KLS's Gogte Institute of Technology
Department of Computer Science & Engineering

Course Name: **Block Chain Management**

Course Code: **18CS743**

Assistant Professor,

Ravi U. Kalkundri

Grasping Blockchain Fundamentals

Tracing Blockchain's Origin

- There is a need for an efficient, cost-effective, reliable, and secure system for conducting and recording financial transactions.

The shortcomings of current transaction systems

- Throughout history, instruments of trust, such as minted coins, paper money, letters of credit, and banking systems, have emerged to facilitate the exchange of value and protect buyers and sellers.
- Still, many business transactions remain inefficient, expensive, and vulnerable, suffering from the following limitations:
  - Cash is useful only in local transactions and in relatively small amounts.
  - The time between transaction and settlement can be long.
  - Duplication of effort and the need for third-party validation and/or the presence of intermediaries add to the inefficiencies.
  - Fraud, cyberattacks, and even simple mistakes add to the cost and complexity of doing business, and they expose all participants in the network to risk if a central system, such as a bank, is compromised.
  - Credit card organizations have essentially created walled gardens with a high price of entry.
  - Half of the people in the world don't have access to a bank account and have had to develop parallel payment systems to conduct transactions.

The emergence of bitcoin

- One solution that has been developed to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems is bitcoin — a digital currency that was launched in 2009 by a mysterious person (or persons) known only by the pseudonym Satoshi Nakamoto.
- Unlike traditional currencies, which are issued by central banks, bitcoin has no central monetary authority.
- No one controls it.
- Bitcoins aren't printed like dollars or euros; they're "mined" by people and increasingly by businesses, running computers all around the world, using software that solves mathematical puzzles.
- Rather than rely on a central monetary authority to monitor, verify, and approve transactions and manage the money supply, bitcoin is enabled by a peer-to-peer computer network made up of its users' machines, akin to the networks that underpin BitTorrent and Skype.

The emergence of bitcoin (Conti..)

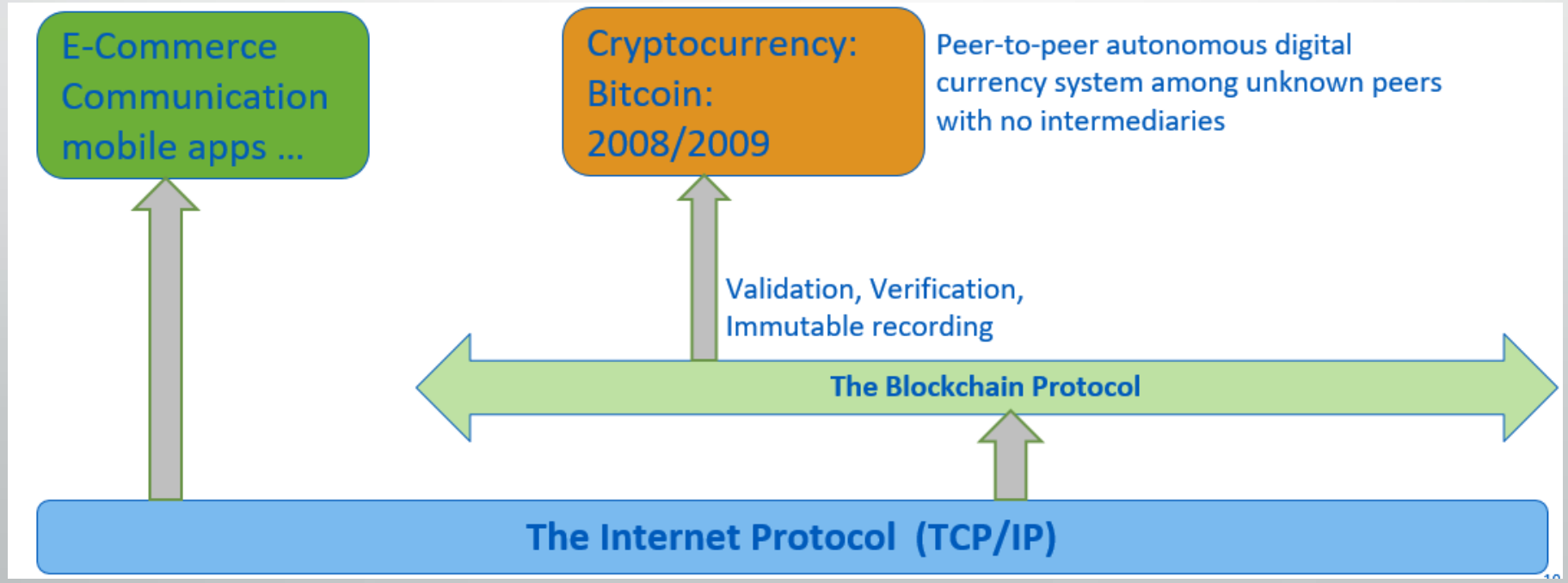
- Bitcoin has several advantages over other current transaction systems, including the following:
  - **Cost-effective**: Bitcoin eliminates the need for intermediaries.
  - **Efficient**: Transaction information is recorded once and is available to all parties through the distributed network.
  - **Safe and secure**: The underlying ledger is tamper-evident. A transaction can't be changed; it can only be reversed with another transaction, in which case both transactions are visible.
- There's a common misconception among people that Bitcoin and Blockchain are one and the same, however, that is not the case.
- Creating cryptocurrencies is one of the applications of Blockchain technology and other than Bitcoin, there are numerous applications that are being developed on the basis of blockchain technology.

