency. Digital identity via blockchain could help refugees and victims of life-changing events like earthquakes or fires recover their identities. Think of it — you may have lost your paper-based identity documents, but their digital twins would be on the blockchain. Digital identity via blockchain could also ease the process of providing government assistance or paying insurance claims. Organizations of all types are just scratching the surface in the area of blockchain applications for achieving digital identity, and ultimately perhaps self-sovereignty of identity.

Looking at Oracle Blockchain supply chain apps

Oracle is currently expanding its support of enterprise blockchain apps. Its new apps are part of a carefully planned effort to provide enterprises with the advantages of blockchain technology without having to write their

apps from scratch. Here is a brief overview of four Oracle supply chain apps to show how blockchain can help address different types of supply chain needs:

- **Intelligent Track and Trace:** Enables end-to-end traceability of goods and transactions in supply chains to reduce delays and automate record keeping. The application creates a digital trail of each step in the business network, during procurement, manufacturing, and transportation. It provides better visibility for easier root-cause analysis and faster dispute resolution. This helps customers execute targeted product recalls, resolve disputes, reduce counterfeits, improve regulatory compliance, and protect against fraud.
- **Product Lineage and Provenance:** Enables product genealogy, serialization, and provenance by managing the life cycle of hierarchical serial numbers, recording origin and authenticity of product components, and tracking all transformations of the product. It helps in regulatory compliance, targeted recalls, and preventing counterfeit components.
- **Intelligent Cold Chain:** Helps monitor and track the temperature-controlled supply chain, creating recommendations to optimize processes and ensure the quality and safety of refrigerated

products in the pharmaceutical and food and beverage industries.

- **Warranty and Usage Tracking:** Removes paper-based processes and automates usage tracking for high-value assets. An auditable and verifiable log for warranty, liability claims, and insurance helps expedite settlements and claim processing and prevents abuse of assets.

Exploring Common Traits of Blockchain Solutions

Blockchain solutions available today are quite creative and cover a wide range of application domains. In spite of the diversity, there are several recurring themes that many blockchain solutions share. In this section, you explore some of the traits that are commonly found in today's blockchain solutions.

This list isn't comprehensive or exhaustive. It doesn't limit what blockchains can do. Instead, it highlights areas in which blockchain shines and helps to emphasize areas in which blockchain may provide measurable cost savings in your environment.

Building trust where it didn't previously exist

One of the more difficult aspects to manage in today's commercial environments is trust. An organization can't expect to convince customers to pay for goods or services unless there is trust. The customer has to trust that his payments are handled properly and that the product or service is delivered as expected. On the other hand, the organization has to trust that the customer will follow through with his obligation to render proper payment.

As commerce becomes more and more distributed and disconnected (from a human contact perspective), trust typically depends on reputation and past behavior. Blockchain solutions remove, or at least noticeably reduce, the need to build trust based on reputation and performance. Customers can trust the blockchain's smart contracts to ensure delivery of purchases, and sellers can trust that payment will be made according to terms.

Both parties that participate in transactions enter into an agreement that executes without human interaction. For example, when a customer purchases a car using a blockchain app, both parties agree that the app's smart contracts handle all the details. The funds are validated and put into escrow, the title is transferred, registrations and taxes are processed, and delivery is scheduled. After the purchaser receives the car, the funds are automatically

released to the seller. The parties don't have to trust, or even know, one another.

Recording information with indelible ink

Indelible ink used to be a type of ink that would never fade and couldn't be erased. You used that type of ink to write something you wanted to last. That's what blockchain solutions do with their data. Anything that gets written to the blockchain stays on the blockchain. Unlike databases or other data repositories, existing data is never updated. The only way to change the state of data, such as update a customer's address, is to append a newer version of the data to the blockchain.

REMEMBER

Only being able to add, and not update, data on the blockchain may seem restrictive, but it provides substantial value that many blockchain solutions leverage. Blockchain provides an automatic audit trail of every transaction. You don't have to store an extra copy of data anywhere — all historical state data remains in previous blocks.

A common trait of blockchain solutions is that they use this historical record as an added-value feature. Blockchain solutions make auditing and investigating prior events easier due to the complete historical record.

Removing intermediaries

Prior to blockchain, most transactions required some intermediary to act as a broker. These brokers either facilitated asset transfers or provided some type of service for each participant. For instance, cross-border funds transfers currently require a bank or other financial institution to carry out the transfer. With blockchain, you can transfer cryptocurrency to any other address, anywhere in the world. Eliminating a single intermediary can dramatically reduce settlement time and add-on fees.

