MDS 区块链考试

期末考：闭卷 90min，可以带资料，占比 40%
期中考了什么，期末会考什么：真假题(注意归类，一般没有明显错可以对？)，选择题（emm 好好选）
看图说话题，network diagram；情境题，给一个 network system，assets，participants，transactions
短问题回答

概念

Hash：Hash algorithms are what keeps blockchain secure. A hash algorithm takes data of any size and converts it into a fixed alphanumeric string based on the hash function (64-bit/128-bit/256-bit) used. This fixed size output is called a hash.
The same hash can be generated from the same input data. Any small change to the data will completely change the hash output.

PoW： Proof of work (PoW) is **a form of adding new blocks of transactions to a cryptocurrency's blockchain**. The work, in this case, is generating a hash (a long string of characters) that matches the target hash for the current block.
In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network.
PoS: With proof-of-stake (POS), cryptocurrency owners validate block transactions based on the number of coins a validator stakes. Proof-of-stake (POS) is seen as less risky in terms of the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantageous.

51%： A **51% attack** refers to an **attack** on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power.

Gossip： A **gossip** protocol or epidemic protocol is a procedure or process of computer peer-to-peer communication that is based on the way epidemics spread.

Signature： Digital **signatures** are a fundamental building block in **blockchains**, used mainly to authenticate transactions

Domain-specific language： A Domain Specific Language is a programming language with a higher level of abstraction optimized for a specific class of problems. A DSL uses the concepts and rules from the field or domain. （less complex than general-purpose language: Java, C, Ruby） **Solidity**

Consortium chain: The **consortium** blockchain is a system that is 'semi-private' and has a controlled user group, but works across different organizations. A blockchain consortium of like-minded companies can leverage information to improve workflows, accountability, and transparency.

Merkle tree: A Merkle tree is a hash-based data structure that is a generalization of the hash list. It is a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children Merkle trees are used in distributed systems for efficient data verification.
index to verify block chain transactions

Smart Contract: A smart contract is code, invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the World State
Chaincode： a program tied to a business process that accesses a blockchain
program code that implements the application logic and runs during the execution phase.

Marshal: To arrange to order 序列化？Programming II – p32

CCKit: programming toolkit for developing and testing Hyperledger Fabric Golang chaincodes.

Turing complete: any real-world general-purpose computer or computer language can approximately simulate the computational aspects of any other real-world general-purpose computer or computer language.

A Turing Complete system means a system in which a program can be written that will find an answer of a computational problem
a programing language is called "Turing complete", if it can run any program
LevelDB & Couch DB: LevelDB is an open-source on-disk key-value store. Apache CouchDB is an open-source document-oriented NoSQL database. **LevelDB** is the default key-value state database embedded in the peer process. **CouchDB** is an alternative external state database

TDD: Test-Driven development automated unit tests—are used to guide, or drive, the development of the production code. Programming III - 22 Build the thing right
BDD: Behavior-Driven Development to foster collaboration between the different actors involved in the software process developer-centric process higher-level and more business-oriented approach. Build the right thing

MockStub: MockStub is an implementation of ChaincodeStubInterface for unit testing chaincode.

Consensus: full-circle verification of the correctness of a set of transactions comprising a block
A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems Consensus – p17 (SOLO, Kafka, Raft – p16)

ZKP: p27/30 a cryptographic technique where no information is revealed during a transaction except for the interchange of some value known to both the prover and verifiers (the two ends of the process)

Next-gen file system controls

ZKPs can help in adding multiple layers of security to files, logins. As a result, ZKPs can present notable obstacles for hackers or manipulators to alter and retrieve the data.

Data Security

Organizations that control sensitive data, such as banks and hospitals, must keep them free from third-party access. ZKPs and blockchain together can make accessing data impossible.

Public Key & Private Key: The public key is used to send cryptocurrency into a wallet, it allows you to receive cryptocurrency transactions. The private key is used to verify transactions and prove ownership of a blockchain address. If someone sends you, say one bitcoin (BTC), a private key will be required to “unlock” that transaction and prove that you are now the owner of that bitcoin.

Secret Key: A secret key is the piece of information or parameter that is used to encrypt and decrypt messages in a symmetric, or secret-key, encryption.

Hyperledger Sawtooth: modular platform for building deploying, running distributed ledgers, Intel, an open source blockchain project under the enterprise platform Hyperledger pertent solution for developing networks and distributed ledger applications

Hyperledger Grid: ecosystem of lib, frameworks, tech, enable solve supply chain problems. a platform for building supply chain solutions that include distributed ledger components

Ethereum: Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether is the native crypto-currency of the platform. Among crypto-currencies, Ether is second only to Bitcoin in market capitalization. Ethereum was conceived in 2013 by programmer Vitalik Buterin

Endorsement: a condition on what endorses a transaction. consensus p17 Every chaincode has an endorsement policy which specifies the set of peers on a channel that must execute chaincode and endorse the execution results in order for the transaction to be considered valid.

1. **What is machine trust, and how does blockchain achieve machine trust?**

   Machine trust is a term mentioned in the Economist's article on Oct 31, 2015 -- *The Trust Machine*. In general, machine trust is to use computer algorithms to guarantee certain governance procedure without human interference. For instance, Bitcoin uses the proof-of-work consensus algorithm to select bookkeepers and ensure accurate maintenance of the Bitcoin accounts and exchanges.

2. **Discuss the importance of nonce in the consensus algorithm under proof-of-work.**

   Nonce is a number that used to achieve a given pattern of Hash value in the proof-of-work process. Determinacy of a particular nonce requires brute-force computation that can take about 10 minutes with a powerful mining computer under certain Bitcoin mining difficulty. This time-consuming process of proof-of-work helps make Bitcoin tamper-proof, and that is why Bitcoin has been running successfully over the past 12 years.