The birth of blockchain

- Bitcoin is actually built on the foundation of blockchain, which serves as bitcoin's shared ledger.
- Think of blockchain as an operating system, such as Microsoft Windows or MacOS, and bitcoin as only one of the many applications that can be run on that operating system.
- Blockchain provides the means for recording bitcoin transactions — the shared ledger — but this shared ledger can be used to record any transaction and track the movement of any asset whether tangible, intangible, or digital.

What is Blockchain?

- The concept of Blockchain first came to fame in October 2008, as part of a proposal for Bitcoin, with the aim to create P2P money without banks.



What is Blockchain? (Conti..)

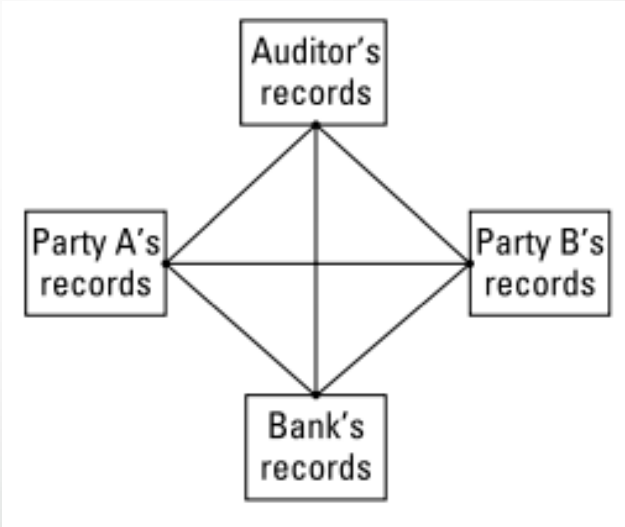
- Bitcoin introduced a novel solution to the age-old human problem of trust.
- The underlying blockchain technology allows us to trust the outputs of the system without trusting any actor within it.
- People and institutions who do not know or trust each other, reside in different countries, are subject to different jurisdictions, and who have no legally binding agreements with each other, can now interact over the Internet without the need for trusted third parties like banks, Internet platforms, or other types of clearing institutions.

Introduction to Blockchain

- Blockchain technology is the technology that:
  - permits transactions to be gathered into blocks and recorded;
  - cryptographically chains blocks in chronological order; and
  - allows the resulting ledger to be accessed by different servers.

Introduction to Blockchain (Conti..)

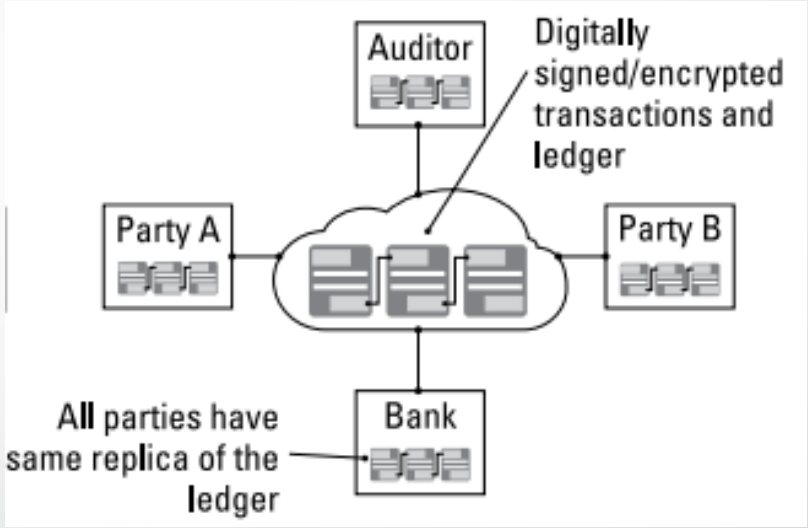
- With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records.



