Book Collection

Learning Path

Blockchain Development with Hyperledger

Build decentralized applications with Hyperledger Fabric and Composer

Salman A. Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O'Dowd, Venkatraman Ramakrishna, Weimin Sun and Xun (Brian) Wu

Packt
www.packt.com

Blockchain Development with Hyperledger

Build decentralized applications with Hyperledger Fabric and Composer

Salman A. Baset
Luc Desrosiers
Nitin Gaur
Petr Novotny
Anthony O'Dowd
Venkatraman Ramakrishna
Weimin Sun
Xun (Brian) Wu

Packt

BIRMINGHAM - MUMBAI

Blockchain Development with Hyperledger

First Published: March 2019

Production Reference: 1250319

Published by Packt Publishing Ltd.
Livery Place, 35 Livery Street
Birmingham, B3 2PB, U.K.
ISBN 978-1-83864-998-2

www.packtpub.com

mapt.io

Mapt is an online digital library that gives you full access to over 5,000 books and videos, as well as industry-leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why Subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Mapt is fully searchable
- Copy and paste, print, and bookmark content

Packt.com

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Contributors

About the Authors

Salman A. Baset is the CTO of security in IBM Blockchain Solutions.

Luc Desrosiers is an IBM-certified IT architect with 20+ years of experience.

Nitin Gaur is the director of IBM's Blockchain Labs, and an IBM Distinguished Engineer.

Petr Novotny is a research scientist at IBM Research, with an MSc from University College London and PhD from Imperial College London, where he was also a post-doctoral research associate.

Anthony O'Dowd works in IBM's Blockchain team and is based in Europe.

Venkatraman Ramakrishna is an IBM researcher with a BTech from IIT Kharagpur and PhD from UCLA.

Weimin Sun is an expert in designing data-driven solutions.

Xun (Brian) Wu is an author, founder, and board advisor for several blockchain start-ups.

Packt Is Searching for Authors Like You

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface

This Learning Path is your easy reference for exploring and building blockchain networks using Ethereum, Hyperledger Fabric, and Hyperledger Composer. It begins with an overview of blockchain and shows you how to set up an Ethereum development environment for developing, packaging, building, and testing campaign-decentralized applications. You'll learn Solidity – the de facto language for developing decentralized applications in Ethereum. You'll configure the Hyperledger Fabric and use these components to build private blockchain networks and applications that connect to them. Starting with the principles first, you'll learn to design and launch a network, implement smart contracts in chaincode, and much more.

By the end of this Learning Path, you'll be able to build and deploy your own decentralized applications by handling the key pain points encountered in the blockchain life cycle.

Who This Book Is For

This Learning Path is designed for blockchain developers who want to build decentralized applications and smart contracts from scratch using Hyperledger. A basic familiarity or exposure to any programming language will be useful to get started with this course.

What This Book Covers

`Chapter 1`, *Blockchain - Enterprise and Industry Perspective*, you've heard about blockchain and you are wondering, what is all the fuss about? In this chapter, we explore why blockchain is a game changer, what innovation it brings, and what the technology landscape is.

`Chapter 2`, *Exploring Hyperledger Fabric*, starts with an understanding of the blockchain landscape, then we turn our attention to Hyperledger Fabric. The aim of this chapter is to walk you through the deployment of each component of Hyperledger Fabric while unveiling/building the architecture.

`Chapter 3`, *Setting the Stage with a Business Scenario*, describes a business use case and then focuses on understanding the process of creating a good business network, using blockchain from requirements to design.

`Chapter 4`, *Designing a Data and Transaction Model with Golang*, aims to define what makes up a smart contract in Hyperledger Fabric. It will also introduce you to some terms regarding smart contracts and get you to experience the development of a chaincode using the Go language.

`Chapter 5`, *Exposing Network Assets and Transactions*, leveraging the smart contract written in the previous chapter, this chapter looks at the required integration of application to the network. It takes the readers through the process of configuring a channel, and installing and invoking chaincode, from a client application and considers the various integration patterns that might be used.

`Chapter 6`, *Business Networks*, has an objective to introduce and uncover the skills and tools needed to model a business network. Working at a higher level of abstraction, the foundation, tools, and framework will provide the reader with a way to quickly model, design, and deploy a complete end-to-end business network.

`Chapter 7`, *A Business Network Example*, putting the concepts of the previous chapter into practice, this chapter walks through the steps to deploy a full business network from end-user application to smart contracts.

`Chapter 8`, *Agility in a Blockchain Network*, focuses on the aspects required to maintain agility in a blockchain network. Applying DevOps concepts, the reader is presented with a continuous integration / continuous delivery pipeline.

`Chapter 9`, *Life in a Blockchain Network*, aims to raise the reader's awareness on the key activities and challenges that organizations and consortium may face when adopting a distributed ledger solution, ranging from management of application changes to maintenance of adequate performance levels. A successful network deployment will hopefully see that many organizations join it and that the number of transactions increase.

`Chapter 10`, *Governance –The Necessary Evil of Regulated Industries*, governance is a necessary evil for regulated industries, but governance is not required only for business network that deal with use cases for regulated industries. It is also a good practice to ensure longevity and scalability of a business network. This chapter explores vital considerations for production readiness for any founder-led blockchain network.

`Chapter 11`, *Hyperledger Fabric Security*, lays the foundation for security design of blockchain networks. Various security constructs are discussed and Hyperledger Fabric security is explained in detail. An essential chapter to understand security design considerations.

`Chapter 12`, *Introduction to Blockchain Technology*, gives an overview of the key concepts, such as cryptography and hash algorithms, the distributed ledger, transactions, blocks, proof of work, mining, and consensus. We cover Bitcoin, the mother of blockchain technology, in detail. We briefly introduce Ethereum by pointing out some limitations of Bitcoin and how they are addressed by Ethereum. While Bitcoin and Ethereum are examples of public blockchains, IBM's Hyperledger is used as an example of enterprise blockchains. Toward the end of this chapter, we look at the evolution of blockchain, through 1.0, 2.0, 3.0, and beyond, and we examine their use cases.

`Chapter 13`, *Ethereum Fundamentals*, covers the basic concepts of Ethereum, such as smart contracts, ether, consensus algorithms, EVM, gas, and accounts. We will discuss Ethereum performance and review ideas on how to improve the overall performance via proof of work, casper, plasma, and sharding.

`Chapter 14`, *Overview of Solidity Programming*, discusses what solidity is, as well as the tools for the solidity development environment. We then discuss smart contracts and their common patterns. We cover the important topic of smart contract security. Finally, we show how to write a smart contract with a use case of crowdfunding.

`Chapter 15`, *Building an Ethereum Blockchain Application*, looks at what a DApp is. We give a quick overview of web3.js. We explain how to set up an Ethereum development environment, as well as how to develop and test a DApp.

`Chapter 16`, *Exploring an Enterprise Blockchain Application Using Hyperledger Fabric*, gets into the key concepts of Hyperledger Fabric, along with the core components. We explain how to create a Hyperledger Fabric environment, how to write a chaincode, and how to set up Hyperledger Fabric configuration.

`Chapter 17`, *Implementing a Business Network Using Hyperledger Composer*, provides an overview of Hyperledger Composer and talks about how to set up a Hyperledger Composer environment. We discuss business scenarios, the business network archive, and how to implement a business transaction function.