概念-解释-例子
概念-如何形成-作用-影响

Bitcoin:

Bitcoin (฿) is a decentralized digital currency, without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Blockchain 1.0 Bitcoin? Consortium blockchain is an instance of Blockchain 1.0. False!! Bitcoin 是 public，联盟链不属于 1.0
Blockchain 2.0 Ethereum (Smart Contract)
Blockchain 3.0 Hyperledger Programmable society
Bitcoin → Ethereum → Fabric

Ethereum is a system that is Turing-complete because it can be used to create blockchains (solve a problem). 对的。。。

Consensus algorithm: Proof of Work, Proof of State/Elapsed Time, Proof of Activity/Burn/Capacity/Importance

Hyperledger composer: 三大元素：**Assets**；**Participants**；**transactions** Register 也算是 transaction

练习：
四种类型：Public, Private, Consortium, Hybrid (real estate) [federated?]
Companies can utilize a hybrid blockchain to run systems securely while exposing certain information to the public, such as listings.

Blockchain 分成两个 path：**fork**。 Unanimous Consensus: verified. Single chain split (soft fork, hard fork, temporary fork: two miners mine a new block at the same time)

Bitcoin 创始人：Satoshi Nakamoto

Blockchain component: Node (Transaction: Full, partial), Ledger (digital database: Public, Distributed, Decentralized)
Wallet: user store crypto currency (Hot Cold) Nonce: number added to a hashed or encrypted block
Hash: data=>fixed size through hashing **No certificate authority**

Block: 密码 hash，时间戳，交易数据
Blockchain 的支柱：Decentralization (no central authority), Transparency (transaction public), Immutability

---

Bitconin 的脚本语言：stack-based　FILO　不是 Turing complete！！serve special purpose. Finite time, zero memory.

Hash pointers: build a linked list, whole data of the previous block, include hash pointer to the one even before
Hash 算法：SHA256

Immutability：　improved security?
Tokens: platform, privacy, currency
Blockchain: flat file & database
Miner: computers that validate and process blockchain transactions

Asymmetric encryption: RSA

Assignment

1：区块链和传统数据库的区别；区块链会比传统交易系统更慢吗？区块链应用的优缺点；源头造假 no，51%攻击. 信息透明度，信息公开，信息流转，防止篡改

i Traditional database is centralized, and there is central authority controlling the system. Blockchain is distributed, the data spread across a network, there is no central authority to mediate disputes for public chain. The transaction relationship is peer-to-peer.

ii Traditional database usually has only one copy (some database may have 2 or 3 to ensure reliability). Blockchain has multiple duplication of the data, and its redundancy level is high.

iii In traditional database, data can be modified, deleted easily. In blockchain, write operation is irreversible and no modification on written information. Data can only be appended to the blockchain but cannot be edited or deleted.

iv Traditional database can organize the data in any logical order. Blockchain is organized as chain in chronological order. Each block contains a "hash" of the previous block. Transactions (data) on the blockchain are time stamped, making it useful for tracking and verifying information.

v In traditional database, the data is usually private and not disclosed to others. In blockchain, every transaction is completely public, and everyone can check data and their history.

vi Traditional database records the data manually without verification. Blockchain uses consensus mechanism to record data, and transactions must be verified and agreed upon as valid by majority of the network.

vii Traditional database uses account-password to secure. It is vulnerable to frauds and cyber crime.Blockchain uses dual-key encryption, cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights, which can avoid malicious activities in the network.

Some people argue that blockchain is slower than traditional transaction system. State your opinion about this argument in terms of correctness and reasons. (30 points)

Correctness: My opinion is **NO**.

Reasons:

i Traditional transaction system requires third-party's involvement or verification, costing lengthy settlement time. Blockchain transaction is point-to-point, without third-party and time-consuming verification procedure.

ii Traditional uses manual or electronic contract to ensure trust, which may take days to agree and sign. Blockchain uses smart contract, which is automatically executed and can process in minutes.

iii Traditional transaction requires manual remittance or escrow. Blockchain uses consensus process to enable payment exchanges and remittance without need of centralized clearing house automatically.

iv Traditional database costs great time to handle trick or accidents. Blockchain can check the authenticity easily and avoid errors caused by manual and accidents, no lawyer is required.

v Take an example: SWIFT takes 3 to 5 days to send money internationally. Ripple sends money in seconds / minutes. Ripple reduces settlement risks, eliminates intermediaries, midpoint failure, delays. It provides instant, bilateral and straight through processing.

Application: Ant chain in Alibaba. Product provenance and lifetime history and real-time tracing. Facilitates chain of custody process for products in the supply chain where the party in custody is able to log evidence about the product.

) **Advantages**: Real-time checking; Easy to trace the origin and find responsibility holder; Consistent; Efficient; Transparency, information can flow through each party easily; Trust-worthy, no modification on data; Security; Resilient.

Limitations: Cannot avoid data origin forge or make sure the offline items/transactions are real; Relatively slow processing, not suited for high-performance transactions (in milliseconds); Not a solution for one participant, only make sense in business network; Not suited for low-value, high volume transactions; Not a messaging solution.

2：评估框架 assessment framework：七个点；UML use cases

Supply chain trace system

1 Intermediary: Yes - intermediaries such as third-party inspection agencies are added for trust in responsibility confirmation, and increase latency, fees, human resources.

2 Transparency: Yes - raw material supplier, product manufacturer, logistic provider, distributor, retailer, customer, etc. are involved in the supply chain and transaction. Higher transparency would increase trust in the system, and speed up the trace process when quality problems happen.

3 Golden Source: Yes - common information such as product id, product size, temperature, humidity, weight, produce time is stored across the participants such as supplier, manufacturer, logistic provider and retailer. Product information has to be gathered from multiple sources for tracing. Each member also stores a copy of the product details.

4 Manual Processing: Yes - it is required throughout the life-cycle of the process, which is paper-intensive with product details. Manual processing is performed at the product record.

5 Trust: Yes - multiple participants are involved in the supply chain and upload information/ issue update. Since these may be unknown to each other, there is a lack of trust and possibility of fraudulent activities.