- This traditional method can be expensive, partially because it involves intermediaries that charge fees for their services.
- It's clearly inefficient due to delays in executing agreements and the duplication of effort required to maintain numerous ledgers.
- It's also vulnerable because if a central system (for example, a bank) is compromised, due to fraud, cyberattack, or a simple mistake, the entire business network is affected.

Introduction to Blockchain (Conti..)

- With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records.



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

Blockchain

A blockchain network has the following key characteristics:

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

Exploring a blockchain application

- Car companies make leasing a vehicle look easy, but in reality, it can be quite complicated.
- By using a shared ledger on a blockchain network, every participant can access, monitor, and analyze the state of the vehicle irrespective of where it is within its life cycle.

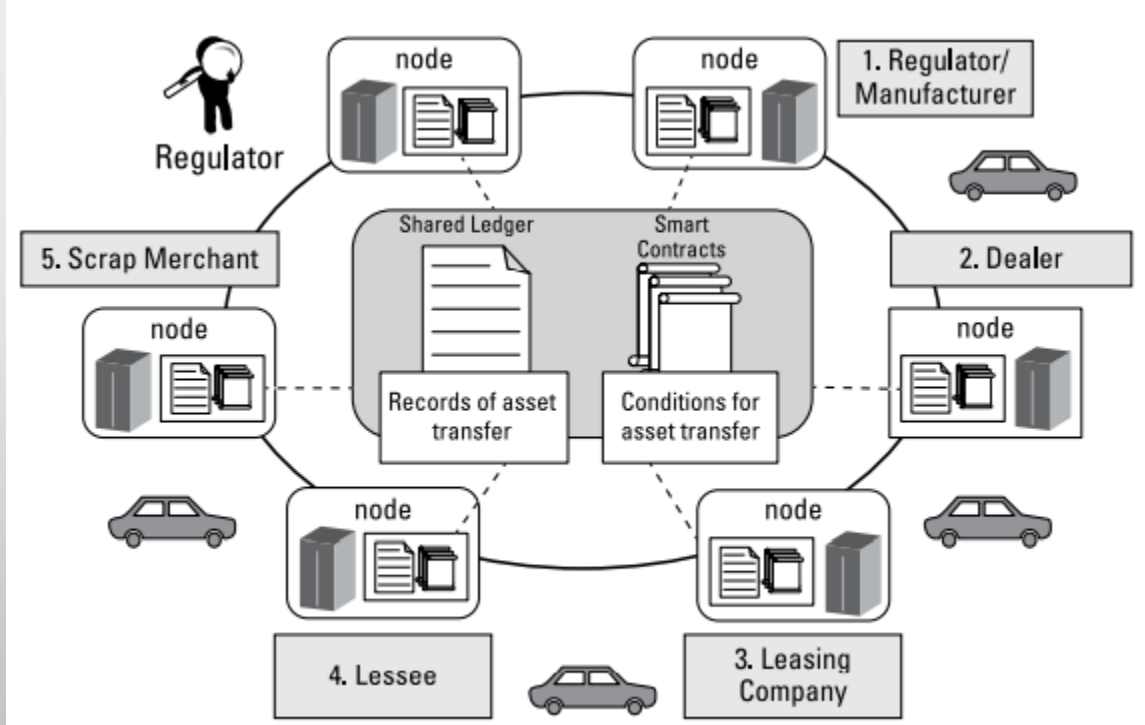


FIGURE 1-3: Tracking vehicle ownership with blockchain.

Exploring a blockchain application (Conti..)

- A significant challenge faced by today's car leasing networks is that even though the physical supply chain is usually integrated, the supporting systems are often fragmented.
- Each party within the network maintains its own ledger, which can take days or weeks to synchronize.

