HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

分布式账本技术概论

杨保华

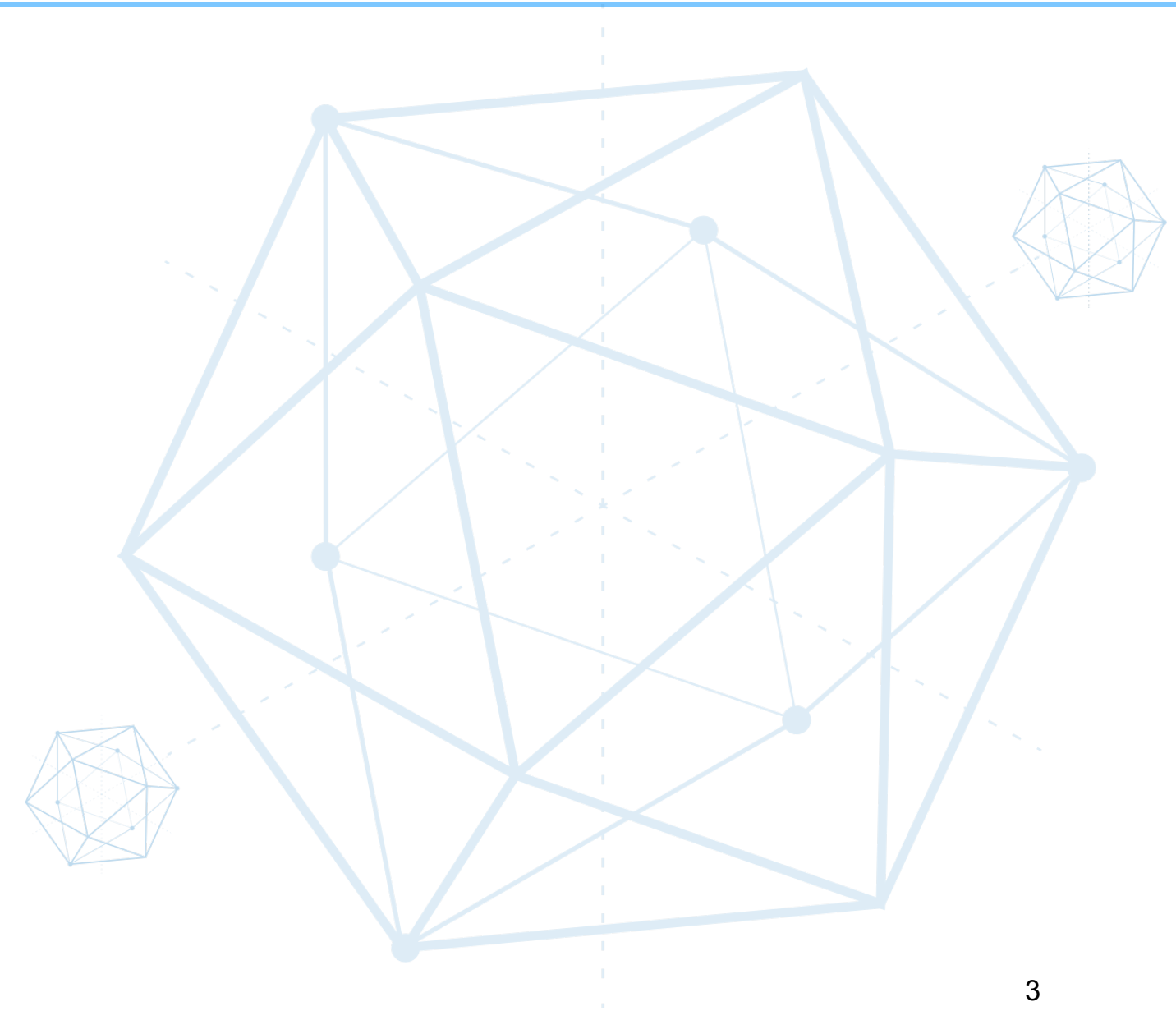
2017年11月30日，清华大学

About Me

- **Interested Areas**
  - Fintech, Cloud and Analytics
- **Technical Leader**
  - Senior Researcher/Architect in IBM, Oracle
- **Open-Source Contributor**
  - Hyperledger, OpenStack, OpenDaylight, etc.
- **Hyperledger Developer**
  - Core designer & committer of Fabric, Cello, sdk etc.
  - Hyperledger Technical Steering Committee (TSC) Member
  - Hyperledger Technical Working Group China Chair