6 Authentication: Yes - The product information, validations report, logistic address, bills, etc. are all paper-based and require documentation. This is not due to regulatory reporting requirements. 7 Time Sensitivity: Yes - it will help in providing enhanced customer experience and responsibility confirmation process, and reduce the exposure risk of quality problems if the recording process is in real time.

Lab

Participants – assets – transactions

Composer – tool, fabric – framework (can customize detail)

Hyperledger Composer provides a set of user-friendly tools for defining blockchain business models and testing models, which supports the existing Hyperledger Fabric blockchain infrastructure and runtime. Hyperledger Fabric provides a set of components for running a blockchain network.

Hyperledger Composer is an extensive, open development toolset and framework to make developing blockchain applications easier

Hyperledger Fabric is a powerful framework for developing permissioned blockchain and Hyperledger Composer is a popular tool to build blockchain business network

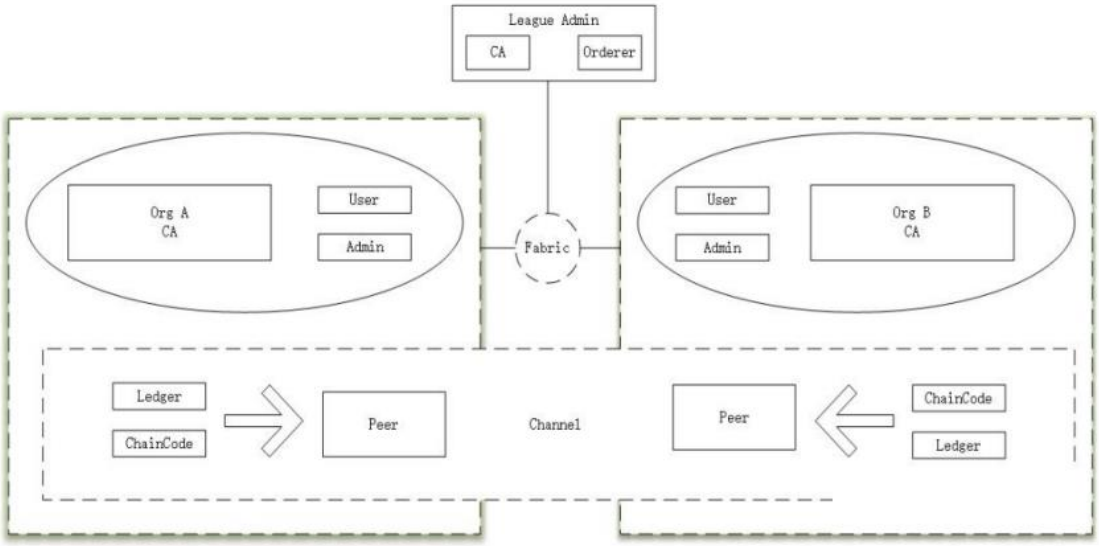
Hyperledger Fabric is a modular and extensible open-source system for deploying and operating permissioned blockchains

technical tools: Composer Modeling Language, JavaScript, Json data format, Linux command, Fabric peer command

permissoned!!

Representational state transfer (REST) is a software architectural style that defines a set of constraints to be used for creating Web services.

Ledger: A ledger is a channel's chain and current state data which is maintained by each peer on the channel.



chaincode is deployed and runs on fabric network, which might be constituted by several nodes. **Fabric SDK** (Software Development Kit) provides interface for web service to manipulate chaincode deployed.

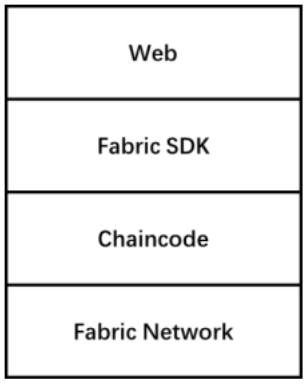


Figure 1. Layers of Fabric-based Blockchain Web Service

Channel: A Hyperledger Fabric channel is a private "subnet" of communication between two or more specific network members, for the purpose of conducting private and confidential transactions. A channel is defined by members (organizations), anchor peers per member, the shared ledger, chaincode application(s) and the ordering service node(s).

Channel: A channel is a private blockchain overlay which allows for data isolation and confidentiality. (C1, C2)

Ledger: A ledger consists of two distinct, though related, parts – **a "blockchain" and the "state database",** also known as "world state". (L1, L2)

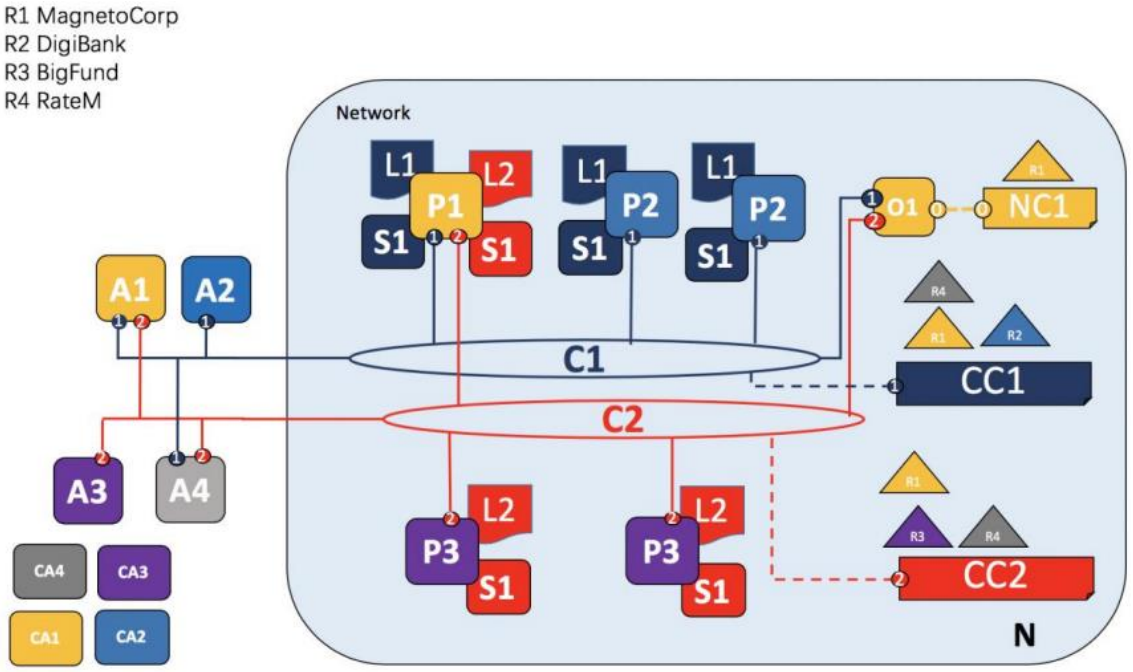
Ordering Service (Orderer Node): A defined collective of nodes that orders transactions into a block. (O4)