`Chapter 18`, *Blockchain Use Cases*, first talks about popular blockchain use cases across industries, including the financial sector, civil services, supply chains, the **Internet of Things** (**IoT**), and healthcare, at a high level. We will then proceed to a discussion of the proper use cases for DApps, before then developing a successful DApp. Finally, we take the health data-sharing use case and comment at a high level on building a DApp for it.

To Get the Most out of This Book

We've focused on organization and flow. The content is made to ensure not only an easy-to-follow and natural flow but also topical modularity. Each chapter explores a facet of blockchain. While Hyperledger projects are specifically discussed, the core areas of focus are universal to blockchain technology discipline.

This learning path aims to be a development path into the world of blockchain technology. The chapters are arranged to ensure that they can be followed easily and flow naturally.

Business users can skip the chapters with detailed descriptions on how to develop blockchain applications and, instead, focus on the chapters with general descriptions of the technology and use cases.

It is recommended that IT users download the code and make modifications for adopting to their own use cases or exercises.

Download the Example Code Files

You can download the example code files for this book from your account at `www.packt.com`. If you purchased this book elsewhere, you can visit `www.packt.com/support` and register to have the files emailed directly to you.

You can download the code files by following these steps:

1. Log in or register at `www.packt.com`.
2. Select the **SUPPORT** tab.
3. Click on **Code Downloads & Errata**.
4. Enter the name of the book in the **Search** box and follow the onscreen instructions.

Once the file is downloaded, please make sure that you unzip or extract the folder using the latest version of:

- WinRAR/7-Zip for Windows
- Zipeg/iZip/UnRarX for Mac
- 7-Zip/PeaZip for Linux

The code bundle for the book is also hosted on GitHub at `https://github.com/PacktPublishing/Blockchain-Development-with-Hyperledger`. In case there's an update to the code, it will be updated on the existing GitHub repository.

We also have other code bundles from our rich catalog of books and videos available at `https://github.com/PacktPublishing/`. Check them out!

Conventions Used

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "The orderer belongs to its own organization called `TradeOrdererOrg`."

A block of code is set as follows:

```
- &ExporterOrg
  Name: ExporterOrgMSP
  ID: ExporterOrgMSP
  MSPDir: crypto-config/peerOrganizations/exporterorg.trade.com/msp
  AnchorPeers:
    - Host: peer0.exporterorg.trade.com
    Port: 7051
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
pragma solidity ^0.4.15;
import 'zeppelin/contracts/math/SafeMath.sol';
….
contract ExampleCoin is ERC20 {
  //SafeMath symbol is from imported file SafeMath.sol'
  using SafeMath for uint256;
   …
}
```