Outline

- Concepts
- History
- Scenarios
- Challenges
- Q&A

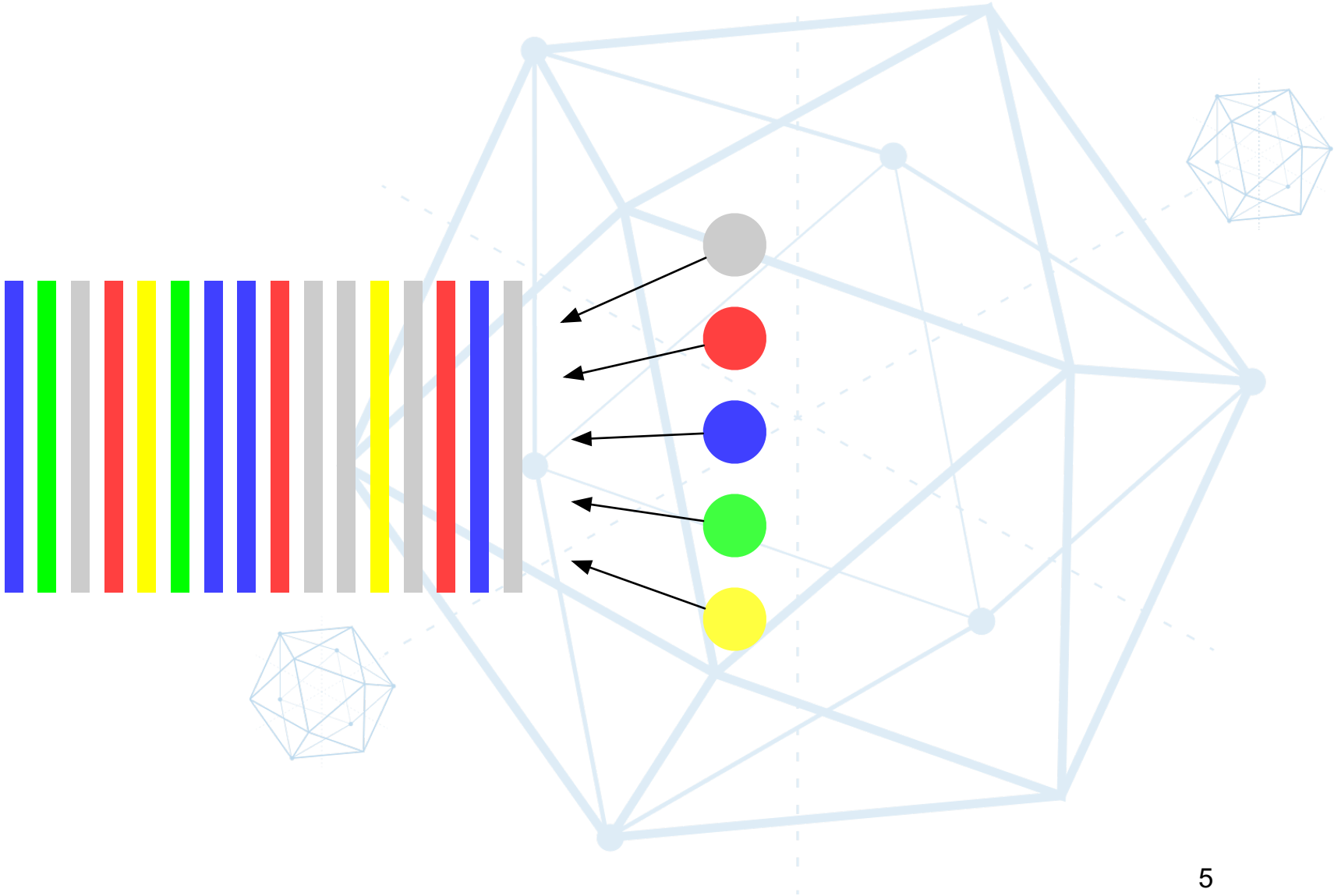


Concepts

- Transaction
  - Agreement, communication, or movement carried out between a buyer and a seller to exchange an asset for payment.
  - Information processing tasks that is divided into individual, indivisible operations.
- Ledger
  - Record transaction history and the result.
- Distributed Ledger
  - Ledger with multiple participants, distributed in deployment and management, and support smart contract to operate the states.
- Blockchain
  - A verifiable data structure that provides immutable transaction history.

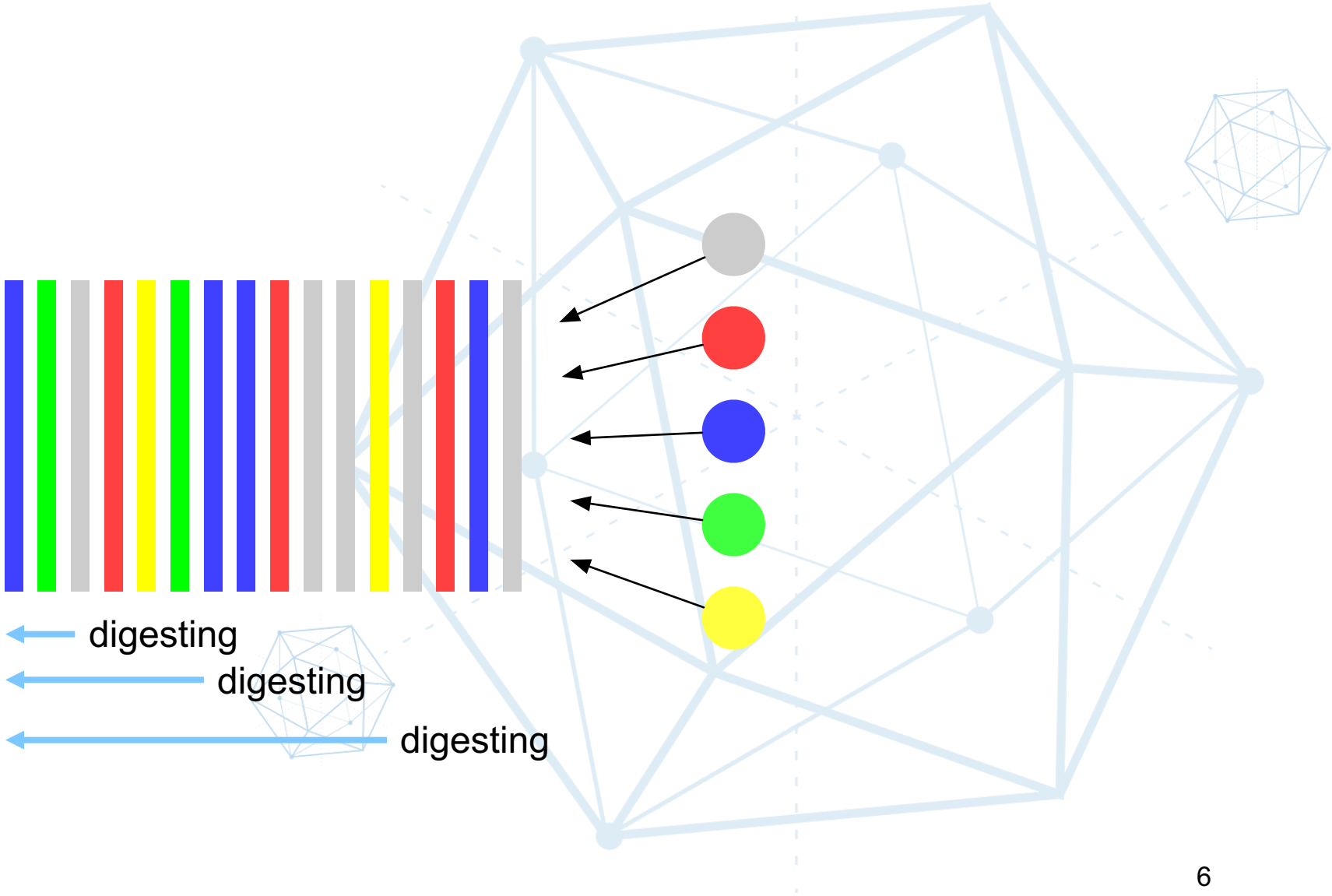
How to Record Transaction with Credit?