Imagine you're purchasing a building to expand operations. Currently, attorneys and agents are commonly involved in the transaction settlement, and each one demands a fee. A blockchain real estate transfer app based on smart contracts can eliminate the need for most, if not all, third-party intermediaries in real estate transactions. The smart contracts validate all steps in the process and protect the participants — the transaction occurs almost instantaneously with limited risk to either party.

Highlighting Unique Blockchain Features

Not surprisingly, most of the features that are unique to blockchain technology are the ones that the most successful blockchain solutions leverage. Blockchain apps aren't just traditional apps with a new spin — they're

foundationally different. In this section, you look more closely at four of the most unique features of blockchain and how today's apps can implement them to address enterprise goals.

Battling lack of trust with consensus

All transactions, whether in person or not, are based on trust. As you learn more about blockchain technology, you'll hear about trust as a recurring theme. The most obvious breakthrough associated with blockchain technology is its ability to provide trust in a trustless environment.

Bitcoin's novel approach of embedding a consensus algorithm in the blockchain design makes this possible. There are many multiple consensus algorithms available today, each with varying requirements and guarantees. Proof of Work (PoW) consensus is very computationally intensive and works well for public blockchains.

Enterprises generally deploy private or hybrid blockchains and have more consensus options. Proof of Authority (PoA), Proof of Stake (PoS), and Proof of Importance (PoI) are just three options. Regardless of the algorithm that a specific blockchain uses, all participating nodes can trust that transactions got on the blockchain by following the rules.

Tracing product provenance

The very nature of blockchain design requires that the details of every transaction remains unaltered in a block. Once recorded, each transaction becomes a part of the permanent record. The first blockchain implementation, Bitcoin, still uses this property to maintain current balances of accounts. Instead of simply updating an account's current balance, the balance is calculated by tracing all transactions for that account. This process works in reverse as well. Because the Bitcoin blockchain is public, anyone can trace transactions back in time to find the transactions' origin or *provenance.*

The real value of this features is evident when an app uses the blockchain to track ownership and state changes for goods and services. Consider an automobile manufacturer that uses blockchain technology to track the process of building vehicles. The process starts as each part of the vehicle is created. Suppliers of every component submits a transaction for each new part. Serial numbers allow physical items to be associated with blockchain transactions.

As each vehicle is assembled, individual parts become sub-assemblies, and those sub-assemblies eventually become a finished automobile. The manufacturer transfers the automobile to the dealer, who in turn sells it to a consumer. When the consumer brings the automobile

back to the dealer for service, the technicians can scan the automobile's ID and see every part, including its provenance.

Maintaining integrity by design

One of the difficulties auditors face is the lack of granular supporting detail. In many cases, historical data either doesn't exist or has been overwritten by the time auditors need it. Blockchain technology automatically protects data from being purged. The fact that blocks can't change once they're written to the blockchain preserves the historical record for all recorded transactions.

This unique blockchain feature is a welcome guarantee for auditors and investigators. It can, however, pose some obstacles. For example, several new and emerging regulations, including the European Union's General Data Protection Regulation (GDPR), require that any consumer can request that her information be deleted (the right to be forgotten). Core blockchain design does not support this, although there are several approaches being researched to address the requirement.

Replicating data to multiple nodes

The last unique highlighted feature of blockchain technology is foundational to its design: All nodes store local

copies of the blockchain. The append-only requirement, along with consensus, provides guarantees that all copies of the blockchain are the same.

This means the blockchain is replicated to every node. Blockchain app users will rarely even realize that this is the case, but it's a huge benefit to any app's ongoing viability. Blockchain technology removes the concern of single point of failure (SPOF). The failure of any node in a blockchain network does not make the blockchain unavailable. The other nodes continue operating as normal.

IN THIS CHAPTER

- Comparing blockchain and databases
- Integrating blockchain into traditional applications
- Deciding what to store in the blockchain

Chapter 4
Integrating Legacy Apps and Blockchain

Unless you develop a completely new, stand-alone blockchain app, your organization will probably need to integrate some existing application with blockchain technology. This process could be to add new functionality or to move traditional processing to a

blockchain. In either case, you'll need to provide a way for both types of applications to communicate and exchange data.

The best use cases for integrated blockchain apps are the ones that leverage blockchain technology's strengths, but don't use blockchain for things it doesn't do well. For example, supply chain apps (like those provided by Oracle) are a good fit for blockchain, but the enterprise resource planning (ERP) software that manages manufacturing probably isn't. Parts of an ERP application may benefit from integrating blockchain, but you wouldn't want to move the whole application to the blockchain.