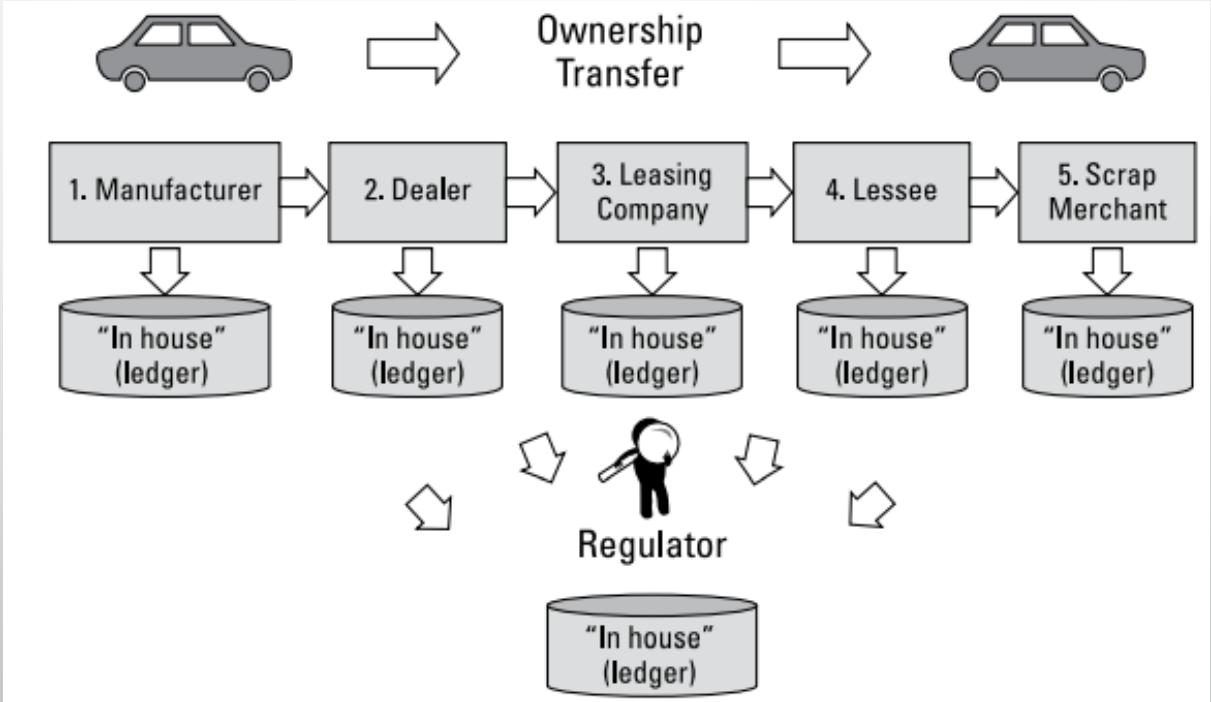


FIGURE 1-2: Tracking vehicle ownership without blockchain.

Recognizing the key business benefits

For business, blockchain has the following specific benefits:

- **Time savings**: Transaction times for complex, multi-party interactions are slashed from days to minutes.
- **Cost savings**: A blockchain network reduces expenses in several ways:
  - Less oversight is needed because the network is self-policed by network participants, all of whom are known on the network.
  - Intermediaries are reduced because participants can exchange items of value directly.
  - Duplication of effort is eliminated because all participants have access to the shared ledger.
- **Tighter security**: Blockchain's security features protect against tampering, fraud, and cybercrime. If a network is permissioned, it enables the creation of a members-only network with proof that members are who they say they are and that goods or assets traded are exactly as represented.

Recognizing the key business benefits (Conti..)

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

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

Building trust with Blockchain

- Blockchain enhances trust across a business network.
- It’s not that you can’t trust those whom you conduct business with; it’s that you don’t need to when operating on a blockchain network.
- Blockchain is particularly valuable at increasing the level of trust among network participants.
- Every transaction is built on every other transaction, any corruption is readily apparent, and everyone is made aware of it.
- This self-policing can mitigate the need to depend on the current level of legal or government safeguards and sanctions to monitor and control the flow of business transactions.
- Third-party oversight is required, blockchain reduces the burden on the regulatory system by making it easier for auditors and regulators to review relevant transaction details and verify compliance.

Building trust with blockchain (Conti..)

- **Distributed and sustainable**: The ledger is shared, updated with every transaction, and selectively replicated among participants in near real-time. Not owned or controlled by any single organization.
- **Secure, private, and indelible**: Permissions and cryptography prevent unauthorized access to the network and ensure that participants are whom they claim to be. Privacy is maintained through cryptographic techniques and/or data partitioning techniques to give participants selective visibility into the ledger; both transactions and the identity of transacting parties can be masked.
- **Transparent and auditable**: Because participants in a transaction have access to the same records, they can validate transactions and verify identities or ownership without the need for third-party intermediaries. Transactions are time-stamped and can be verified in near real-time.
- **Consensus-based and transactional**: All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Orchestrated and flexible**: Business rules and smart contracts can be built into the platform, blockchain business networks can evolve as they mature to support end-to-end business processes and a wide range of activities.

Taking a Look at How Blockchain Works

Why It's Called "Blockchain"

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

Why It's Called "Blockchain" (Conti..)