- Option 1



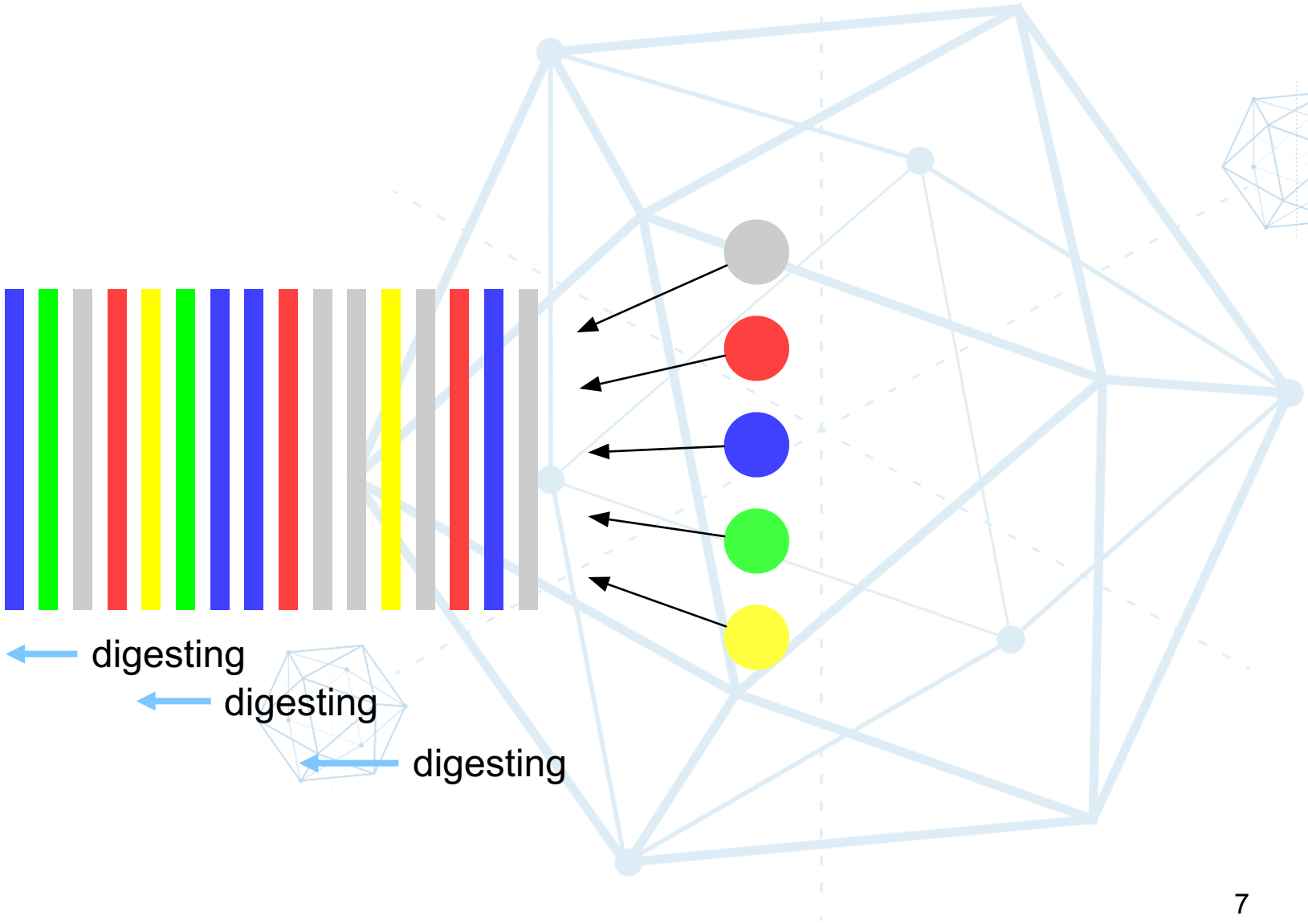
How to Record Transaction with Credit?

- Option 2

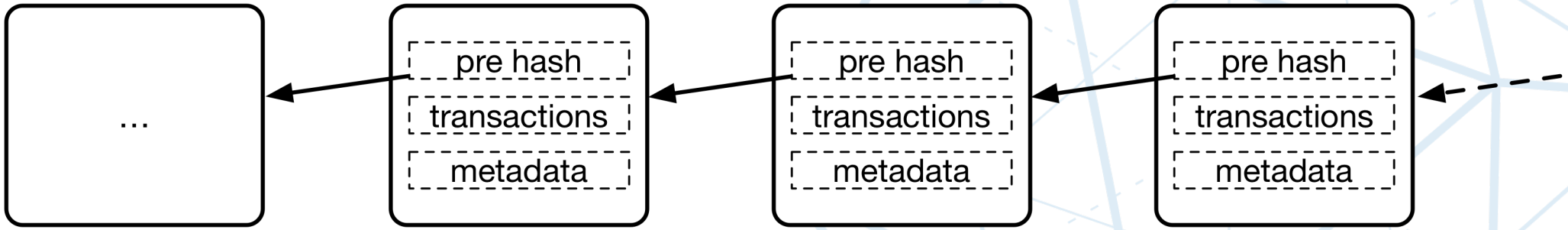


How to Record Transaction with Credit?