Certificate Authority: Certificate Authority (CA) issues the certificates for organizations to authenticate to the network.

Smart Contract: A smart contract is code – invoked by a client application external to the blockchain network – that manages access and modifications to a set of key-value pairs in the World State. (S5, S6)

R: organization L: ledger P: peer node
N: network NC: network configuration CC: channel configuration
A: client application O: ordering service
C: channel CA: certificate authority S: Smart Contract

Network diagram



- Four **organizations** in the network: **R1, R2, R3 and R4** R1 is the network initiator with **network configuration NC1.**
- R4 does not do transactions but only **query information**.
- Two **channels**: C1 for R1, R2 and R4 and C2 for R1, R3 and R4.

* **Four Applications, A1 to A4 for R1 to R4**, respectively. 一个 application 对应一个 organization

- A1 does issue/redeem/query on **C1 and C2**, A2 (A3) does buy/sell/query on C1 (C2), and A4 does query on C1 and C2.
- **Peer node P1 maintains ledger L1 in C1 and ledger L2 in C2**, and Peer node P2 (P3) maintains ledger L1 (L2).
- **Network N is governed with NC1 controlled by R1**.
- Channel C1 (C2) is governed by **channel configuration CC1** (CC2) and controlled by R1, R2, R4 (R1, R3, R4).
- **Ordering service O1** is for network N under the system channel and supports **channels C1 and C2.**
- Each of {R1, R2, R3, R4} has a preferred **Certificate Authority**.

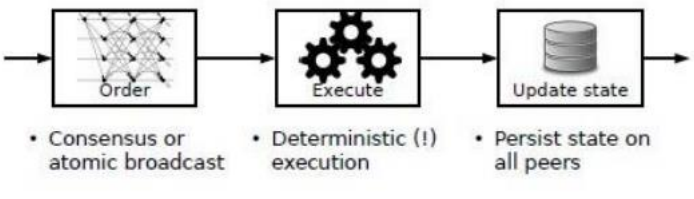
It supports modular consensus protocols, smart contracts written in standard and general-purpose programming languages, and it doesn't have to systemically depend on a native crypto currency.

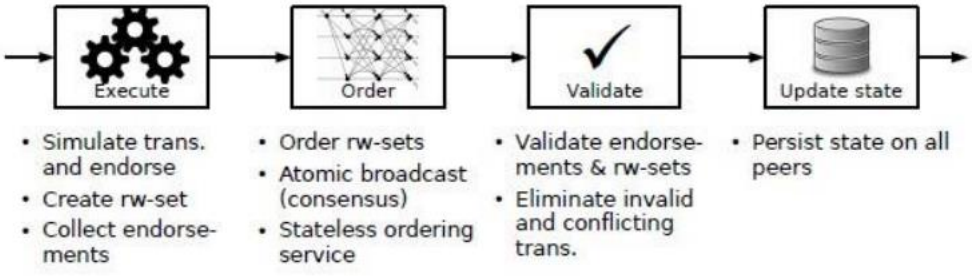
Fabric has several distinct features [1]: 1. Modular design. 2. Identity and membership. 3. Execute-order-validate paradigm. 4. Supporting smart contracts written in general-purpose programming languages.

Architecture: What is **order-execute architecture**?

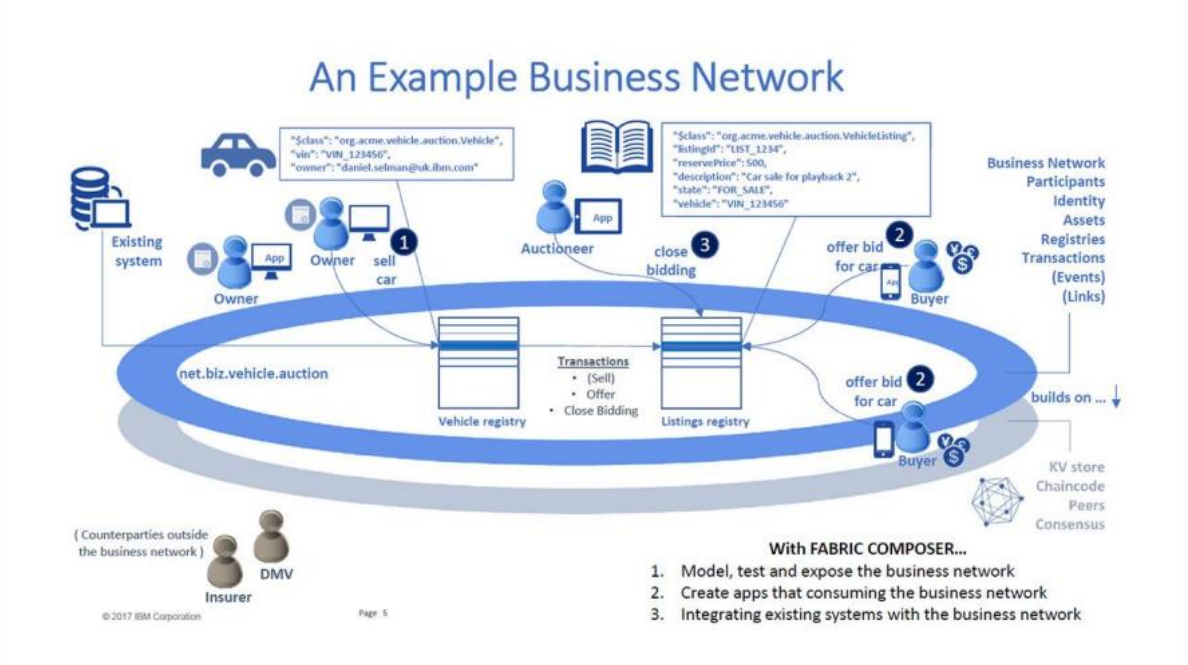
the blockchain network orders transactions first, using a consensus protocol, and then executes them in the same order on all peers sequentially.