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

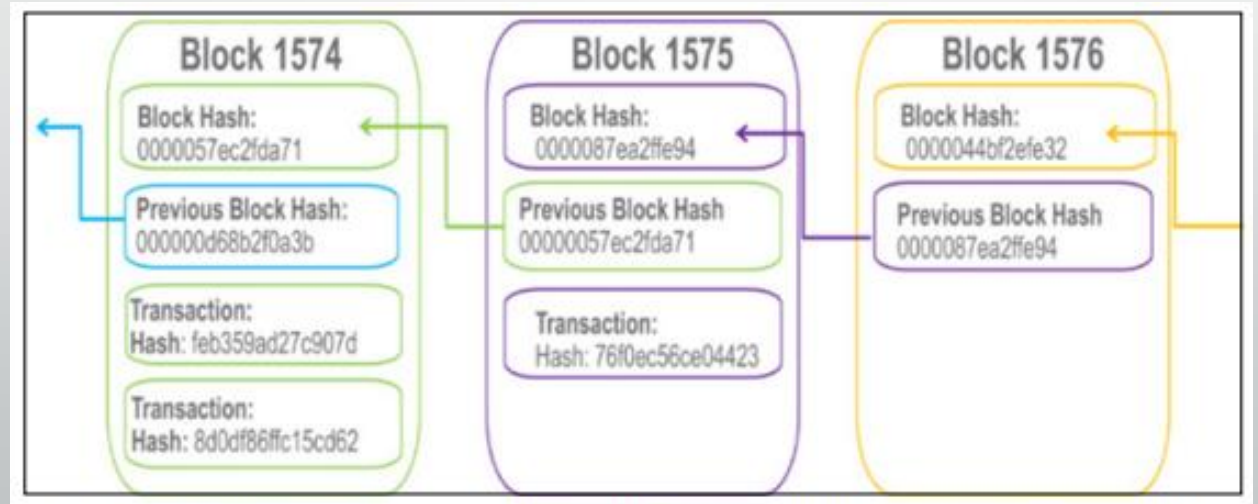


FIGURE 2-1: Blockchain stores transaction records in a series of connected blocks.

What Makes a Blockchain Suitable for Business?

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

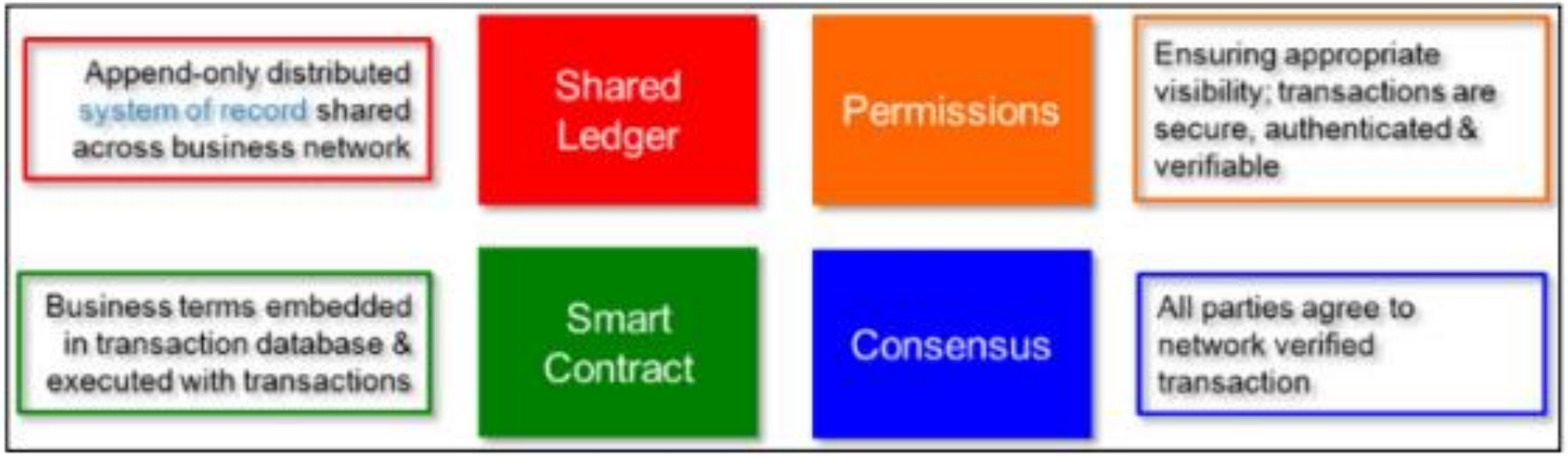


FIGURE 2-2: The key concepts of blockchain for business.

Why It's Called "Blockchain" (Conti..)