- Option 3

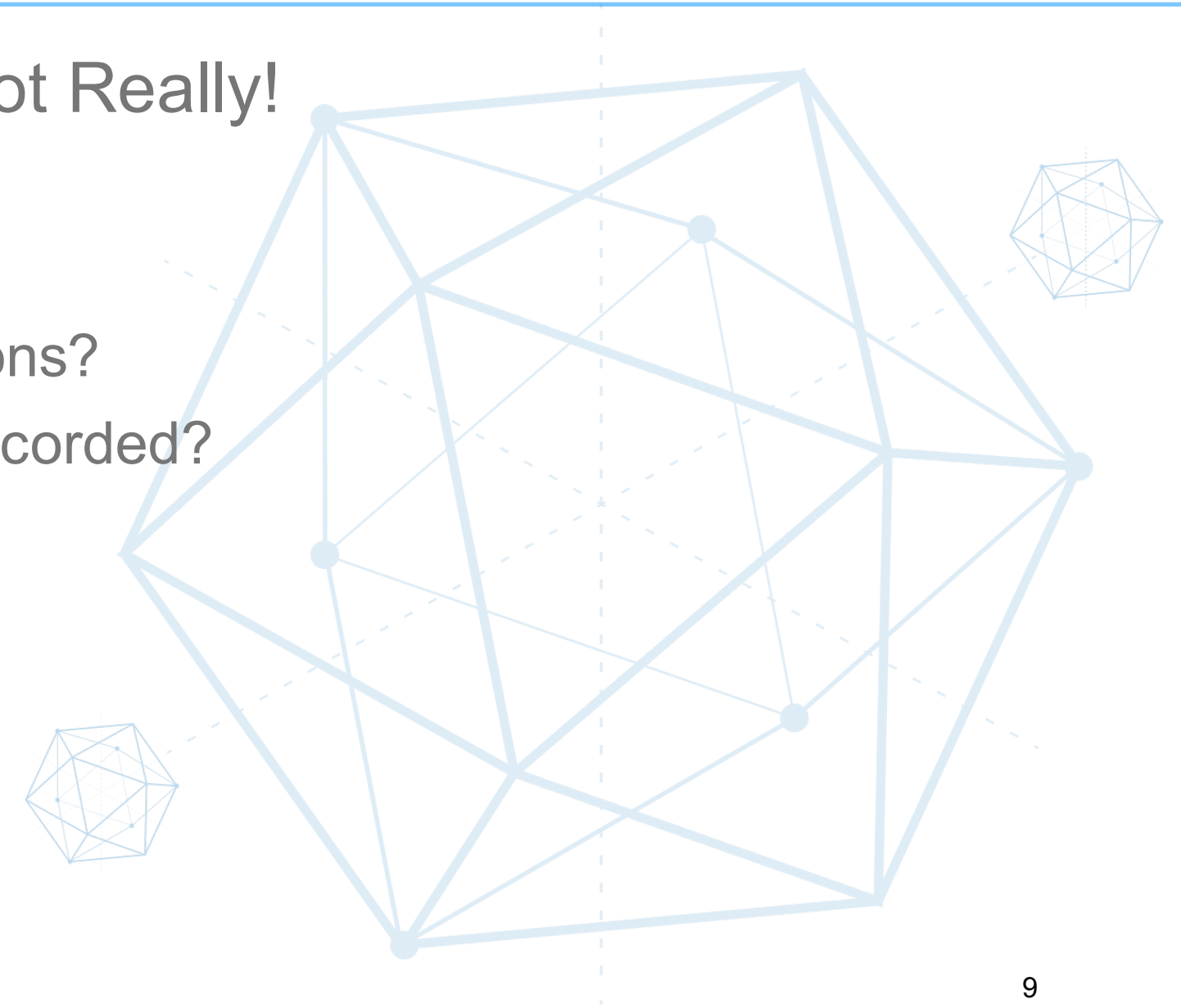


How to Record Transaction with Credit?