(1) every peer (i.e., a node that participates in consensus) assembles a block containing valid transactions (to establish validity, this peer already pre-executes those transactions);
(2) the peer tries to solve a PoW puzzle;
(3) if the peer is lucky and solves the puzzle, it disseminates the block to the network via a gossip protocol;
(4) every peer receiving the block validates the solution to the puzzle and all transactions in the block.





The chaincode is the central part of a distributed application in Fabric and may be written by an untrusted developer. Special chaincodes exist for managing the blockchain system and maintaining parameters, collectively called system chaincodes.



Given the business network above, what elements do you see that can be modelled with an Enterprise Business Network model in Hyperledger Composer and how. Please apply what you have learned in the lectures and the labs.

assets: vehicles, listings

Participants: Owner, Auctioneer, Buyer

Transactions: Register, Sell, Offer, Close Bidding

General Transaction Flow is shown below:

1) The car owner runs register function by submitting the information about the vehicle, where the original owner will fill in the VIN and initiate the class: org.acme.vehile.auction.Vehicle. The ownership will automatically be certified with the owner's identity. (Possible verification from DMV/Insurer)

2) In the Vehicle registry, entries will be created accordingly whilst Step 1 is done. Or the record is directly imported from the existing system.

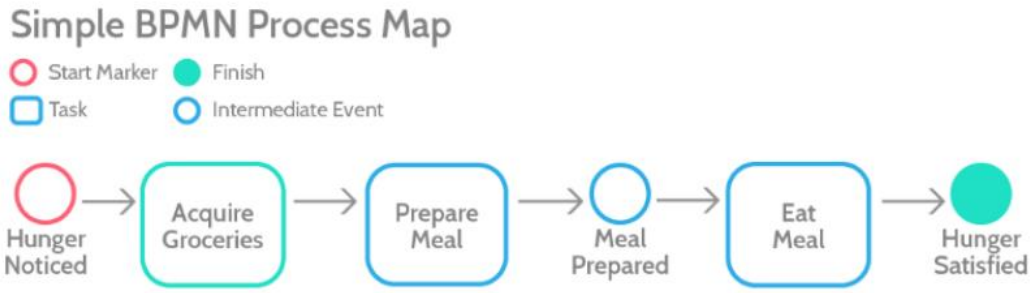
3) Next, listing registry will be updated when the seller uses the sell function and the auction begins. Information such as description from Vehicle Registry will be used in an entry of listing. The listing entry also entails the reserve price, listingId. Also, class:org.acme.vehicle.auction.VehicleListing will be instantiated. And the state for the listing is marked as FOR_SALE.

4) Then, buyers can browse the current available listings and offer bid for their interests with Offer function.

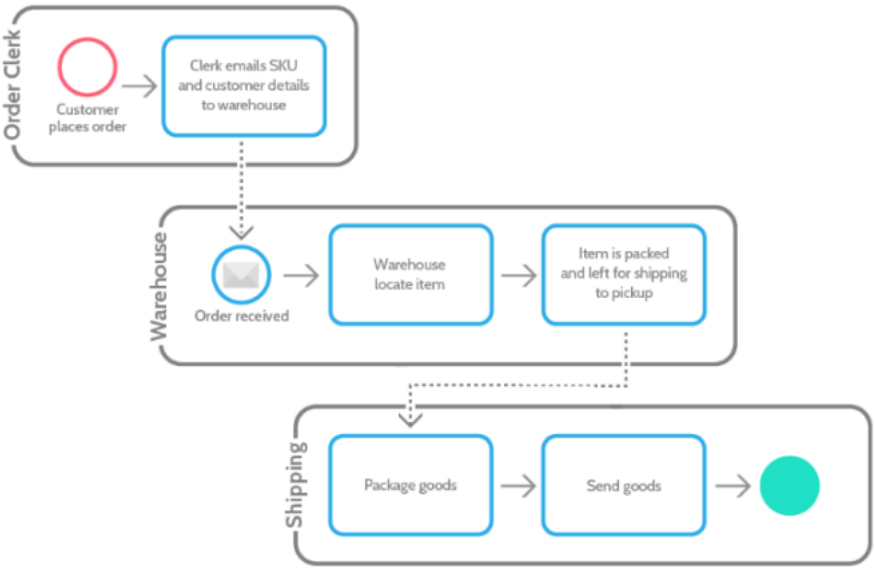
5) Finally, the auctioneer announces the close of the auction by function Close Bidding. The state of this listing is then set as CLOSED. The deal is either successfully made with the best offer or the reserve price has not been reached. This transaction flow is ended. (In this step, the insurance/ownership may be updated to outside counterparties such as DMV or Insurer)

看图说话

Business Process Modeling Notation (BPMN)1



Pools represent different organizations or entirely separate processes. Lanes represent different teams or individuals within the same organization. Pools are the biggest unit on a map: they're the areas that contain lanes, events, tasks, etc. They represent who is doing the task. • Each pool can contain a maximum of one process • Pools represent participants: companies, customers, or departments



- **Activity** is the work that is performed within a Business Process;