1. Shared ledger

- Ledgers are nothing new; they've been used in double-entry bookkeeping since the 13th century.
- Here the transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.
- The shared ledger has the following characteristics:
  - Records all transactions across the business network;
  - Is shared among all participants in the network; through replication, each participant has a duplicate copy of the ledger.
  - Is permissioned, so participants see only those transactions they're authorized to view. Participants have identities that link them to transactions, but they can choose the transaction information that other participants are authorized to view.

Why It's Called "Blockchain" (Conti..)

2. Permissions

- Blockchains can be Permissioned or Permissionless.
- Permissioned blockchain:
  - each participant has a unique identity, which enables the use of policies to constrain network participation and access to transaction details.
  - are also more effective at controlling the consistency of the data that gets appended to the blockchain.
- Example
  - if Party A transfers an asset to Party B, both Party A and Party B can see the details of the transaction.
  - Party C can see that A and B have transacted but can't see the details of the asset transfer.
  - If an auditor or regulator joins the network, privacy services can ensure that they see full details of all transactions on the network.

Why It's Called "Blockchain" (Conti..)

3. Consensus

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

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

Why It's Called "Blockchain" (Conti..)

4. Smart Contracts

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

Identifying Participants and Their Roles

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

- **Blockchain user:** A participant (typically a business user) with permissions to join the blockchain network and conduct transactions with other network participants.
- **Regulator:** A blockchain user with special permissions to oversee the transactions happening within the network. Regulators may be prohibited from conducting transactions.
- **Blockchain developer:** Programmers who create the applications and smart contracts that enable blockchain users to conduct transactions on the blockchain network. Applications serve as a conduit between users and the blockchain.
- **Blockchain network operator:** Individuals who have special permissions and authority to define, create, manage, and monitor the blockchain network.
- **Traditional processing platforms:** Existing computer systems that may be used by the blockchain to augment processing. This system may also need to initiate requests into the blockchain.
- **Traditional data sources:** Existing data systems that may provide data to influence the behavior of smart contracts and help to define how communications and data transfer will occur between traditional applications/data and the blockchain — via API calls, thru MQ style cloud messaging, or both.
- **Certificate authority:** An individual who issues and manages the different types of certificates required to run a permissioned blockchain. For example, certificates may need to be issued to blockchain users or to individual transactions.

Propelling Business with Blockchains

Recognizing Types of Market Friction

- Market friction is anything that impedes the exchange of assets — anything that adds costs or delays, such as taxes, regulations, bureaucracy, fraud, the involvement of intermediaries, delays in executing contracts, and so on.
- Various types of market friction impact different industries in different ways and to varying degrees.

Recognizing Types of Market Friction (Conti..)

1. Information frictions

Information frictions result from the following limitations:

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

Recognizing Types of Market Friction (Conti..)

2. Interaction frictions

- Interaction frictions arise when either the cost of the transaction is too high or the degree of separation (physical or otherwise) between parties is too great.
- Business transactions that take days and are costly to manage via intermediaries are prime candidates for disruption by nimbler competitors.
- Interaction frictions are often magnified by the number of interactions required.
- Blockchain's peer-to-peer architecture can often reduce the number of interactions or parties required to execute a transaction, thus reducing the number of potential sources of interaction friction.

Recognizing Types of Market Friction (Conti..)

3. Interaction frictions

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

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

Moving Closer to Friction-Free Business Networks

1. Reducing information friction

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

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

Moving Closer to Friction-Free Business Networks

2. Easing interaction friction

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

- **State-based communication**: Today, banks communicate via secure messaging architecture, such as SWIFT, to accomplish tasks, with each bank maintaining its state of the task locally.
- **Peer-to-peer (P2P) transactions**: Participants exchange assets directly, without having to process the transaction through intermediaries or a central point of control → reducing the costs and delays associated with the use of intermediaries.
- **Consensus**: In place of intermediaries, blockchain uses consensus algorithms to validate and authorize transactions. Participants can conduct business at a pace of their business decisions.
- **Smart contracts**: Smart contracts eliminate the hassles and delays inherent in contracts by building the contract into the transaction. Through smart contracts, the blockchain establishes the conditions under which a transaction or asset exchange can occur.

Moving Closer to Friction-Free Business Networks

Easing innovation friction

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

- **Eliminate the cost of complexity**: As an organization's operations become increasingly complex, blockchain eradicates the cost of complexity and ultimately redefines the traditional boundaries of an organization.
- **Reduce costs and delays of regulatory processes**: Automation can't entirely eliminate governance through regulation, but it can lower the costs and reduce delays inherent in regulatory processes
- **Expand opportunities**: Blockchain can be both good and bad for businesses by providing the technology that enables businesses to develop new competitive business models. Some businesses will fail, while others redefine entire industries.