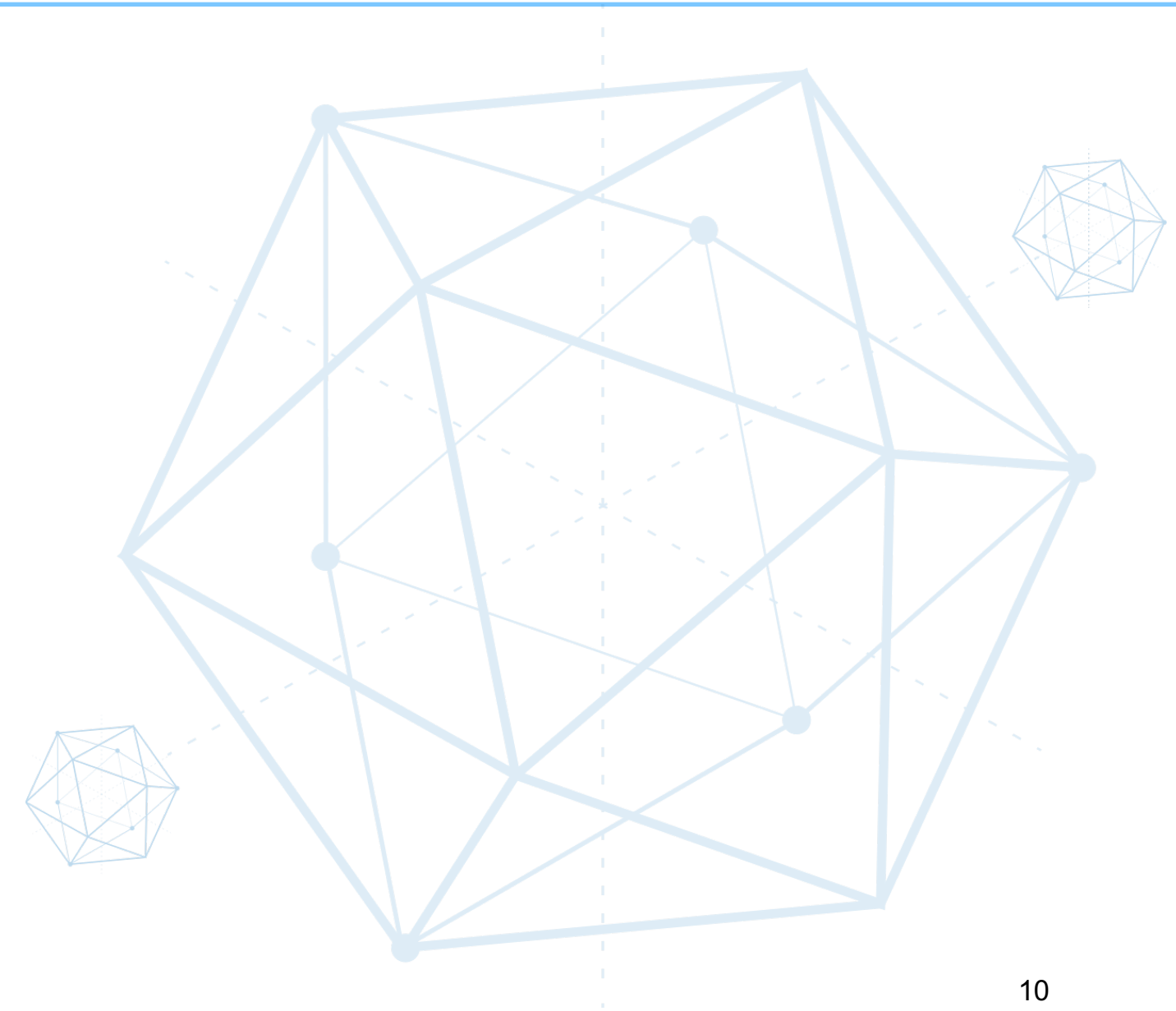
From Blockchain to Ledger Technology

- Is Blockchain Enough? Not Really!
  - Who maintains the records?
  - Who can use the service?
  - Who executes the transactions?
  - Who decides what can be recorded?
  - …