TIP

To help users share data among their applications Oracle provides a comprehensive blockchain offering, including business-ready Oracle Blockchain Applications Cloud and the Oracle Blockchain Platform for developers who need to build or integrate their applications. Oracle's blockchain solutions seamlessly connect with Oracle Supply Chain Management (SCM) Cloud, Oracle Enterprise Resource Planning (ERP) Cloud, and other Oracle Cloud applications.

Additionally, as blockchain becomes an important data store in the enterprise, the platform enables Oracle Autonomous Data Warehouse customers to transparently capture blockchain transaction history and current state

data for analytics and to integrate it with other data sources.

Contrasting Traditional Data Storage with Blockchain

Blockchain technology radically changed how we store data. When data is in a block on the chain, you could argue that blockchain is just another type of database. Technically, that may be true, but it doesn't tell the whole story. In practice, there are distinct differences between traditional databases and blockchains, and those differences require attention when extending traditional applications into the blockchain space.

Examining logical data storage

From an application perspective, one of the biggest differences between database and blockchain is how each technology stores and retrieves data. Databases store data in rows and columns, or in key-value pairs. Either way, you can access data quickly using an index or key. Access languages such as Structured Query Language (SQL) make it easy to retrieve data based on flexible selection criteria. Data generally isn't stored in any particular order, but it can be retrieved in any desired sort order.

Blockchains store transaction information in blocks, with each block linked to its predecessor. The order of transactions in any block isn't guaranteed, but the blocks are logically stored in chronological order. There is no generic query language for retrieving blockchain data, so any retrieval operations must rely on a specific blockchain implementation's features. The differences in how data gets stored on a blockchain means that you must carefully design components that you migrate from a database to a blockchain.

Exploring data operations

Along with differences in how data is logically stored, the operations permitted differ as well. Traditional database query languages support four common data operations: Create, Read, Update, and Delete (CRUD). CRUD support is nearly universal and foundational in most database application designs. The last two operations, Update and Delete, are the two that differ with blockchain. Traditional database applications rely on the ability to remove (Delete) rows when they're no longer needed and change (Update) data as needed. Neither of these two operations is permitted in a blockchain environment.

Blockchain only supports Append and Read operations. The only way to write to the blockchain is to add a new block. After a block has been added to the blockchain, the only valid operation is to Read the contents of the block. There

is no support for modifying data. You can only add an updated version of the data to the end of the blockchain.

The operations differences lead to differences in application design philosophy. Because each state *variable* (any data item stored on the blockchain) may have many values, applications must ensure that they're working with the latest value and also be able to handle and leverage the history of changes to the variable over time.

Describing where data gets stored

Traditional databases store data in a single location. That location may be separated into many files spread across multiple directories, or even physical disks, but generally all reside on a single server or device. Storing all your data in a central location leads to a single point of failure (SPOF). Any event that damages or removes the database can cause widespread disruption. Most enterprises invest in multiple technologies to maintain up-to-date secondary database copies to use in case of primary data loss.

Each node in a blockchain network stores a copy of the blockchain. Some nodes may only store a portion of the blockchain, but all full nodes house a complete copy of all blocks. That single design feature removes the SPOF and makes blockchains far more resilient than traditional databases without relying on external measures (and cost).

Comparing performance

Recall that one of the benefits of blockchain technology is that of speed. Blockchain solutions reduce the amount of time to complete many transactions. But that description refers to transactions from real-world interactions with other humans. From a database technology perspective, the idea of transaction speed refers to how fast an application can write groups of changes to the database.

Database management systems have been optimized for high-throughput transaction processing for several decades. Using current technology, blockchain solutions cannot match the raw throughput of databases, at least today. It is expected that as blockchain technology matures, its performance and scalability will improve. But for now, it's important to keep the performance differences in mind when designing integration components. Blockchain currently offers integrity and decentralized trust over throughput.

Extending Legacy Application Design to Include Blockchain

In most cases, the best approach to integrating blockchain in an enterprise environment is to integrate small portions of existing applications. Because blockchain doesn't solve every problem, it should be expected to

support complete enterprise legacy applications. In this section, you learn how to identify where blockchain makes sense and how parts of your existing enterprise applications may benefit from blockchain technology.