Moving Closer to Friction-Free Business Networks

Easing innovation friction

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

- **Eliminate the cost of complexity**: As an organization's operations become increasingly complex, blockchain eradicates the cost of complexity and ultimately redefines the traditional boundaries of an organization.
- **Reduce costs and delays of regulatory processes**: Automation can't entirely eliminate governance through regulation, but it can lower the costs and reduce delays inherent in regulatory processes
- **Expand opportunities**: Blockchain can be both good and bad for businesses by providing the technology that enables businesses to develop new competitive business models. Some businesses will fail, while others redefine entire industries.

Blockchain in Action: Use Cases

Financial Services

Commercial financing

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

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

The benefits of implementation are:

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

Financial Services

Trade finance

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

The benefits for trade finance include the following:

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

Financial Services

Cross-border transactions

- Banks need a way to manage nostro/vostro accounts.
- Nostro (ours) refers to an account a domestic bank holds in a foreign bank in the foreign country's currency.
- Vostro (yours) is how the foreign bank refers to that account. Such accounts are used to facilitate and simplify trade and foreign exchange transactions through reconciliation.

The benefits are:

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

Financial Services

Insurance

- Insurance providers need an efficient way to process claims, verify that an insurable event (such as an accident) actually occurred, and provide customers with fair and timely payouts.
- With automated insurance claim processing, policy conditions are written into a smart contract stored on the blockchain and connected to publicly available data via the Internet.

The benefits of implementation are:

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

Financial Services

Government

- A considerable amount of government involves recording transactions and tracking ownership of assets, all of which can be made more efficient and transparent through the use of blockchain.
- Organizations can apply blockchain by issuing digitally authenticated birth certificates that are unforgeable, time-stamped, and accessible to anyone in the world.

The benefits of implementation are:

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

Financial Services

Supply Chain Management

- When something goes wrong with a complex “system of systems,” such as an aircraft, it’s important to know the provenance, through supply chain management, of each component, down to the manufacturer, production date, batch, and even the manufacturing machine program.
- Blockchain holds complete provenance details of each component part, accessible by each manufacturer in the production process, the aircraft owners, maintainers, and government regulators.

The benefits of implementation are:

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

Financial Services

Healthcare

- The healthcare industry needs a more efficient and secure system for managing medical records, pre-authorizing payments, settling insurance claims, and performing and recording other complex transactions.
- Electronic medical records are currently maintained in data centers (in a cloud-like environment), and access is limited to hospital and care provider networks.
- Centralization of such information makes it vulnerable to security breach and can be expensive.
- Blockchain holds the complete medical history for each patient, with multiple granularities of control by the patient, doctors, regulators, hospitals, insurers, and so on, providing a secure mechanism to record and maintain

Financial Services

Healthcare

The benefits are:

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

Financial Services

The Internet of Things (IoT)

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

The benefits are:

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

Hyperledger, a Linux Foundation Project

Hyperledger

History

- Hyperledger, a Linux Foundation project, is an open-source community to help advance technology and thought leadership.
- It is deemed an “umbrella” for developer communities building open-source blockchain and related technologies.
- Hyperledger was announced and formally named in December 2015 by 17 companies in a collaborative effort created to advance blockchain technology for cross-industry use in business.
- Hyperledger is curated by the Linux Foundation, which provides tools, training, and events to scale any open source project.
- IBM initially contributed what was then called Open Blockchain and is now called Fabric, and arguably that is the biggest/highest profile project.

Hyperledger

Hyperledger Vision

- To provide robust and efficient standards for blockchain ledger technology to facilitate mainstream commercial adoption.
- Another goal is to provide a modular blockchain technology that contains a rich, easy-to-use application programming interface (API) and numerous core modules that enable easy development and interoperability.

HYPERLEDGER Vs HYPERLEDGER FABRIC

- **Hyperledger** is an open-source, collaborative effort to create blockchain technology suitable for the enterprise.
- **Hyperledger Fabric** is an open-source platform for developing blockchain solutions with a modular architecture and pluggable, interchangeable services using container technology.

The primary goals of Hyperledger Fabric are to

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

HYPERLEDGER FABRIC

- Hyperledger Fabric provides a framework for developing blockchain solutions with a m[illegible] architecture, pluggable implementations, and container technology.
- While leveraging open-source best practices, Hyperledger Fabric enables confidentiality, scalability, and security in business environments.
- Unlike other blockchain implementations like Bitcoin or Ethereum, Hyperledger Fabric is the only one that fulfills all four key elements of a blockchain for business:
  - **Permissioned network**: Collectively defined membership and access rights within your business network
  - **Confidential transa**ctions: Gives businesses the flexibility and security to make transactions visible to select parties with the correct encryption keys
  - **Doesn’t rely on cryptocurrencies**: Doesn’t require mining and expensive computations to assure transactions
  - **Programmable**: Leverages the embedded logic in smart contracts to automate business processes across your network

How Can IBM Help Developers Innovate With Blockchain?