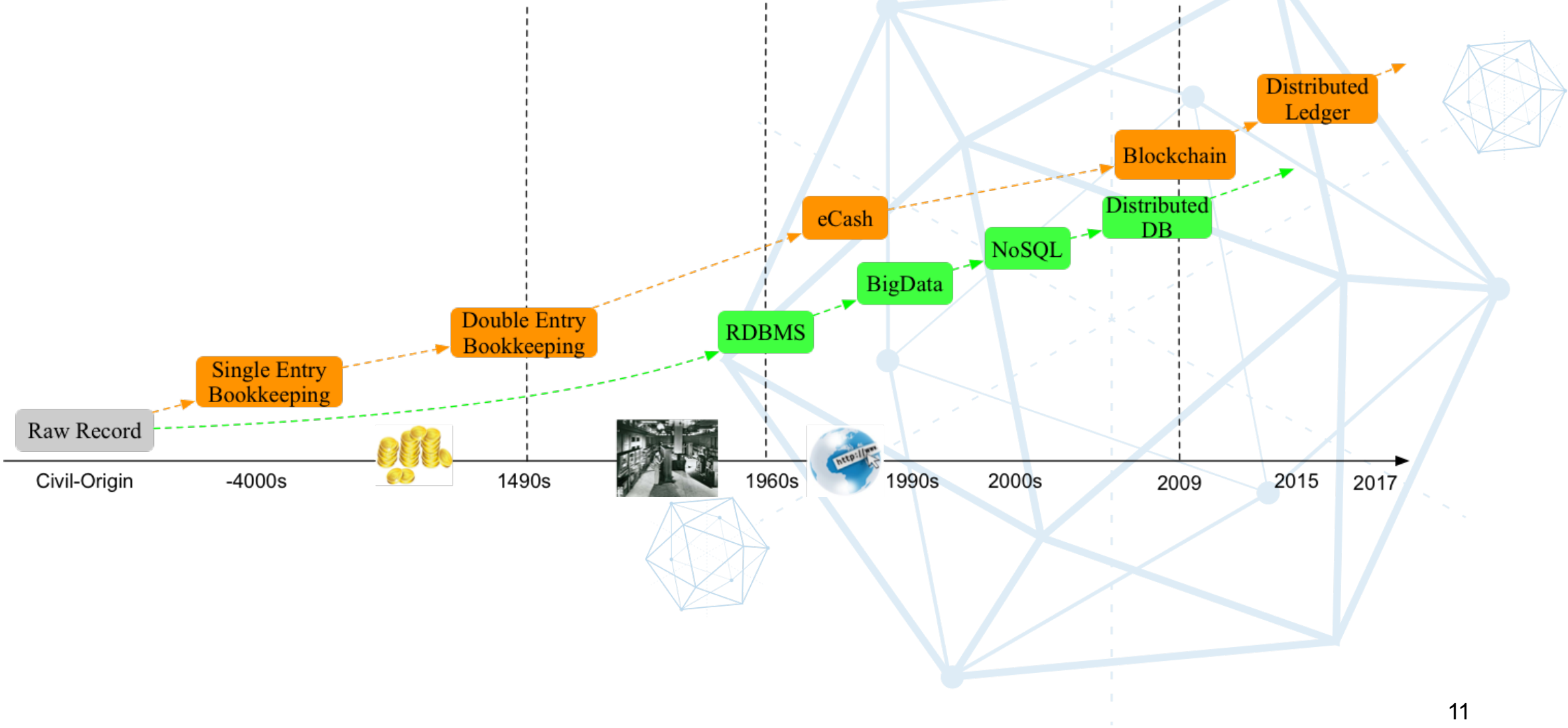


Outline

- Concepts
- **History**
- Scenarios
- Challenges
- Q&A

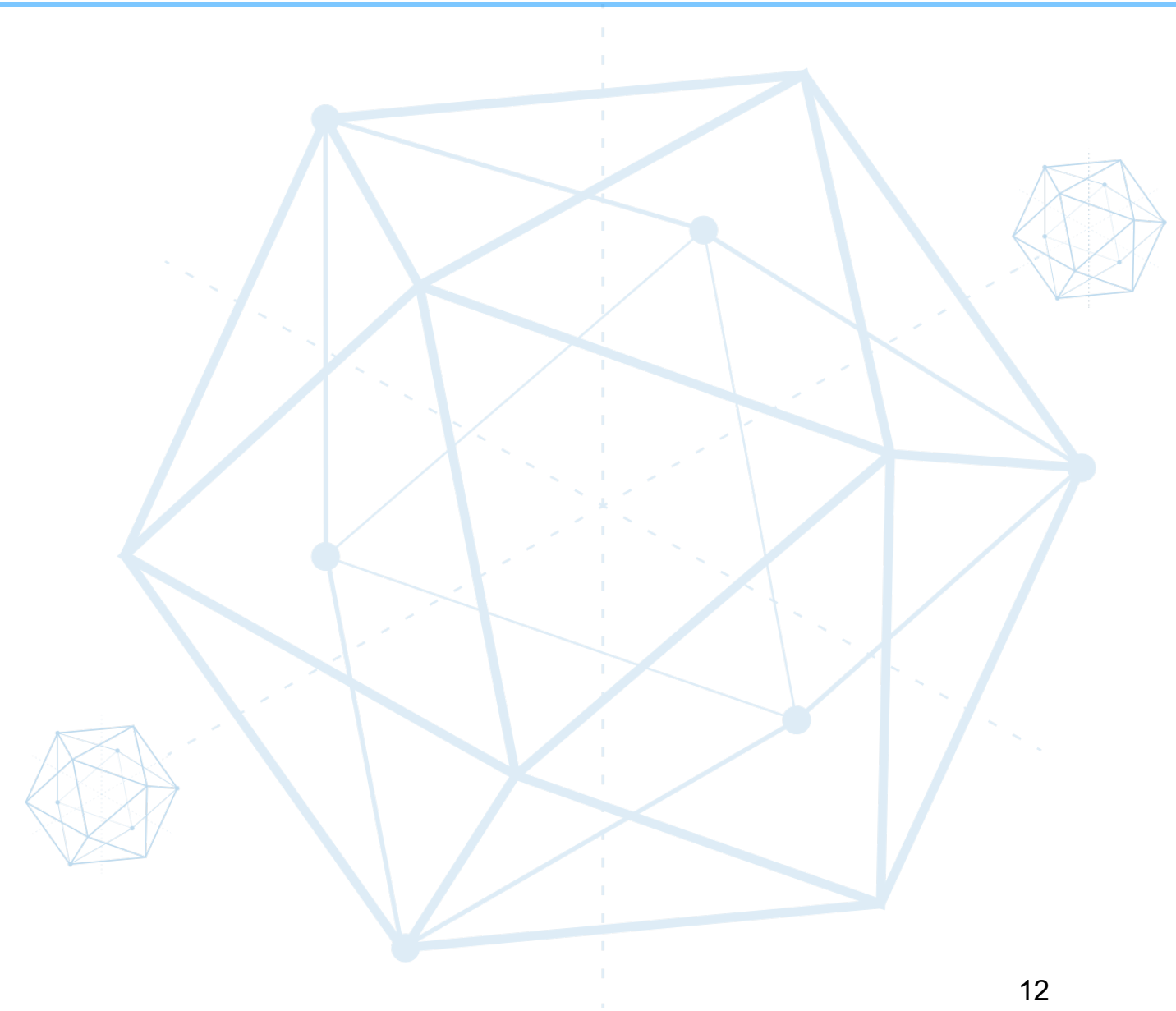


Ledger Technology's History



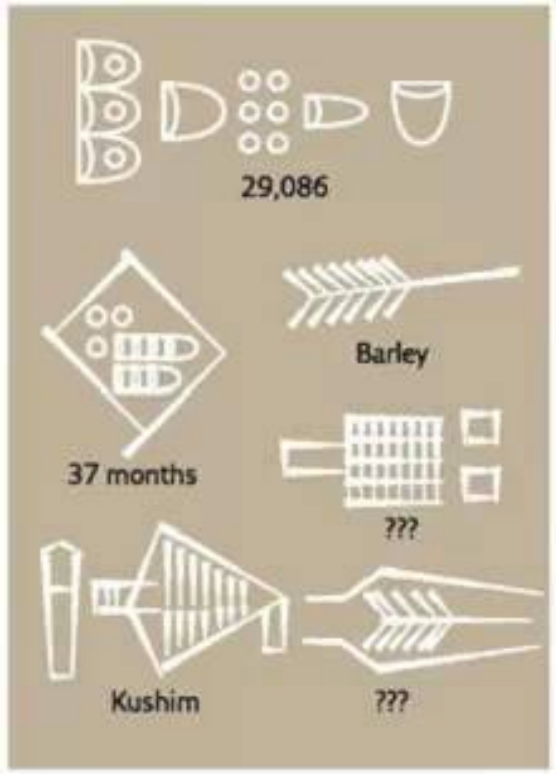
Four Phases in History

- Phase 1: -3000s ~ 1490s
  - Primitive Ledger: 4500y
- Phase 2: 1490s ~ 1960s
  - Modern Ledger: 470y
- Phase 3: 1960s ~ 2009
  - Electronic Ledger: 40y
- Phase 4: 2009 ~?
  - Blockchain: 5y
  - Distributed Ledger: ?