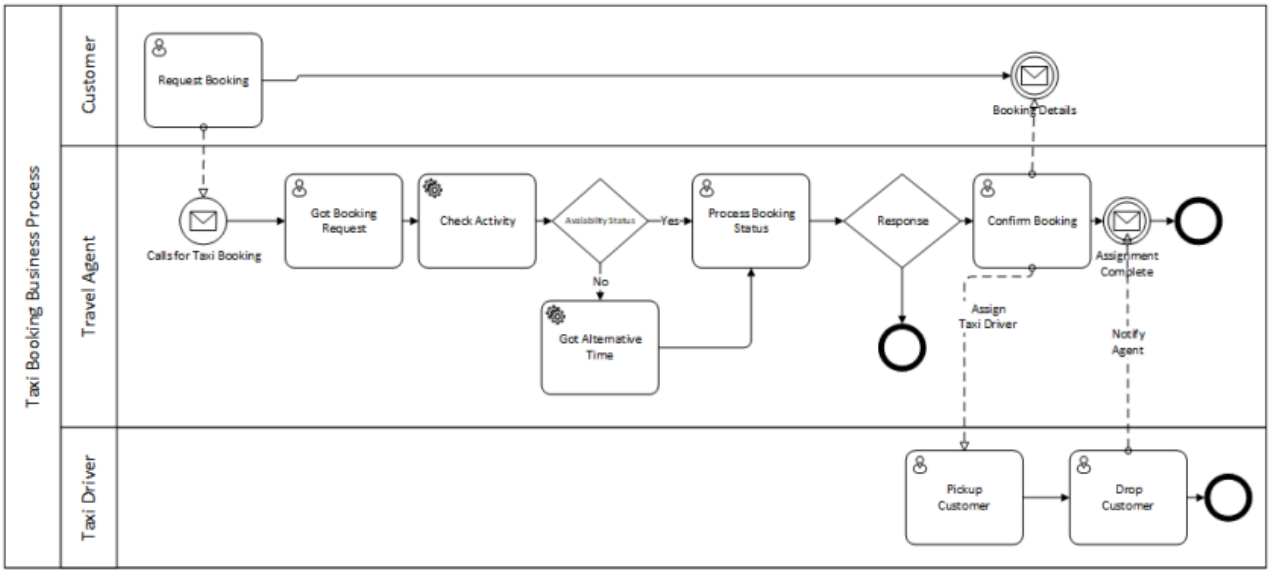
- **Event** is something happens during the Process;

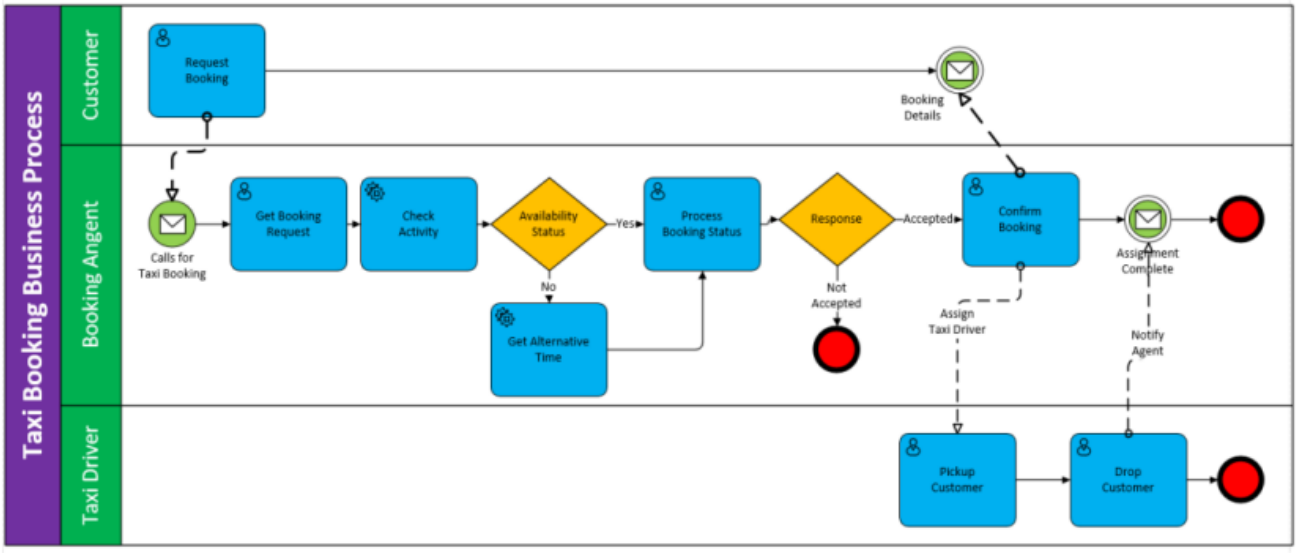
- **Gateway** is used to control the divergence and convergence of Sequence Flow in a Process;

- **Flow**:
  - Sequence Flow is used to show the order that Event will be performed in a Process;
  - Message Flow is used to show the flow of Message between the Participants of a Process;

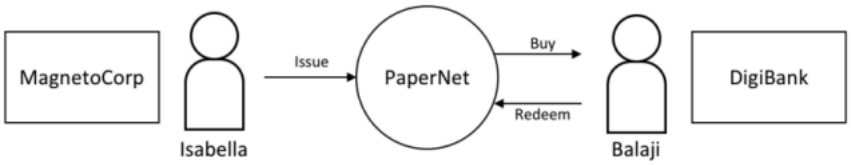
User Task: A User Task represents that a human performer performs the Task with the use of a software application.

Service Task: A Service Task is a Task that uses a Web service, an automated application, or other kinds of service in completing the task.