Any command-line input or output is written as follows:

```
mkdir ~/insurance-claim && cd ~/insurance-claim
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "When the preceding request is validated by mining nodes, the **HelloWorld** smart contract is invoked."

Warnings or important notes appear like this.

Tips and tricks appear like this.

Get in Touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packt.com/submit-errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packt.com`.

1
Blockchain - Enterprise and Industry Perspective

Blockchain promises to fundamentally solve the issues of time and trust to address inefficiencies and costs in industries such as financial services, supply chains, logistics, and healthcare. Blockchain's key features include immutability and a shared ledger where transactional updates are performed by a consensus-driven trust system, which can facilitate a truly digital interaction between multiple parties.

This digital interaction is not only bound by systemic trust, but ensures that the provenance of the transactional record maintains an immutable track record of interaction between parties. This very characteristic lends itself to culpability and non-repudiation, and incentivizes fair play. With the blockchain system design, we are attempting to build a system that has implied trust. This trust system leads to reduced risks, and various applied technology constructs such as a cryptography, encryption, smart contracts, and consensus essentially create gates to not only reduce risk but to also infuse added security into the transaction system.

We will be covering the following aspects of blockchain in our discussion for this chapter:

- Defining a blockchain
- Building blocks of blockchain solutions
- Fundamentals of the secure transaction processing protocol
- Applications of blockchain
- Blockchain in an enterprise
- Enterprise design principles
- Business considerations for choosing a blockchain framework
- Considerations for choosing a blockchain framework

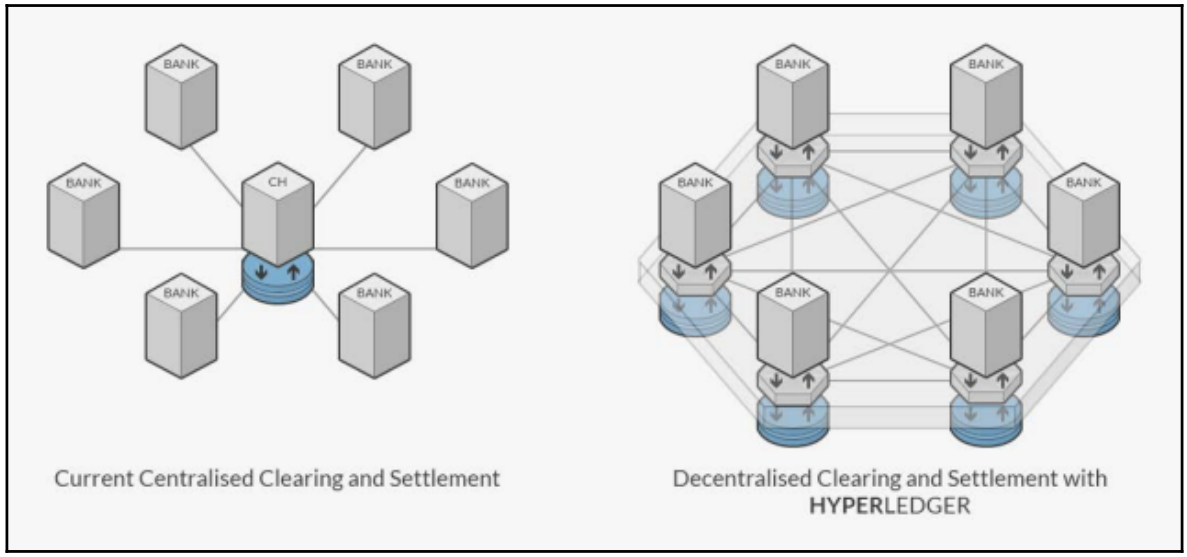
Defining the terms – what is a blockchain?

At a technical level, a blockchain can be defined as an immutable ledger for recording transactions, maintained within a distributed network of mutually untrusting peers. Every peer maintains a copy of the ledger. The peers execute a consensus protocol to validate transactions, group them into blocks, and build a hash chain over the blocks. This process forms the ledger by ordering the transactions as is necessary for consistency. Blockchain has emerged with bitcoin (`http:// bitcoin.org/`) and is widely regarded as a promising technology to run trusted exchanges in the digital world.

A blockchain supporting a cryptocurrency is public, or permissionless, in the sense that anyone can participate without a specific identity. Such blockchains typically use a consensus protocol based on **proof of work** (**PoW**) and economic incentives. In contrast, permissioned blockchains have evolved as an alternative way to run a blockchain between a group of known, identified participants. A permissioned blockchain provides a way to secure interactions between a group of entities who share a mutual goal but don't fully trust each other, such as businesses that exchange funds, goods, or information. A permissioned blockchain relies on the identities of its peers, and in so doing can use the traditional **Byzantine-fault tolerant** (**BFT**) consensus. BFT is a protocol that has been widely used in IT solutions to reach a consensus on the state of faulty nodes of a network. This protocol is based on the Byzantine General's Problem, whereby a group of general need to reach a consensus on their strategy but one of them maybe treacherous.

Blockchains may execute arbitrary, programmable transaction logic in the form of smart contracts, as exemplified by Ethereum (`http://ethereum.org/`). The scripts in bitcoin were predecessors of this concept. A smart contract functions as a trusted, distributed application and gains its security from the blockchain and underlying consensus among its peers.

Discerning permissions from a permissionless blockchain is vital for enterprises looking to utilize the blockchain platform. The use case dictates the choice of technology, which depends on consensus systems, governance models, data structure, and so on. With permissioned blockchains, we can do some of the things we already do but in an incrementally better way, which can be significant. In the chart that follows, you can see how a consortium of banks could use Hyperledger, a type of permissioned blockchain, for clearing and settlement without relying on a central clearing house:



Clearing house have been created because banks do not fully trust each other and thus as the intermediary between trades, reduces the risk the one party does not honor his terms leads to a never-ending debate around permissioned versus permissionless blockchains, and while this chapter will not address the debate, blockchain can present a way to either transform or disrupt the current business and business models. Most use cases in regulated industries embark on permissioned blockchain models.

This is due to regulatory requirements and the economic viability of transaction processing, and while permissionless blockchains provide a platform for new business models such as **Peer-to-Peer** (**P2P**) transactions and disintermediation-led models, by definition permissionless blockchain architecture relies on a very compute-intensive compute model to ensure transactional integrity. Regardless of the choice in blockchain models, blockchain provides a lot of possibilities for transformation and disruption.

Blockchain has extraordinary potential as a technology platform. In the enterprise, blockchain can provide:

- A design approach that keeps transaction data, value, and state inherently close to the business logic
- Secure execution of business transactions, validated through a community, in a secure process that facilities the trust and robust transaction processing that are foundational to blockchain
- An alternative, permissioned technology that conforms to existing regulations

Blockchain promises to solve longstanding industry concerns—and this is where its potential can really be seen, with issues such as modernizing financial and trade systems, and speeding up securities and trade settlements.

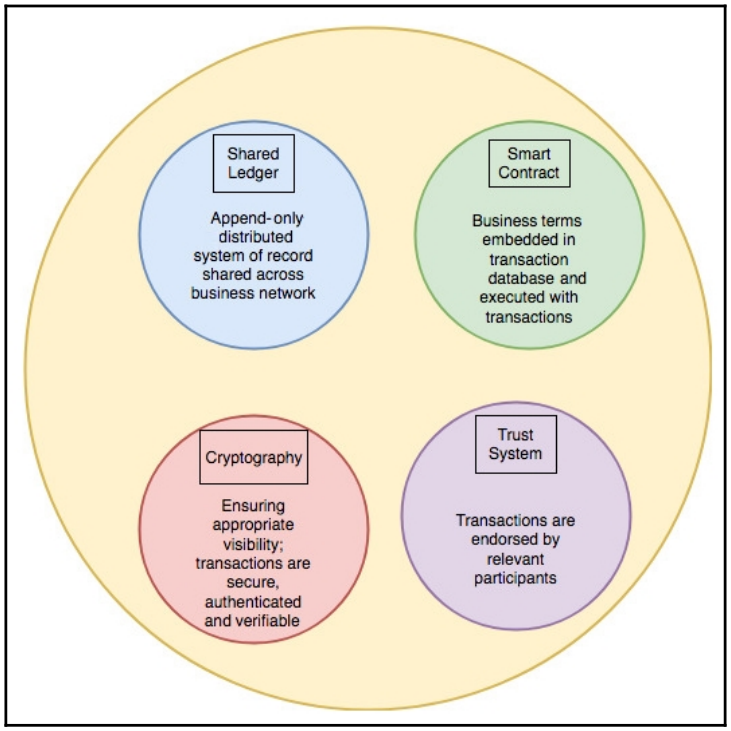
Four core building blocks of blockchain framworks

Blockchain frameworks typically include the following four building blocks:

- **A shared ledger**: The shared ledger appends only the distributed transaction record. Bitcoin blockchain was designed with the intent to democratize visibility; however, with blockchain, consumer data regulations also need to be considered. Using a properly configured SQL or noSQL distributed database can achieve immutability, or append-only semantics.
- **Cryptography**: Cryptography in a blockchain ensures authentication and verifiable transactions. Blockchain design includes this imperative because of the focus on assuming computational hardness and making encryption harder for an adversary to break. This is an interesting challenge with bitcoin blockchain because of the economic incentive and its system design. When you're working in a less democratic or permissioned business ledger network, considerations around cryptography change.