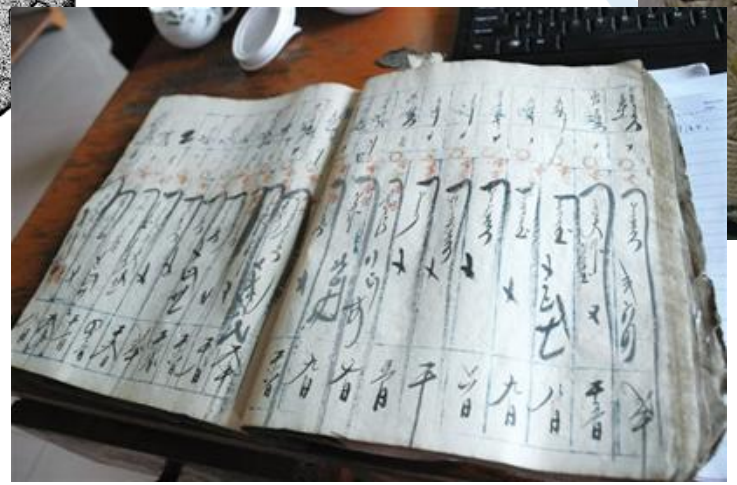
Phase1: Primitive Ledger

- -3000s: Bruk's Kushim Board



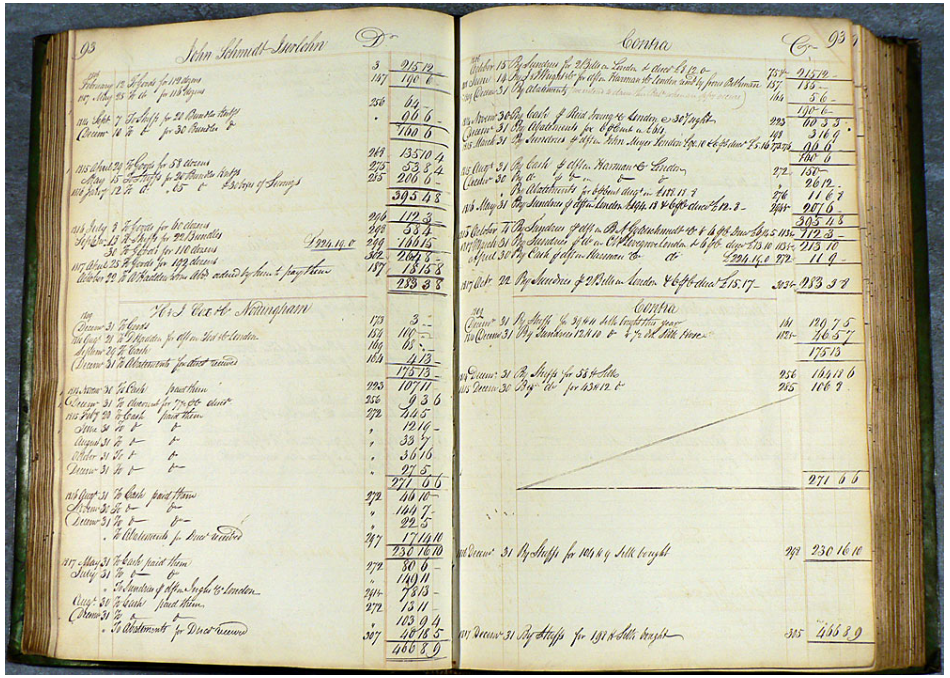
Phase1: Primitive Ledger

- All ancient civilizations have ledgers



Phase 2: Modern Ledger

- 1494: Luca Pacioli, Italy



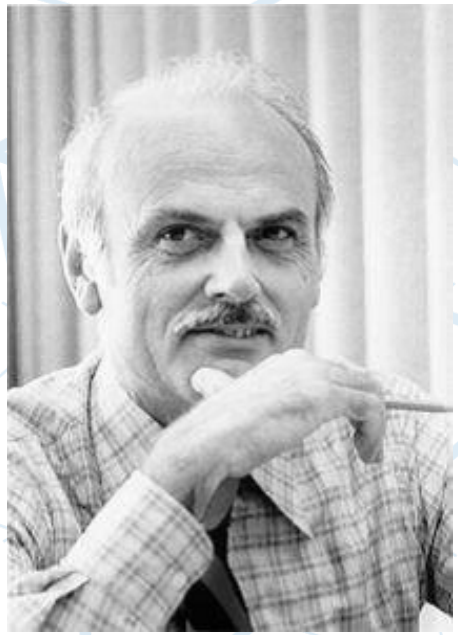
账户 | 科目 | 发生业务 | **账户卡**

	日期	文件	摘要	收入 RMB	支出 RMB	账户	科目	余额 RMB
1			**1001 库存现金**					
2			期初余额					970.00
3	1/1/2010	1	商品A销售	8,000.00		1001	6001	8,970.00
4	1/1/2010	2	购买原材料		1,500.00	1001	5001	7,470.00
5	1/2/2010	4	存款利息	2,000.00		1001	6011	9,470.00
6	1/3/2010	5	银行存款-工行		1,000.00	100201	1001	8,470.00
7	1/10/2010	6	材料费		600.00	1001	5101	7,870.00
8	1/12/2010	7	商品B销售	400.00		1001	6001	8,270.00
9	1/12/2010	8	车间管理人员工资		10.00	1001	5101	8,260.00
10	1/14/2010	9	商品C销售	200.00		1001	6001	8,460.00
11	1/14/2010	10	购买配料		90.00	1001	5001	8,370.00
12			**发生额汇总**	**10,600.00**	**3,200.00**			**8,370.00**
13								
14			**100201 工商银行**					
15			期初余额					15,200.00
16	1/3/2010	5	银行存款-工行	1,000.00		100201	1001	16,200.00