Offering an easily accessible cloud and development platform

- Implementing blockchain solutions on IBM Cloud is the quickest way to get started.
- IBM has a number of cloud-based solutions to enable you to easily develop applications while testing the security, availability, and performance of a permissioned blockchain network.
- IBM blockchain networks are built to benefit from decentralized control, but some cloud environments are open to vulnerabilities.
- Working with teams of security experts, cryptographers, hardware experts, and researchers, IBM has created essential cloud services for tamper-resistant, trusted blockchain networks.

How Can IBM Help Developers Innovate With Blockchain

IBM Blockchain on Bluemix

- You can create and deploy a blockchain network based on Hyperledger Fabric.
- Offers a high-security plan that provides an isolated environment for business networks.
- Offers high levels of security that close any back doors to unauthorized access and tampering.
- Key features of the plan include:
  - Protects host administrators and provides proof to ensure the blockchain executes in an agreed-upon manner.
  - High evaluation assurance level enables protection across environments where blockchain peers run in isolation from other peers and parties. This prevents leaks into another party's environment.
  - Crypto-optimization supports an environment that moves hashing and the creation of digital signatures to optimized accelerators that don't drain CPU performance.
  - FIPS 140-2 (the highest Federal Information Processing Standard) supports the use of blockchain in regulated industries such as government, financial services, and healthcare.)

How Can IBM Help Developers Innovate With Blockchain

Hyperledger Fabric images on DockerHub

- Alternatively, you can pull Hyperledger Fabric images directly from Docker Hub to create and manage your own local blockchain network.
- Set up and run a blockchain network with IBM-certified Docker Compose script and images.
- For more detailed instructions on how to get started, visit http://ibm.biz/QuickStartGuide.
- After you've deployed a network, you're ready to build your first chaincode!
- To earn your chaincode badge, take this course: http://ibm.biz/BlockchainChaincodeCourse.

Ten Steps to Your First Blockchain application

Deciding Whether Blockchain Has a Place in Your Industry

Deciding Whether Blockchain Has a Place in Your Industry

If you're uncertain of whether blockchain has a place in your industry, answer the following questions:

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

Deciding Whether Blockchain Has a Place in Your Industry

Identifying Speed Bumps in Business Processes

- Examine your current business processes for inefficiencies, particularly steps in the process that are prone to delays, frustration, errors, and duplication of effort.

Determining How Blockchain Can Help

- After identifying challenges in your transaction network, consider various attributes of blockchain that can address the inefficiencies, costs, and other issues.
- For example, if a lack of trust is causing friction, blockchain's shared ledger can provide increased visibility into transaction and asset histories to improve trust.

Deciding Whether Blockchain Has a Place in Your Industry

Choosing an Appropriate Use Case

- When choosing a use case, make sure it's a good fit for what you're trying to accomplish — something that adds real value as opposed to something that could be achieved just as well using a mature technology.
- Your use case needs to pass the following four acid tests:
  - **Consensus**: Does agreement across the business network that each transaction is valid provide some benefit?
  - **Provenance**: Is the maintenance of a complete audit trail important?
  - **Immutability**: Is it important that the train of transactions is tamper-evident?
  - **Finality**: Is there a need for an agreed "system of record" across the business network?

Deciding Whether Blockchain Has a Place in Your Industry

Determining the Goal of Your Blockchain Network

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

Identifying Dependencies

- When you have an appropriate use case in mind, consider what else you need, in addition to internal resources you already have, to start on your first blockchain project.
- Do you need a services partner to help deploy the first project?
- Do you need a platform or fabric that enables you to meet certain regulatory or compliance objectives?

Deciding Whether Blockchain Has a Place in Your Industry

Choosing a Blockchain Provider and Platform

- Choose a provider and platform that are the best fit for your industry and business needs.
- As you compare the suitability of different providers and platforms, seek answers to the following questions:
  - Do you require a permissioned network?
  - Do you need to know the identities in your business network? For example, to adhere to regulations such as anti-money laundering (AML) or know your customer (KYC)?
  - Do you have frequent exchanges with others that could be automated and pre-programmed, freeing up valuable time and resource?
  - Would you benefit from transaction resolution in minutes rather than days or weeks?

Deciding Whether Blockchain Has a Place in Your Industry

Developing and Deploying Chaincode

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

Testing and Fine-Tuning Your Application and Network

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

Thank You