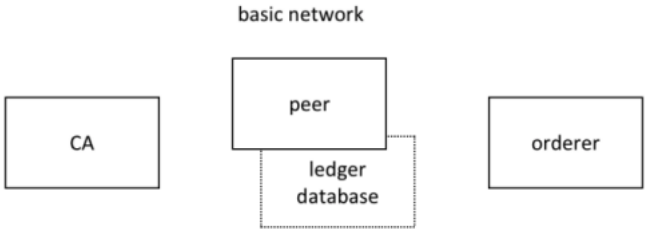


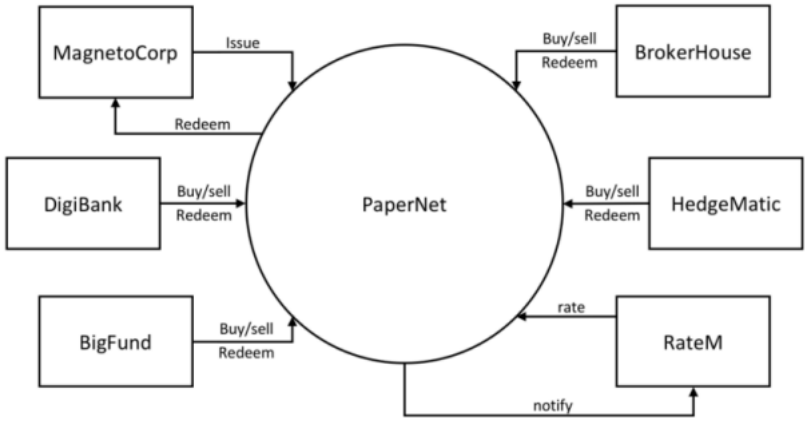
PaperNet



Commercial papers, usually issued by companies, are short-term negotiable documents, such as a bill of exchange, promissory note, etc., calling for the transference of a specified sum of money at a designated date

The basic Fabric network has been set up already, and you will play two commercial roles for both parties in PaperNet. • First, you'll act as Isabella, an employee of MagnetoCorp, who will issue a commercial paper on its behalf; • You'll then switch to the role of Balaji, an employee of DigiBank, who will buy this commercial paper, hold it for a while; • Then you, in the role of Balaji, redeem this commercial paper with MagnetoCorp for a small profit.

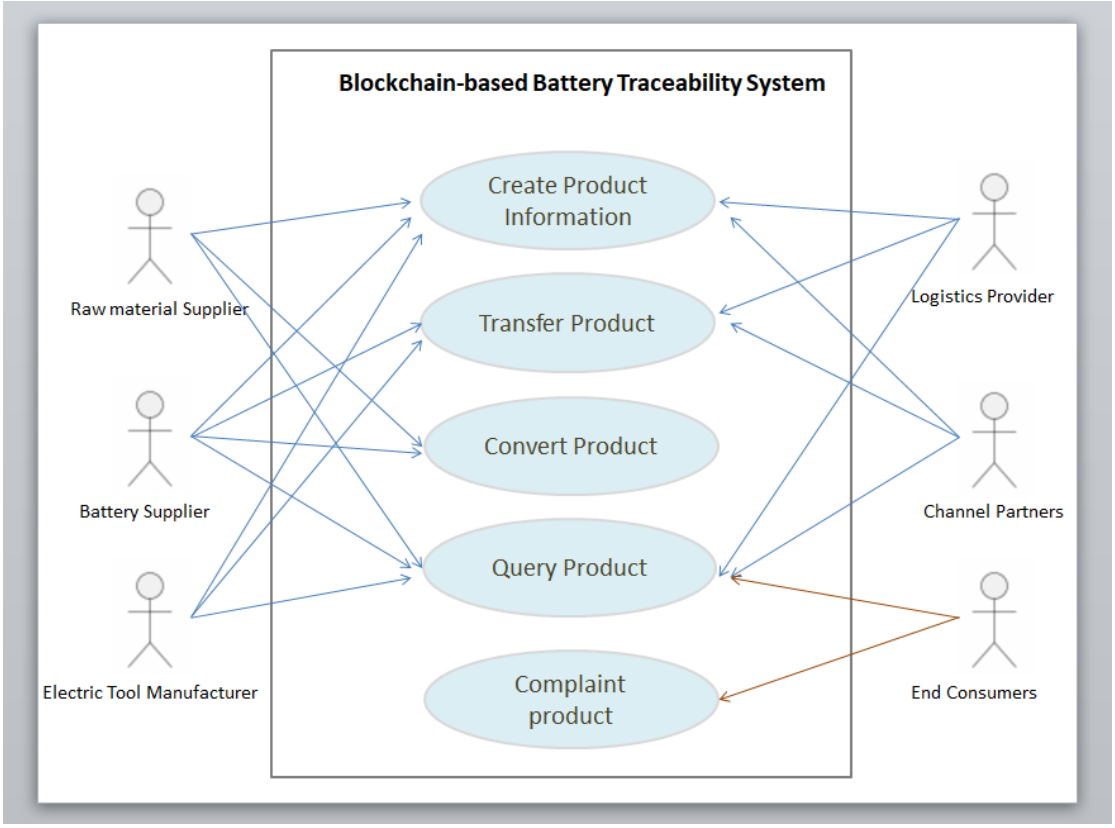




Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	- Generic blockchain platform	- Modular blockchain platform	- Specialized distributed ledger platform for financial industry
Governance	- Ethereum developers	- Linux Foundation	- R3
Mode of operation	- Permissionless, public or private	- Permissioned, private	- Permissioned, private
Consensus	- Mining based on proof-of-work (PoW) - Ledger level	- Broad understanding of consensus that allows multiple approaches - Transaction level	- Specific understanding of consensus (i.e., notary nodes) - Transaction level
Smart contracts	- Smart contract code (e.g., Solidity)	- Smart contract code (e.g., Go, Java)	- Smart contract code (e.g., Kotlin, Java) - Smart legal contract (legal prose)
Currency	- Ether - Token via smart contract	- None - Currency and token via chaincode	- None

Features	Database	Blockchain
Firewalls	Yes	No
Dual-key encryption	No	Yes
Consensus mechanism	No	Yes
Vulnerable to frauds	More	Less
Open organizations	No	Yes
Data duplication	Small	Great
Automatic rules	Triggers	Smart contracts

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc.