- **Trust systems or consensus**: Trust systems refer to using the power of the network to verify transactions.
  Trust systems are central to blockchain systems in my view; they are at the heart of blockchain applications, and we believe trust system is the preferred term over **consensus system** since not all validation is done through consensus. This foundational element of trust dictates the overall design and investment in a blockchain infrastructure. With every new entrant in the blockchain space, the trust system is modified, forming variations that are specialized for specific blockchain use cases. Trust, trade, and ownership are staples of blockchain technology. For inter-company transactions, the trust system governs transactions for trade between participating companies.
  Much work still needs to be done to define the best trust system for specific use cases, such as P2P and sharing economy models with B2B models.

- **Business rules or smart contracts**: Smart contracts are the business terms that are embedded in a blockchain transaction database and executed with transactions. This is also the rules component of a blockchain solution. It is needed to define the flow of value and state of each transaction.

The following use diagram gives a good idea of these concepts:



The four building blocks are generally accepted and well understood. They have existed for decades prior to blockchain. Shared ledgers are an evolutionary change, similar to the move to computer-based spreadsheets, but the underlying business rules have stayed the same.

Additional capabilities to consider

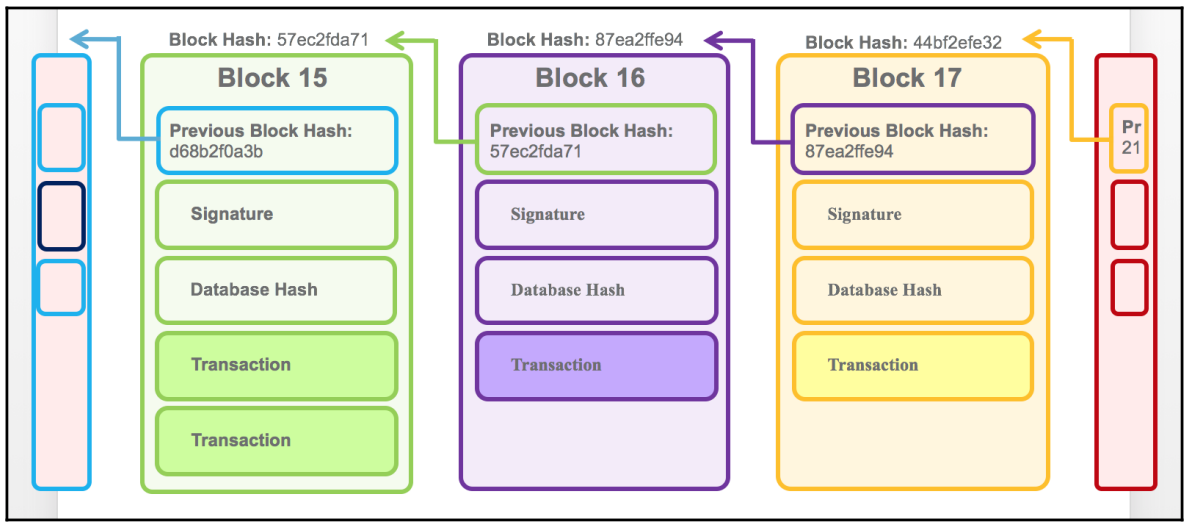
What else should be included in enterprise blockchain proposals? Here is a non-exhaustive list of other capabilities to consider:

- **Auditing and logging**: Including auditing and logging in a blockchain solution can help with addressing regulations for the purposes of non-repudiation, technology root cause analysis, fraud analysis, and other enterprise needs.
- **Enterprise integration**: It's also worth considering how the solution will be integrated into the enterprise:
    - **Integration with the incumbent Systems of Record** (**SoR**): The goal here is to ensure that the blockchain solution supports your existing systems such as CRM, business intelligence, reporting and analytics, and so forth
    - **Integration as a transaction processing system**: If you want to preserve the system of record as an interim approach to adopting blockchain, integrating it as a transaction processing system makes sense
    - **Design with the intent to include blockchain**: The path of least disruption to your existing systems will accelerate enterprise adoption of blockchain
- **Monitoring**: Monitoring is an important capability for addressing regulations and ensuring high availability, capacity planning, pattern recognition, and fault identification.
- **Reporting and regulatory requirements**: Being prepared to address regulatory issues is also very important, even for interim adoption of a blockchain as a transaction processing system. It's recommended that you make connectors to your existing SoR to offload reporting and regulatory requirements until blockchain is enterprise-aware, or the enterprise software is blockchain-aware.
- **Enterprise authentication, authorization, and accounting requirements**: In a permissioned enterprise world (unlike permissionless bitcoin blockchains), all blockchain network participants should be identified and tracked. Their roles need to be defined if they are to play a part in the ecosystem.

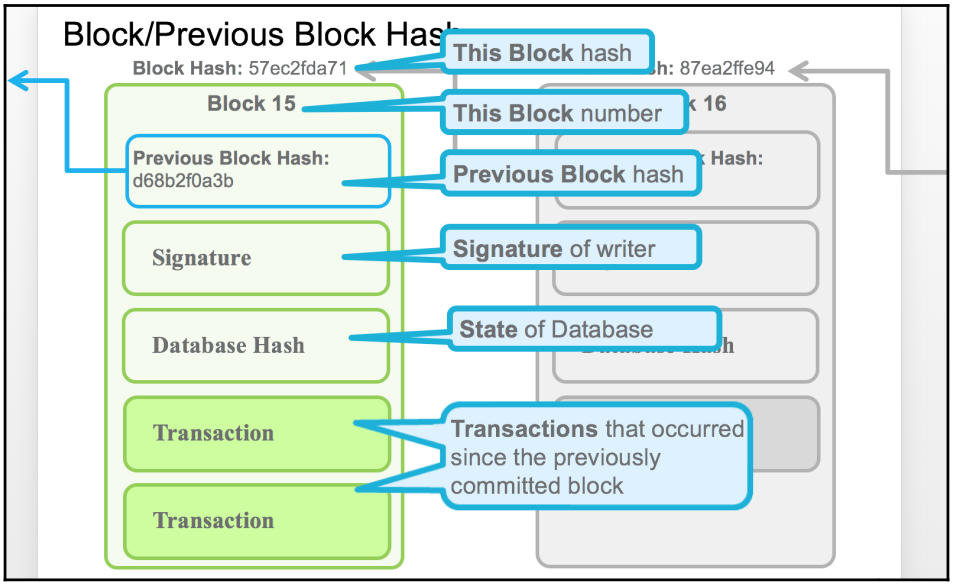
Fundamentals of the secure transaction processing protocol

We mentioned previously that cryptography is one of the core building blocks of a blockchain solution. The fundamental security of the bitcoin blockchain is the elegant cryptographical linkage of all major components of the ledger. Specifically, transactions are linked to each other, mainly through the Merkle tree. A Merkle tree is based on the concept of a tree data structure where every leaf node has a hash calculated of its data and where the non-leaf node have a hash of all of their underlying child. This method provides a way to ensure the integrity of the data, but also provides privacy characteristics by allowing one to remove a leaf that is deemed private but leave the hash, thereby preserving the integrity of the tree. The Merkle tree has its roots incorporated into the block header. The block header includes a reference to the block headers that precede it.

That cryptographically enforced interconnectivity fosters the stability and security of distributed ledgers. At any point, if a link between any of the components is broken, it leaves them exposed to malicious attacks:



Transactions are also cryptographically connected to the rest of the blockchain structure, mainly through the Merkle tree. Once a transaction is modified within a block, with all other parts remaining stable, the link between all transactions of the block and its header are broken:



The new resulting Merkle tree root does not match the one already in the block header, hence providing no connectivity to the rest of the blockchain. If we proceed to change the Merkle tree root in the block's header, we will in turn break the chain of headers and thus the security model of the blockchain itself. Therefore, if we only change the contents of a block, the rest of the blockchain components remain stable and secure, especially as the block headers provide the connecting links by including a hash of the previous block header in the header of the next block.

Where blockchain technology has been and where it's going

Blockchain has already been a business disruptor, and I expect it to significantly transform industries, the government, and our lives in the near future.

The great divide

A significant divided exists between the cryptocurrency and **Initial Coin Offering** (**ICO**) world, and the world of regulated business. The latter consists of banks and financial institutions working collectively to assess market potential and operational efficiencies.

Both sides of this division have taken advantage of the momentum around blockchain to further their interests. The blockchain ecosystem has challenged the status quo and defied all odds to make a point—often behaving like an adolescent. It is driven by new business models, promises of disintermediation, and interesting technological innovations. As blockchain gains momentum, the value of bitcoin and other cryptoassets is seeing a meteoric rise, and now that ICO has emerged, it has defied the traditional regulatory framework around fundraising.

On the enterprise side, there are a growing number of industry initiatives around clearing and settlement to enable faster settlement and interbank transfers, transparency through digitization, symmetric dissemination of information in supply chains, and creating adhoc trust between **Internet of Things** (**IoT**) devices.