Deciding what to move to blockchain

Moving any part of an existing enterprise application to a blockchain can be a big undertaking. A common mistake is to make the decision to move to the blockchain, and then decide what to move. That reasoning is backwards.


TIP

The right way to approach the process is to identify areas of your application that appear to be good candidates for moving to a blockchain.

After identifying likely candidates, invest resources to determine if each function that makes up the application segment you want to move is a good fit for blockchain technology. For example, are you trying to share data among multiple parties? Do you need enhanced security for your data and an audit trail? If you have to search for a reason why a function should move to a blockchain environment, it probably isn't a good fit for blockchain. The most successful blockchain migration projects are the ones that are clear candidates for migration.

One of the primary reasons for migrating to a blockchain is to increase the scope of access and usability of your data. In most cases, you want to ensure that there is real value realized in exchange for migrating. Here is a quick checklist to help you determine if you should pursue a blockchain migration project. If you can answer "yes" to these questions, it's likely worth investigating further:

- Are you prepared to lead an effort that engages participants across your industry or perhaps multiple industries?
- Does your organization value expanding collaboration with extended business partners to improve business processes?
- Is verifying or authenticating digital assets, which may represent physical assets, throughout a business process a requirement?
- Would decreasing processing or payment times through automation allow your organization to leverage contract terms and conditions to realize favorable costs?
- Do you trust other business partners that participate in a blockchain to consistently participate in good faith or must you incentivize good faith participation?

For example, suppose part of your enterprise application manages the supply chain for components that you assemble into vehicles. Your organization is planning to join a consortium of automobile manufacturers that is developing a blockchain for managing the supply chain for its members. Extending your enterprise supply chain application functions to use the consortium blockchain instead of your in-house database could be a strong candidate for blockchain migration.

Choosing the best interaction actions and events

Migrating to a blockchain environment doesn't mean that everything has to move or all your data now resides on the blockchain. In fact, it makes more sense to limit what migrates to the blockchain. And just because you migrate data to the blockchain, that doesn't remove it from your IT infrastructure. For example, Oracle Blockchain assumes that enterprise blockchain data has tremendous analytics value and makes it easy to transparently capture data to a data warehouse. After you isolate functional areas you want to migrate, document the procedural flow. Identify the actions and events that trigger some response.

TIP

The more narrowly you can scope your blockchain-specific actions, the easier time you'll have migrating or integrating your code. When you know what actions should trigger blockchain functions, such as adding new transactions or fetching state data, you can isolate the code that should interact with the blockchain. This step should also define what events, initiated by smart contract code, your enterprise application should expect to receive. In this way, you can begin to develop a detailed specification of how your integrated applications must communicate.

Rethinking transactions and scope

One of the more difficult obstacles you may encounter is the difference in the notion of transactions and scope. Traditional database applications consider a transaction to be a group of database updates that must be processed as a group. If you can't process any part of a transaction, the whole transaction must be rolled back.

Blockchain transactions are simply individual entries that change some state variable. There is no notion of multiple writes that may be rolled back in the future. Also, blockchain transactions are asynchronous in nature. After submitting a transaction, there is likely a delay before that transaction gets written to the blockchain.

A user doesn't normally wait for the transaction to be added to a block before continuing.

Legacy enterprise applications cannot continue to operate under traditional transaction requirements when integrating with a blockchain. You'll likely need to rewrite portions of your existing application to incorporate the asynchronous and distributed nature of blockchain transactions. This effort can be simple or complicated depending on the data you manage and the applications you use to manage your organization. You don't have to write everything from scratch, though. Several tools, such as REST APIs and other types of toolsets exist to ease the integration. For instance, Oracle provides a comprehensive collection of REST APIs for event subscription, blockchain administration and configuration, and monitoring of network health, transaction rates, and other statistics, which simplify integration with existing enterprise IT tools.

Planning for Blockchain Component Integration

As with any enterprise project, proper planning is crucial for success. Blockchain is an exciting new technology, and too many well-intentioned projects have failed to meet goals because of a lack of good planning. In this section, you learn about some of the elements necessary

to increase the odds of a positive blockchain project outcome. There are no guarantees, but paying attention to some of the early building blocks can save you time and money later.

Building your development environment

When you're ready to start developing smart contracts for a blockchain environment, you'll either need to build a development environment or use a blockchain app with preconfigured components instead of writing code. If you'll be writing your own code, the specific environmental components you'll need will vary based on your blockchain implementation, but there are some basic components you'll use in the development process.