1 Overview

2- Blockchain as New Database Systems DDBMS, Distributed ledgers 4 - Bitcoin
8,9,11,23 – Blockchain definition header contents hash
14 – nonce, transaction process 15,16 – cryptography, symmetric, asymmetric
17 – P2P 18,19 – verify process, encryption, digital signature, fund transfers
20 – irreversible 24 – security 25 – ASIC, crypto puzzle 26,27 – PoW, PoS
28 – PoA, Permissioned 29 – types, consortium 联盟链
30,31 – public, private 32 – public VS consortium (permission)
34 – Hyperledger
36 – limitations 37 – smart contract consensus-based，mining39
其他用途 41，平台 42
Ethereum Blockchain 2.0 44 智能合约 45，46 传统 VS 智能 48
智能合约 use case 49 Ethereum，加密货币，智能合约 50
Ethereum v. Bitcoin Turing complete 51
Gartner's 2017 Hype Cycle for Blockchain 54 好处 55
Blockchain 3.0 56 business 57 industry 58 Hyperledger 59 Linux Foudation 60
Hyperledger Goals 61 Hyperledger Modular Umbrella Approach 62 data – 64
Members – 65 Blockchain 3.0: Healthcare 67 drug traceability 68
advantages 69
advantages 74

2 Blockchain Systems and Platforms

Top platform 对比 4
Ethereum Smart Contracting Cross-Industry Platform5
Hyperledger Fabric framework 6
R3 Corda OS finance 7 Ripple Global Payments 8
Quorum . Enterprise-focused Version of Etheruem9
Ethereum History 11 Ethereum Blockchain 12 Ethereum Smart Contracts 13

Ethereum Blockchain Processing 15 Ether 计量方法 wei 17
Users 18 value 19 Geth = Ethereum Client 20 Parity = Ethereum Client 21
Ethereum Javascript Library web3.js 22 Solidity language 23
Remix = Ethereum Web IDE 24 Truffle / Embark = dApps Frameworks 25
Metamask = Chrome Plugin 26 Swarm storage – 27 IPFS storgae 28
Whisper is a comm protocol for dApps diagram 29
Bitcoin VS Ethereum 30 31 33 Phased Ethereum Development 34 35
Ethereum Forkings 36 Quorum Overview 38 39 Quorum Network 40
Quorum Consensus Protocol 41 Quorum Privacy 42 43
Quorum is Enterprise-focused Version of Etheruem 44 45
Quorum: Permissioned Ethereum 46
Ripple Helps Banks Transact consensus 50 51
Cross Border Payments – Today 53
Cross-Border Payment Process 55 Payment using SWIFT 56
SWIFT 57 The HomeSend Payment Hub 58
Ripple Payment Network 59 Key Ripple Components 60
Cross Border Payments – Today 61 Ripple Benefits 62

3 Hyperledger Overview

What is Hyperledger? 4 6 Hyperledger Key Features 7
Hyperledger Greenhouse 10 Burrow smart contract machine, framework 11,12
Fabric 13 14
Indy distributed ledger purpose-built for decentralized identity 15 16
Iroha simple and easy to incorporate into infrastructure projects requiring distributed ledger technology C++ 17 18
Sawtooth utilizes a modular platform for building, deploying, and running distributed ledgers 19 Proof of Elapsed Time (PoET) 20
Hyperledger Grid supply chain focused solution n ecosystem of libraries, frameworks, and technologies 21 22
Relationships of Five Hyperledger Frameworks 23
Hyperledger Tool: Explorer visualizing blockchain operations 24
Cello Blockchain-as-a-Service (BaaS) 25
Composer a suite of tools for building blockchain business networks. 26
Quilt a business blockchain tool 27
Caliper blockchain benchmark tool 28
Hyperledger Fabric Architecture Glossary Chaincode Channel Hyperledger Fabric Certificate Authority 30
Ledger Endorsement Endorsement policy Peer 31
Commitment Software Development Kit (SDK) 32
Gossip Protocol State Database 33 What is Hyperledger Fabric? 34
Three Components of Fabric CA Peer Orderer 35
CA Workflow 36
Hyperledger Architecture 37
Participants in a Blockchain Network 38 39
Components of Blockchain 40 Integration with Existing Systems 41
Permissioned Ledger Access 42
Transaction and Identity Privacy 43
Hyperledger Fabric Deployment Model 44
Hyperledger Fabric Models – Assets/Chaincode 45
Hyperledger Fabric Models – Ledger 46 47 48
Hyperledger Fabric Ledger Data Architecture levelDB CouchDB 49 50
Hyperledger Fabric Ledger Data Architecture Data steps 51
Fabric Channels channel separate 52
Gossip Protocol 53

4 Basic Blockchain Mechanisms

5 Evolution of Blockchain Technology

6 Blockchain Use Cases

Key Characteristics of Blockchain 5
Blockchain Assessment Framework 6
Assessment of Generic Blockchain Impact 7
How Does Hyperledger Fabric Work 9
Different layers 11
Vendor Financing 14 Traditional Vendor Financing Workflow 15
Vendor Financing Pain Points 16 17
Blockchain vendor financing workflow 20
Advantages of blockchain vendor financing: 21 22
Customer loyalty program: 24
Traditional customer loyalty program workflow 25
Customer loyalty program pain point 27 interoperability 互通性
Advantages of Blockchain customer loyalty program: 28
Other use cases in financial service 29
Challenges 30,31 Implementation considerations 32 Implementation Roadmap 33
Supply chain + block chain 35
Pharmaceutical Supply Chain Challenges 36
Purchasing Platform Challenge 38
Getting Started with Blockchain in Supply Chain Concerns 40
Blockchain implementation decision tree 41
Traditional healthcare ecosystem 43
Healthcare pain points and blockchain opportunities 44

7 Smart Contract Techniques

Fives Types of Financial Services 4

• A smart contract defines the rules between different organizations in executable code that can be invoked to generate transactions that are recorded on the ledger.

还没讲

Every smart contract needs an endorsement policy that identifies which organizations must approve transactions generated by the smart contract before those transactions can be identified as valid