There's a common theme here—that blockchain is here to stay. As it continues to evolve and generate innovative solutions for industry use cases, it will keep inching towards maturity and deliver on its promises of efficiency and significant cost savings built on the foundation of trust.

An economic model for blockchain delivery

Business networks, underpinned by blockchain technology, may bring transformation or disruption to industries, but in any case, in order to thrive, blockchain needs an economic model. If disruption is the aim, investments in technology, talent, and market synergy can be combined with the lure of economic incentives. ICOs, for example, typically rely on tokenomics, a term that describes the economic system of value generation in those networks. The token is the unit of value created by the system or network, either through making a platform for providers or consumers, or through co-creating a self-governing value network in its business model that various entities can use to their advantage for creating, distributing, and sharing rewards that benefit all stakeholders.

The ICO front, largely funded by cryptocurrencies, has defied current fundraising mechanisms in venture capitalism (led by crowdfunding projects), and, importantly, the struggle to discern the difference between a security and utility coin is disruptive in principle.

ICOs are looking to create an economic system built on the principles of **decentralization**, **open governance** (or self-governance), and transparency, a system that rewards innovation and eradicates disintermediation. ICOs saw some initial failures and some successes, but they nevertheless provided a preview of the future, where cryptoassets will become a basic unit of value—with valuation and fungibility defined by the network they originate from—fueling an economy built for and around innovation.

On the enterprise front, there's been more focus on understanding the technology and reimagining ecosystems, business networks, regulations, confidentiality and privacy, and the business models that impact blockchain networks in various industries. Enterprises looking to explore blockchain want to see quick proof points, use cases that can demonstrate results quickly and help them innovate with blockchain.

Blockchain is helping industries move to a more symmetric dissemination of information by providing built-in control of transactional data, provenance, and historical context. This can lead to more efficient workflows and transformed business processes. Many early projects, however, didn't focus on the core tenets of blockchain, leading to disintermediation, decentralization, and robust self-governance models. There's a good reason for it, though: industries and conventional businesses tend to be focused on their current business agenda, models, growth, and preceding all, regulatory compliance and adherence. This emphasis on current business operations means they're not naturally inclined towards disruptive models.

Learning as we go

With any new technology, there is always a learning curve. As blockchain evolved and we began to work with regulated industries, we quickly recognized that in such industries, there are important design considerations to address, things such as confidentiality, privacy, scalability, and performance. These elements can have significant cost implications when it comes to designing blockchain networks, as well as the business models that govern these networks. These challenges have not only been interesting to solve; they've had a positive effect on conventional, regulated industries and businesses by re-energizing innovation in these organizations and inviting the best talent to join in tackling these challenges. Businesses are seeing that ecosystems and networks driven by blockchain technology will contribute to progress and success.

Permissioned networks (regulated, conventional, and enterprise business networks) may also need to begin uncovering an incentive model to motivate organizations to join a platform that promotes the idea of creation, distribution, and sharing of rewards, benefiting all stakeholders. The economic incentives behind tokenomics can't be blindly adopted by a lot of conventional businesses and industries, but that doesn't mean those industries shouldn't start the journey of exploring possible business models that will enable value creation and elevate some desperately needed modernization efforts.

The promise of trust and accountability

Blockchain technology promises to be the foundation for a secure transaction network that can induce trust and security in many industries that are plagued with systemic issues around trust and accountability. From a technology point of view, blockchain facilitates a system of processing and recording transactions that is secure, transparent, auditable, efficient, and immutable. These technology characteristics lend themselves to addressing the time and trust issues that current-day distributed transaction systems are plagued with.

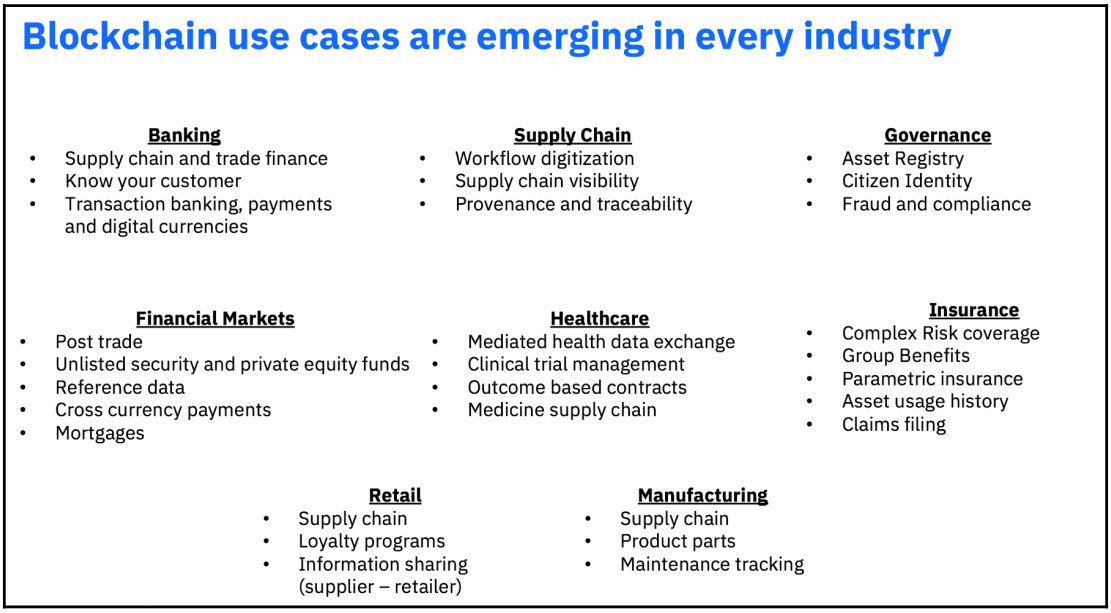
Blockchain fundamentally shifts the multi-tier model to a flat-tier transaction processing model. This carries the promise to fundamentally disrupt industries by disintermediation, by inducing efficacy in new system design or simply by creating new business models.

Disintermediation indicates reducing the use of intermediaries between producers and consumers, such as by investing directly in the securities market rather than going through a bank. In the financial industry, every transaction has historically required a counter party to process the transaction. Disintermediation involves removing the middleman, which by definition disrupts the business models and incentive economies that are based on mediation. There's been a wave of disruption in recent years as a result of digital technologies, which have, in turn, been driven by marketing insights and the desire for organizations to provide a richer user experience.

Blockchain is a technology that aims to catapult this disruption by introducing trade, trust, and ownership into the equation. The technology pattern represented by blockchain databases and records has the potential to radically improve banking, supply chains, and other transaction networks, providing new opportunities for innovation and growth while reducing cost and risk.

Industries putting blockchain technology to work

Let's briefly look into blockchain use cases:



Blockchain in the enterprise

Now that we've looked at where blockchain is emerging in various industries, let's talk about what principles should guide the use of blockchains in an enterprise. Why would an enterprise want to apply blockchain technology to one of its systems or applications?

What applications are a good fit?

Organizations will need to establish criteria for use during the application design process to help them assess where they can best apply blockchain technology. The following are some examples of criteria that could help an enterprise determine which applications or systems would benefit from it:

- **Applications that adhere to trade, trust, and ownership**: As described previously, these three tenets—trade, trust and ownership—are fundamental to any blockchain system. Trade and ownership imply the churn and the transfer of ledger entries, while trust points to the trustless nature of a transaction system.