Here is a list of the basic components you'll need to develop smart contracts for a blockchain environment:

- **Blockchain client:** This software runs the blockchain software, making a computer a blockchain node.
- **Development and testing blockchain:** This tool sets up a local, or non-live, blockchain to use before deploying code to the blockchain.

- **Compiler and testing framework:** A compiler translates source code into chaincode, and testing tools help to identify and fix bugs.
- **Source code editor and integrated development environment (IDE):** These tools include editors and suites of tools designed to help developers write code.

You can build an environment yourself, or you can use enterprise development environments already populated with the components you'll need, such as the Oracle Blockchain Platform. Based on Hyperledger Fabric, Oracle has built the tools and environment to make blockchain development accessible to any organization. For more information on the Oracle Blockchain Platform, go to `www.oracle.com/blockchain`.

Starting with a Proof of Concept

Unless you and your organization have experience in enterprise blockchain development, start with a small Proof of Concept (PoC) project. Although it may seem to delay the start of a "real" project, you'll benefit from the experience. Blockchain apps are radically different from traditional applications. And enterprise blockchain apps have different requirements from purpose-built or stand-alone blockchain apps.

Because you're likely integrating your enterprise blockchain app with some other application and data source, start small. Don't try to solve the whole problem on day 1. Also, stay away from mission-critical functions. Migrate functions that aren't central to your organization's day-to-day operation. Although no one anticipates failures or other disruptions, they do happen.

Although blockchain migration will result in new smart contracts, it will also put some data on the blockchain. Spend as much time as necessary to investigate how placing any of your enterprise data on a blockchain will impact regulatory compliance.

REMEMBER

Once that data is on the blockchain, it stays on the blockchain. Ensure that you aren't violating any confidentiality or privacy regulations. If you do discover sensitive data on the blockchain, the only way to remove it is if all parties agree to data changes.

Testing from the beginning

Although testing is the last topic in this chapter, it should never be the last step is any software development project. Testing should be incorporated from the very beginning. Thorough testing will not only help identify program bugs early in the project, but it will also highlight any departures from specifications or design goals.

WARNING

The result of allowing program flaws into production is far greater in a blockchain environment. Data that a flawed program writes to the blockchain can't be purged. You can't get it back. Plus, flawed programs themselves can't be directly changed. You have to release an updated version of your code, along with a way to ensure that no one executes the old version.

In short, test exhaustively. Then test again. Continuously.

IN THIS CHAPTER

- Designing with blockchain in mind
- Acquiring blockchain development skills
- Mapping blockchain development to the software development life cycle

Chapter 5
Designing and Implementing Blockchain Solutions

In previous chapters, I explain blockchain technology and how to determine if blockchain is a good fit for your organization. If you've identified a use case that maps to blockchain's features, the next step is to design

your solution. If you don't want to design a solution from scratch, you can use a preconfigured app (like the Oracle Supply Chain apps). Designing blockchain solutions shares many aspects of the development process with non-blockchain applications, but there are a few areas that are unique. In this chapter, I outline the process of designing and implementing enterprise blockchain solutions and explain how some of the steps differ from traditional application development.

Cultivating Blockchain-Centric Application Design

Designing blockchain solutions can be time consuming. You're introducing a new technology that is steeped in hype and buzzwords. To the general public, blockchain is nearly the same as black magic. Much of a designer's work in blockchain is to build, signal, and reinforce trust. In this section, you learn about fostering trust.

Solving a people problem

All too often, software design focuses on solving a technical problem. That approach may produce efficient software, but it may not meet users' needs. Blockchain

solutions already have at least two perception problems. First, the technology is new, and second, one of the drivers for blockchain is to serve users who don't trust one another.


TIP

From the very beginning of any blockchain project, there will be trust issues. Users can trust the technology, but they may not know that yet. Your design should provide substantive coverage and reinforcement that their data is being handled properly. Your design should include both passive and active techniques for users to verify that trust.

For example, any transfer of items of value should provide an end-of-transaction confirmation. Users should also be able to look up the results of transactions to verify that everything happened as it should have. Confirmations and post-transaction inquiries can go a long way toward reassuring users that they can trust the technology.

Above all, your design should emphasize the people problem that you're solving. Users don't really care how efficiently you store their data in a block that is linked to other blocks. They want to see that your app tells them where their romaine lettuce came from, or that the transmission in their car wasn't

one that was just recalled. Providing value and ease of use to the end user should always be the ultimate design goal.

Focusing on the value

REMEMBER

Solving a people problem should provide some value to the user. Your design should not only provide the value, but also make that value clear to the user. The very beginning of the design process should focus on clearly defining the value your app will provide, and then enumerating ways to provide that value and communicate it to the end user.

Many retailers currently add a "You saved . . ." section to their receipt. They point out, often in a substantially larger font, how much the customer saved by shopping with that retailer. An important design goal targeted at building trust is to focus on your solution's value. A well-placed solution should deliver value that is easy to articulate. That isn't unique to blockchain solutions, but it's very important when building trust.

Protecting your users

One of the concerns that many users express with blockchain is the loss of privacy. Blockchain is generally perceived as being completely public and permanent. Any

personal data that gets on the blockchain is there to stay and available to anyone.

This concern does have some elements of truth, but the problem isn't as bad as many users perceive. First, many enterprise blockchains are private, also called permissioned. That means there is an authority that governs blockchain access and makes certain data available to certain parties on the blockchain. So, most enterprise blockchains aren't publicly available.

Second, enterprise blockchains routinely use encryption to protect personal information. The trusted authority that controls blockchain access can also manage encryption keys. This is why it's said that blockchain provides a high level of security for data on the chain.

Third, blockchain data is permanent, but because of the first and second points, permanent encrypted data that isn't publicly available isn't as much of a risk as is perceived.

One core goal of any blockchain solution should be to protect its users and their data, and to go to great lengths to educate users on those measures. Building trust is central to blockchain success, and designing for trust helps your solution to be successful.

Learning Blockchain Development Technical Skills

Developing blockchain is similar to developing other software solutions, but it does have nuances that make it a distinct process. Similar to developing non-blockchain apps, to create blockchain apps you either need to write the code yourself, hire someone else to do it, or rely on framework with prebuilt application components that you can use to assemble apps. The process of writing code is the most similar activity, but design must take into account the cost of blockchain interaction, the impact of writing to a structure you can't modify, and the unique nature of transaction recording.

Some of the benefits of Oracle's Blockchain Platform include the ability to

- Enable new business models with a preassembled blockchain platform
- Rapidly onboard network participants with an enterprise-grade blockchain
- Improve transparency across your IT ecosystem with plug-and-play integrations

Testing and deployment have their own twists on the tried-and-true development process. In this section, you learn about the most common nuances in blockchain development.

Gaining experience with the infrastructure

Enterprises have multiple options for blockchain solutions. Two of the most promising solutions are Hyperledger Fabric and Ethereum Enterprise. Developers of each product are members of the other's alliance. This collaboration provides enterprises with exceptional standardization and flexibility for a wide range of implementors. When your organization chooses a platform, the next step in deploying a viable solution is to gain experience in your chosen platform.

Developing software in a new language

Regardless of the blockchain implementation your organization chooses, there will be a learning curve for the environment and the primary smart contract programming language.

Ethereum Enterprise relies on Solidity for its main smart contract language. Solidity is very much like JavaScript,

so developers who know JavaScript should have an easy transition.

Hyperledger Fabric smart contracts are written in the Go language, which is much like C and C++. Developers who have experience in C and object-oriented programming (OOP) languages will likely find the Go language easy to learn.

Regardless of the blockchain implementation or language, the primitives required to interact with a blockchain will be a little different than with traditional environments. Each language provides abilities to alter state variables and query existing blockchain data. Although these abilities are similar to traditional data operations, the lack of update and delete operations makes processing a little different. As much as the blockchain languages are similar to existing languages, there are some structural and syntactic differences that require time to digest.

Testing and deploying apps

Traditional application development best practices recommend separate development, testing, and production environments. Blockchain development all but requires separation of environments. Because both code and data written to the blockchain are permanent, all smart

contract code must be exhaustively tested before deploying it to a live environment.

Deploying smart contracts with bugs has several detrimental effects:

- The code must be replaced with a newer version. All references to the older version must be deactivated and all subsequent calls to the smart contract must reference the newer, fixed version.
- If the software fix changed the way the smart contract interacts with data, the new version of the smart contract has to handle data in the old format and in the new format. This complexity alone is good enough reason to test smart contracts exhaustively to resolve all the bugs before deploying to a live blockchain.

Another common reason to separate testing environments from deployment environments is the level of control developers and testers have on the blockchain data. A test blockchain is an ideal place to test smart contracts because the entire blockchain can be deleted and rebuilt as needed. This is a valuable ability when attempting to run newly developed code multiple times using repeatable data and states.