- **Applications that are fundamentally transactional in nature**: There is often a debate about why we can't achieve the benefits of blockchain from a distributed database, that is, a no-SQL or a relational database. But a multi-party transaction is what makes an application suitable for blockchain. There needs to be long-running processes with numerous micro-transactions that will be verified and validated by the blockchain-powered transaction system. However, databases can still be used for persistence or replication to fit enterprise systems. Other considerations include small data set sizes that could increase over time, logging overhead, and so on.
- **Business networks that are comprised of non-monopolistic participants**: This third criteria addresses distributed versus decentralized computation models. Blockchain trust systems can work within any model; however, the trust aspect of a blockchain business network comes from multi-party participants with non-monopolistic participation (the consortium permissioned network model). Oligopolistic participation might be acceptable (the private permissioned network model), but it's essential to devise a trust model that assures the prevention of centralized control, even with rational behavior of the participants. Many internal use cases do not adhere to this principle and are more for distributed application models.

For enterprises trying to either understand or determine where to employ blockchain meaningfully, there's a simple approach to thinking through use case selection. An appropriate use case for a sustainable blockchain solution will achieve long-term business objectives and provide a strong return on technology investment.

This starts with an **enterprise problem**—an issue big enough for the enterprise to expend resources/time—and the recognition of cohorts that have the same problem. When companies realize that an enterprise problem is also an **industry problem** (such as security lending, collateral lending, and so on), they've found a use case where the promise of blockchain has the most potential.

While organizations are determining the benefits of various aspects of blockchain for their enterprise applications, they also need to recognize the fragmentation of the whole blockchain landscape. There are numerous innovative approaches available for solving a specific challenge with blockchain. A lot of vendors offer variants of the trust system that are specialized to address particular use cases, and they've defined the use cases that will benefit most from blockchain in a given industry, for example. Such specialized vendors often promise a fast solution to meet consumer demands for quick digital interactions.

The tenets of blockchain can be instrumental in delivering rapid consumer-driven outcomes such as decentralized, distributed, global, permanent, code-based, programmable assets, and records of transactions. We should exercise caution with regards to thinking of blockchain as a hammer to solve every enterprise application challenge, but it can be of use in many transactional applications.

Now, let's discuss how blockchain is perceived in the enterprise and some of the challenges that arise with enterprise adoption of the technology. In the following section, I'll focus on three areas that help set the tone for blockchain in an enterprise context.

How does the enterprise view blockchain?

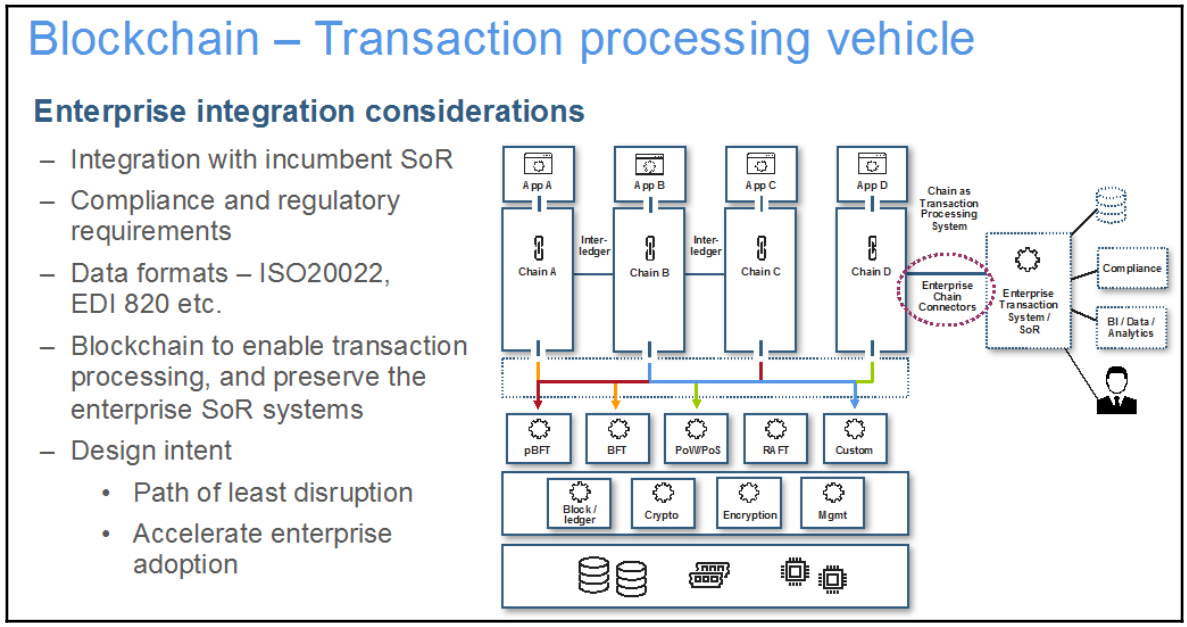
Radical openness is an aspect of blockchain as a digital trust web, but in an enterprise, it's vital to consider the impact and implications of radical openness.

A public blockchain can operate with extreme simplicity, supporting a highly distributed master list of all transactions, which is validated through a trust system supported by anonymous consensus. But can enterprises directly apply the model of the trustless system without modifying the fundamental tenets of blockchain?

Do organizations view this disruptive technology as a path to their transformation or merely a vehicle to help them improve their existing processes to take advantage of the efficiencies that the trust system promises? No matter what, enterprises will want the adoption of blockchain to be as minimally disruptive to the incumbent system as it can be, and that won't be easy to achieve! After all, the design inefficiencies of the incumbent system are what have compelled the enterprise to consider this paradigm shift. A lot of the concepts and use cases for blockchain are still distant from enterprise consumption.

The first industry to experiment with and adopt blockchain was the financial services sector, as it has been facing down the fear of being disrupted by another wave of start-ups. Like many industries, it is also driven by consumer demands for faster, lower-cost transactions. Financial services has a well-defined set of use cases including trade financing, trade platform, payment and remittance, smart contracts, crowd funding, data management and analytics, marketplace lending, and blockchain technology infrastructure. The uses for blockchain we've seen in this industry will likely permeate to other industries such as healthcare, retail, and the government in the future.

The blockchain is a nascent technology that brings together a lot of good ideas, but it still has some maturing to do for enterprise use. The lack of defined standards to promote interoperability between multi-domain chains could be a challenge. Enterprises that adopt it will therefore need to build competency so that they can contribute to further innovation and help with necessary blockchain standards development. This, in turn, could help bring unique opportunities to both improve existing business practices and develop new business models built in a blockchain-powered trust web:



Litmus testing to justify the application of blockchain technology

Fundamentally, blockchain addresses three aspects of the transaction economy:

- Trade
- Ownership
- Trust

The notable technology elements of blockchain are:

- **Technology behind the trust system**: Consensus, mining, and the public ledger
- **Secret communication on open networks**: Cryptography and encryption
- **Non-repudiation systems**: Visibility to stacks of processes

While the implications of blockchain technology may be profound, organizations should devise a set of enterprise-specific criteria that can be applied to existing or new projects that may gravitate towards enterprise blockchains.

Given the versatility of blockchain technology and the current hype curve, enterprises should use a chain decision matrix as a tool to ensure that they have a structured approach to apply a foundational technology to a business domain. This approach will also lend itself to a consistent blockchain infrastructure and trust system management, which will prove vital as many application-driven chains evolve and the demand for enterprise visibility, management, and control grow.

Integrating a blockchain infrastructure for the whole enterprise

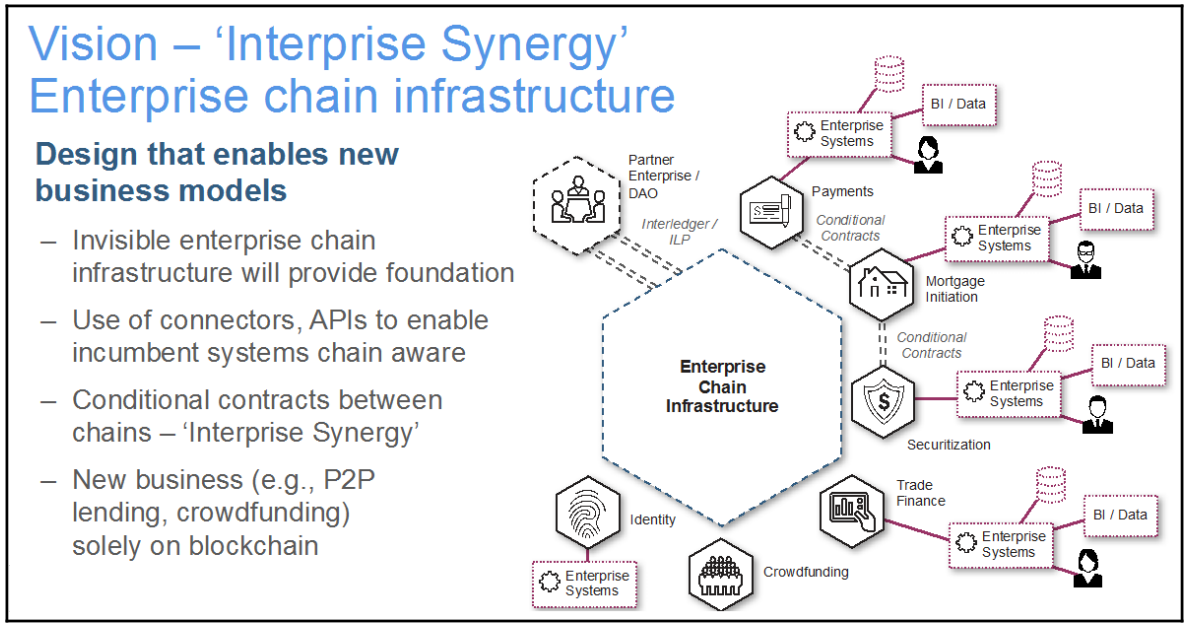
Any enterprise adoption of blockchain should have the goal of disrupting incumbent systems. Thinking about integration with enterprise systems of record is one way to work towards this. In this manner, an enterprise can implement blockchain-driven transaction processing and use its existing systems of record as an interface to its other applications, such as business intelligence, data analytics, regulatory interactions, and reporting.

It's vital to separate the infrastructure for enterprise blockchain technology from the business domain that uses chain technology to gain competitive advantage. Blockchain can be seen as an enterprise chain infrastructure that's invisible to businesses and operating behind the scenes, while promoting the **interprise synergy** between various business-driven chains. The idea is to separate the business domain from the technology that supports it. A chain application ought to be provisioned by a business domain that has a suitable trust system. The trust system, as I've stated repeatedly, is central to any blockchain endeavor, and therefore it should be appropriate to the needs of a given business application. The cost of the infrastructure and compute requirements will be dictated by the choice of trust system available to an enterprise.

By separating out the blockchain technology infrastructure, designing an architecture around a pluggable trust system by using trust intermediaries and a design that promotes flexibility, and a modular trust system, the business can focus on the business and regulatory requirements, such as AML, KYC, nonrepudiation, and so on. The technology infrastructure for blockchain applications should be open, modular, and adaptable for any blockchain variant, thereby making the blockchain endeavor easy to manage.

Interprise synergy suggests driving synergies between numerous enterprise blockchains to enable inter and intra enterprise chain (interledger) connections. In this model, the transactions would cross the various trust systems, giving visibility into the interactions to enterprise governance and control systems. Fractal visibility and the associated protection of enterprise data are important to consider when looking at these interactions between business units and external enterprises. An invisible enterprise chain infrastructure can provide a solid foundation to evolve enterprise connectors and expose APIs to make incumbent systems more chain-aware.

Interprise synergy will flourish due to conditional programmable contracts (smart contracts) between the business chains:



How can an enterprise know if it is ready for blockchain? More importantly, when considering blockchain consumption, should its focus be on integration with incumbent transaction systems, or an enterprise-aware blockchain infrastructure?

To take full advantage of the promise of enterprise blockchain, an integrated enterprise will need more than one use case and will need to drive **interprise synergy**. The most successful blockchain consumption strategy should focus on technology initially and then consider integration with existing enterprise business systems. This will facilitate collective understanding and accelerate enterprise adoption of the blockchain, hopefully on the path of least disruption.

Enterprise design principles

As stated previously, blockchain technology promises to be the foundation for a secure transaction network that induces trust and security in industries that are plagued with systemic issues around trust and accountability. It aims to generate market and cost efficiencies.

In the past few years, as blockchain technology has come to maturity, we've focused on how enterprises and businesses can use the technology to relieve pain points and herald new business models. Organizations that have begun to see blockchain's potential are now beginning to reshape business networks that are burdened by the systemic costs of archaic processes, paperwork, and technology.

Business drivers and evolution

In the recent past, organizations would run internal business systems and IT infrastructure out to the internet to harness the collaborative potential of interconnected and accessible systems. Blockchain technology is taking this to the next level, offering true digital interaction facilitated by trusted business networks. In the internet era, successful enterprises adopted and adapted to technological challenges, whereas in the blockchain era, business, rather than technology, is the driver for proliferation.

While blockchain technology is interesting on its own, there are a lot of other mechanics of a business network that ought to be evaluated as well, including:

- **Consensus models**: Which trust system is most fitting for your business network?
- **Control and governance**: What entities are permitted to do what? Who will own the investigative process if there's a system anomaly?
- **Digital asset generation**: Who creates an asset in the system? Who governs it?
- **Authority for issuance**: In a system that's truly decentralized, the notion of authority does not hold together. So in a blockchain network, who would be responsible for governance, culpability, and eventually regulations?
- **Security considerations:** How will the network address enterprise security, including new security challenges imposed by a shared business network?

We imagine a purpose-built blockchain network that's focused on a plurality of business domains, for example, mortgages, payments, exchanges, clearing, and settlement of specific asset types. In an enterprise context, we visualize a centralized network in which like-minded business entities share a consensus consortium. There are several practical reasons to back this idea of a centralized network, including the following:

- The use of domain-specific business language, which leads to the construction, management, and governance of smart contracts as proxy business representations
- A defined asset type, which leads to governance, management, and valuation (for exchange, fungibility, and so on) of the digital representation of assets

- Appropriate regulation, given that every industry and business network is regulated separately, and therefore the burden of adhering to regulations and other related costs can be shared in the business network
- Other related business functions such as analysis, analytics, market data, and so on

We've now covered the business drivers for enterprise blockchain, so next let's consider what can ensure the sustainability and longevity of a blockchain network.

Ensuring sustainability

Blockchain-based business networks are continuing to evolve and grow, and as they do, there will be no turning back on core issues such as trust models, data visibility, and exploiting a network for competitive advantage.

Focusing on sustainability can seem paradoxical because it promotes open collaborative innovation while at the same time locking down constructs such as consensus or trust systems and the governance systems for managing assets, smart contracts, and overall interaction in a multiparty transaction network. Blockchain system design needs to take all of this under consideration.

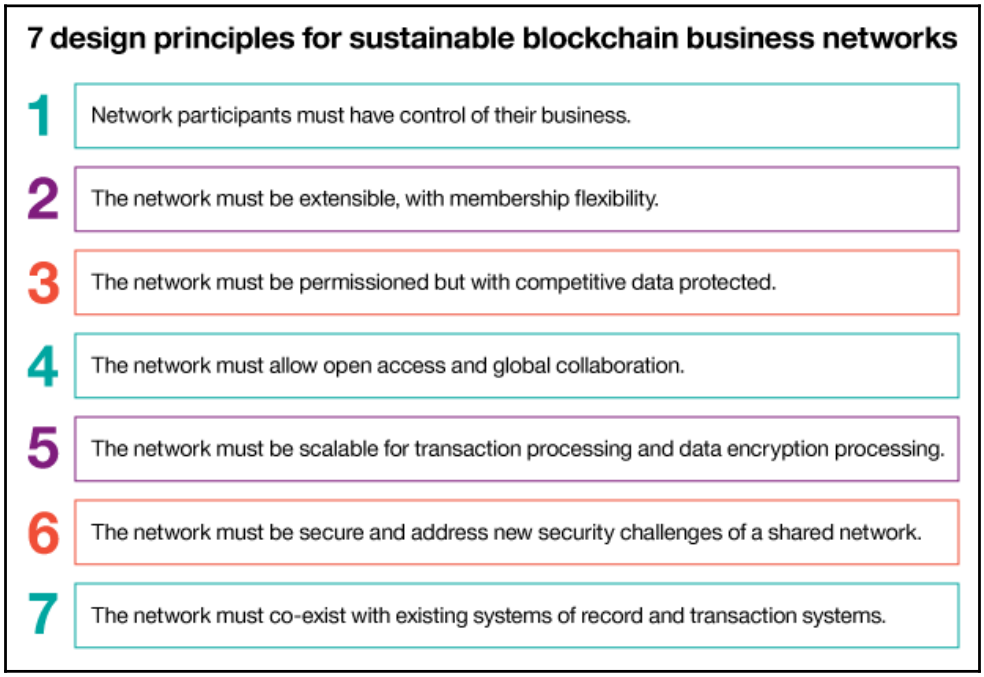
A business network with a successful system design needs to align well with the blockchain tenets of trade, trust, ownership, and transactionality in a multi-party scenario. Without building on these core tenets, business networks may not realize the promise of blockchain technology in a sustainable way.