Integrating Blockchain Development in the Software Development Life Cycle

Most organizations that decide to engage in blockchain application development already have active software developers engaged in ongoing projects. The most productive approach to migrating enterprise applications to blockchain technology is to leverage existing talent and experience.

Instead of creating a brand-new development group, many organizations leverage their existing personnel and extend development effort into the blockchain space. This approach can flatten the learning curve and increase effectiveness of existing personnel.

Developing architecture for risk and compliance first

Blockchain application development punctuates the need to approach every development activity in the context of risk management and compliance. The unique aspects of blockchain transparency and persistence brings compliance issues to the foreground.

In reality, every software modification in any enterprise should be given the same level of consideration with respect to risk management and compliance. But in reality, too little time is invested in assessing risk and evaluating compliance impact of software change.

Migrating to a new technology exposes the enterprise to a new category of risk. Existing controls to address known risks may no longer be sufficient. It's important to carefully assess risk associated with structural application changes, and to determine how those changes may affect regulatory compliance.

Designing with deployment in mind

One of the more difficult realities to keep in mind when writing smart contract code is how the deployment environment differs from development or testing. Although the testing environment should approximate the deployment runtime environment, that is rarely the complete case. Data on the live, or deployment, blockchain is always different from any sensitized testing environment. Because the live blockchain continually adds new blocks, any copy for testing will quickly become stale.

TIP

There is an approach to make the testing environment more like the live environment. Before each test, you can remove the testing private blockchain data and rebuild it as a copy of the current live blockchain. The copy won't be exactly the same as the live blockchain, but it will be close.

Regardless of the state of the test environment, it will always be only a simulation of the live environment. Ignoring data differences, the live environment supports multiple nodes and potentially many users. Test blockchains generally do not include the complex interactions of live users. This simplification can make your testing environment only partially effective. If your tests depend on assessing the intricate interaction of dozens of users, a local test environment may not be completely sufficient.

Testing is an important aspect of any blockchain solution. Testing helps identify software flaws and helps to make smart contracts more trustworthy.

Testing every day

All too often, testing is viewed as an activity that takes place after primary development finishes. Post-development testing is important, but it's only one small part of overall testing.

Every output of the development process should be tested in an ongoing manner. From the very beginning, all new design or architectural documents should be compared to the specification and initial requirements documents as new documents become available. This review process helps to identify gaps at a very early stage.

As frequent reviews validate that all ongoing activity complies with previous stage documents, the development process can continue with renewed confidence that the resulting software solution satisfies the project requirements.

REMEMBER

Daily testing is necessary to maintain quality and to ensure that the eventually delivered product meets its original goals. Test every day, and you'll only encounter minor gaps. If you wait longer to test, you're likely to encounter some disruptive findings.

IN THIS CHAPTER

- Leveraging blockchain's global reach
- Providing transparency and provenance
- Securing transactions
- Shortening time to market

Chapter 6
Ten (Or So) Enterprise Blockchain Projects

After learning about blockchain technology and many of its features, you may be wondering how your enterprise can get involved in a blockchain project. A great way to determine the best way to get involved is by looking at existing enterprise blockchain projects. This chapter presents current projects that

highlight how other organizations are implementing their own blockchain solutions. Read through the overviews here and follow the provided links to get more information. You may find an idea that ends up being your organization's gateway into the enterprise blockchain world!


TIP

For more information on how customers and partners are using Oracle Blockchain, visit the Oracle Blockchain website at `https://www.oracle.com/cloud/blockchain/customer-successes.html`.

Simplifying Supply Chain Tracking with CargoSmart

CargoSmart is leveraging blockchain to simplify complex shipping documentation processes and improve customers' operational efficiency by building a collaborative network with Oracle Blockchain. Connected through a blockchain documentation platform, the entire shipping ecosystem can improve documentation accuracy, expedite documentation turnaround times, better manage detention and demurrage costs, and reduce disputes. CargoSmart projects a 65 percent reduction in the amount of time required to collect, consolidate, and confirm data from multiple parties and to handle shipping data that is repetitive in different documents by leveraging its blockchain shipment documentation solution.

Learn more about CargoSmart and Oracle Blockchain at https://www.oracle.com/hk/customers/cargosmart-1-blockchain-cl.html.

Easing Invoice Factoring at Neurosoft

Neurosoft chose the Oracle Blockchain Platform to leverage blockchain technology for its new Proxima+ product. Proxima+ is an E2E Factoring and Supply Chain Finance platform that helps firms manage supply chain receivables. Proxima+ incorporates predictive analytics and workflow support to increase efficiency and reduce the effort commonly required to optimize cash flow and reduce receivables turnaround.