Here are seven design principles to support and sustain growth in a blockchain business network:

- The network participants need to have control of their business
- The network has to be extensible, so that participants have flexibility to join or leave the network
- The network must be permissioned but also protected, to safeguard competitive data while facilitating peer-to-peer transactions
- The network should allow open access and global collaboration for shared innovation
- The network must be scalable for both transaction processing and encrypted data processing

- The network has to be able to accommodate enterprise security and address new security challenges
- The network needs to coexist with established systems of record and transaction systems in the enterprise

We will list the design principles graphically as follows:



The principles that drive blockchain adoption

In any enterprise, blockchain adoption is driven by three principles: the business blueprint, the technology blueprint, and enterprise integration.

The following are some indispensable things to consider when choosing a blockchain framework according to these three principles:

- **Business blueprint**: Blockchain promises to create a business network of value based on trust. To do this, it's vital to understand how various blockchain frameworks handle network interaction patterns, inefficiencies, and vulnerabilities.
- **Technology blueprint**: If technology is to align with business imperatives, organizations need to make appropriate technology and architecture choices for their needs. **Transactions per second** (**TPS**), enterprise integration, external system integration, and regulatory and compliance requirements may be taken under advisement here. These decisions are all part of the technical due diligence necessary to properly budget for blockchain adoption.
- **Enterprise integration**: Integrating blockchain into enterprise systems, especially an adjacent system, is an important business and technology consideration (because downstream transaction systems affect critical business systems) as well as a cost point. Based on my experience, if organizations don't focus on adjacent system integration early in the planning, it can impede adoption, because it has a significant cost impact on blockchain projects.

In the following sections, I cover each of these design considerations in a bit more detail.

Business considerations for choosing a blockchain framework

Numerous criteria come into play when organizations are evaluating whether to adopt blockchain to address their pain points. Here are some considerations from a business perspective:

- **Open platform and open governance**: The technology standards a business chooses will set the stage for enterprise blockchain adoption, compliance, governance, and the overall cost of the solution.
- **Economic viability of the solution**: Whatever blockchain framework an organization chooses should provide cost alignment to its existing business models, chargebacks, compute equity, and account management. This flows into ROI.

- **Longevity of the solution**: As organizations aspire to build a trusted network, they'll want to ensure that they can sustain the cost and operation of the network so that it can grow and scale to accommodate additional participants and transactions.
- **Regulatory compliance**: Compliance issues are closely tied to transaction processing and can include events such as industry-specific reporting and analysis for business workflows and tasks, both automated and human-centric.
- **Coexistence with adjacent systems**: A blockchain network needs to be able to coexist with the rest of the enterprise, network participants, and adjacent systems, which may have overlapping and complementary functions.
- **Predictable costs of business growth**: Business growth depends upon predictable metrics. Historically, a lot of industries have focused on transactions per second, but that measurement differs from system to system based on system design, compute costs, and business processes.
- **Access to skills and talent**: The availability of talent affects costs as well as maintenance and the longevity of a blockchain solution as the industry and technology evolve with continued innovation.
- **Financial viability of technology vendors**: When choosing vendors, it's vital to think about their viability when it comes to long-term support and the longevity of your blockchain solution. You should examine the long-term vision and the sustainability of the vendor or the business partner's business model.
- **Global footprint and support**: Blockchain solutions tend to involve business networks with a global reach and the related skills to support the network's expansion with minimal disruption.
- **Reliance on technology and industry-specific standards**: Standards are critical, not only in helping to standardize a shared technology stack and deployment, but also in establishing an effective communication platform for industry experts to use for problem solving. Standards make low-cost, easy-to-consume technology possible.

Blockchain vendors offer various specializations, including:

- **Variant trust systems**: Consensus, mining, proof of work, and so on.
- Lock-in to a single trust system
- Infrastructure components that are purpose-built for particular use cases
- Field-tested design through proof of concept

The technological risk of a vendor not adhering to reference architecture based on standardized technology set is a fragmented blockchain model for the enterprise.

From a business point of view, an open standards-based approach to blockchain offers flexibility, along with a pluggable and modular trust system, and therefore is the most ideal option. This approach keeps an enterprise open to specialized blockchains such as Ripple, provides a provisioning layer for the trust system, and offers a separate business domain with the technology to support it.

Technology considerations for choosing a blockchain framework

When organizations consider the technology implications of blockchain, they should start with the premise that it is not just another application. It's a production network that involves risks and costs to ensure correct upkeep and maintenance.

Here are some important things to ponder when evaluating blockchain's technological impact.

Identity management

Identity management is a complicated, involved topic, especially in regulated industries where identities must be managed and have significant business consequences, such as around activities including **Know Your Customer** (**KYC**), **Anti-Money Laundering** (**AML**), and other reporting and analytics functions:

- **Permissioning** is the concept of **member enrollment certificates** (**eCerts**) and **transaction certificates for each member** (**tCerts**); these enable an entity to be permissioned and identified while transactions are completed
- **End user identity**, which is maintained by a participating entity in the blockchain network, is the mapping of the LDAP/User registry to the tCerts or transaction ID for the sake of tracing (Know Your Customer, as well as Know Your Customer's Customer)