Learn more about Neurosoft's Proxima+ with Oracle Blockchain at https://www.oracle.com/emea/customers/neurosoft-1-blockchain-platform.html.

Expediting Cross-Border Money Transfers at AJIB

Arab Jordan Investment Bank (AJIB) developed a blockchain-based solution for the problem of transferring money across national borders. Current solutions

require ongoing relationships with partner banks and third-party intermediaries, which leads to slow transaction settlements and multiple transaction fees. AJIB chose the Oracle Blockchain Platform to accelerate product development to launch its blockchain-based apps to transfer money across national borders faster and with lower fees.

Learn more about AJIB's cross-border money transfer solution at `https://www.oracle.com/jo/customers/ajib-1-blockchain-cl.html`.

Creating a Secure and Reliable Integrated Mileage Platform at MTO

MTO Global is a Korean startup with a unique blockchain application. MTO adopted the Oracle Blockchain Platform to develop its platform that allows its users to exchange reward points from airlines, hotels, and other sources into its own cryptocurrency token. MTO named its platform the Mileage-to-Opportunity (M2O) platform. M2O users can spend their M2O tokens to pay for products or services using cryptocurrency.

Learn more about M2O at `https://www.oracle.com/customers/mto-global-1-blockchain.html`.

Delivering Safer and Faster Invoicing at SERES

SERES provides solutions to support secure electronic document exchange. SERES is a prime example of an enterprise that extended its core functions to incorporate blockchain. SERES used the Oracle Blockchain Platform to build decentralized applications to manage the transfer of electronic data interchange (EDI) invoicing transaction exchange. Its deployed products increase transparency, security, and efficiency.

Learn more about SERES at `https://www.oracle.com/customers/seres-1-blockchain-platform.html`.

Enabling Transparency for Mineral Sourcing and Ethical Trade at Circulor

Circulor is a UK company that supports mineral mining supply chains. Circulor helps miners and consumers of mineral products track raw materials from initial collection from mines all the way through the finished product, and then even to recycling. It uses the Oracle Blockchain

Platform to develop and deploy its supply chain platform to provide transparency to all participants and help manage payments throughout the process.

Learn more about Circulor at `https://www.oracle.com/uk/customers/circulor-1-blockchain.html`.

Verifying Trusted Supply Chain for Authentic Extra Virgin Olive Oil at Certified Origins

Certified Origins Italia is another company that saw the advantage of a transparent end-to-end supply chain management app. Certified Origins produces and exports high-quality extra virgin Italian olive oil. Its customers want assurance that the products they purchase are of the highest quality. Certified Origins uses the Oracle Blockchain Platform to track and trace its olive oil from its Italian bottling facility all the way to the consumer. This implementation of blockchain technology is a continuation of Certified Origins' commitment to providing greater food supply chain transparency.

Learn more about Certified Origins at `https:// www.oracle.com/it/customers/certified-origins-1-blockchain-story.html`.

Speeding Development Time and Testing at Finotek

Finotek is a company located in Seoul, Korea, that provides financial services for organizations to simplify financial transaction processing. Finotek selected the Oracle Blockchain Platform to develop and deploy its financial transaction data platform application. Finotek found Oracle to be a better fit than Oracle's competitors in both performance and cost effectiveness. Finotek plans to use the Oracle Blockchain Platform as a core development and testing cloud environment for its ongoing advanced platform development.

Learn more about Finotek at `https://www.oracle.com/customers/finotek-1-blockchain.html`.

Collaborate with trusted data in enterprise applications

Enterprise Blockchain For Dummies introduces blockchain technology and describes how enterprises can leverage its features. You'll learn how to identify areas in your enterprise that may benefit from blockchain integration, and how to plan, develop, and deploy effective blockchain apps. Understand how blockchain technology can help your organization create transparent and secure apps with unprecedented built-in auditability.

Inside...

- Discover the benefits of blockchain
- Learn how storing data in a blockchain is different from storing in a database
- Align blockchain benefits to business goals
- Find out why enterprise blockchain apps can affect business outcomes
- Integrate blockchain data with enterprise apps

ORACLE®

Michael G. Solomon, PhD, is an author, speaker, consultant, and educator who specializes in GRC and blockchain services. Michael is a Principal Consultant for GRC as a Service, and a professor of Cyber Security and Global Business with Blockchain Technology at the University of the Cumberlands.

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

ISBN: 978-1-119-59401-7
Not for resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

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