17	1/15/2010	11	银行存款支出		1,000.00	100201	[*]	15,200.00
18	1/16/2010	12	银行存款-工行	2,000.00		100201	[*]	17,200.00
19			**发生额汇总**	**3,000.00**	**1,000.00**			**17,200.00**
20								
21			**100202 建设银行**					
22			期初余额					6,500.00

基本 | 成本中心 | 到期日

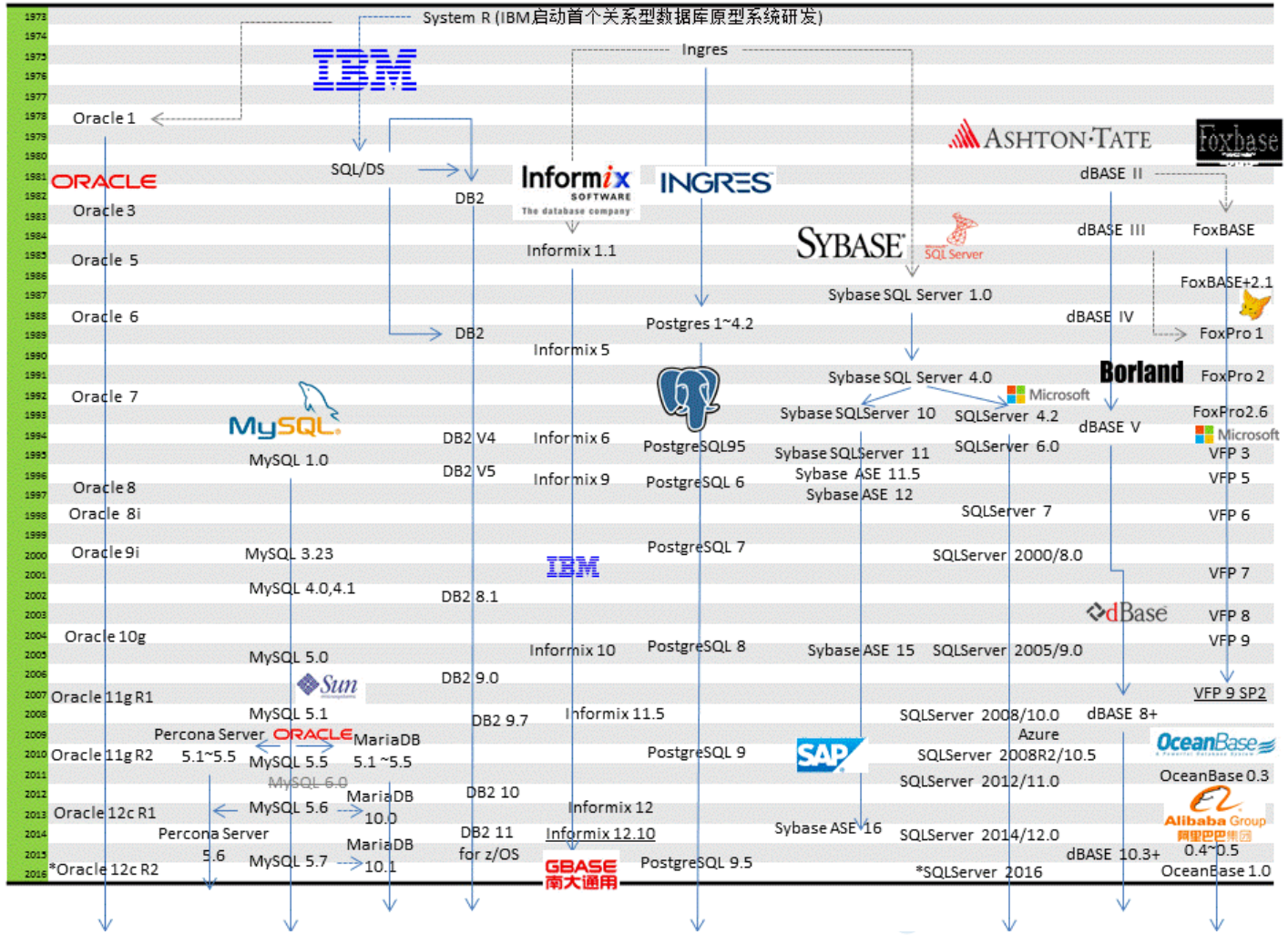
Phase 3: Electronic Ledger

- 1970: ” A Relational Model of Data for Large Shared Data Banks”, Edgar Frank Codd, IBM
- 1978：Oracle
- 1980s: Internet
- 1983: eCash
- 1990s: BigData
- 2000s: NoSQL
- 2004: keepaccounts.com (Gooot.com)



Phase 3: Electronic Ledger

国际主流通用关系型数据库家谱图



Phase 4: Blockchain to Distributed Ledger

- 2009.1: Bitcoin
- 2015.7: Ethereum
- 2016.2: Hyperledger

Bitcoin P2P e-cash paper *2008-11-01 19:16:33 UTC*

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Ethereum Launches

Posted by Stephan Tual on July 30th, 2015.

A few minutes ago, many of you generated and loaded the Ethereum Genesis block, marking the inception of Frontier, the first Live release of the Ethereum project.

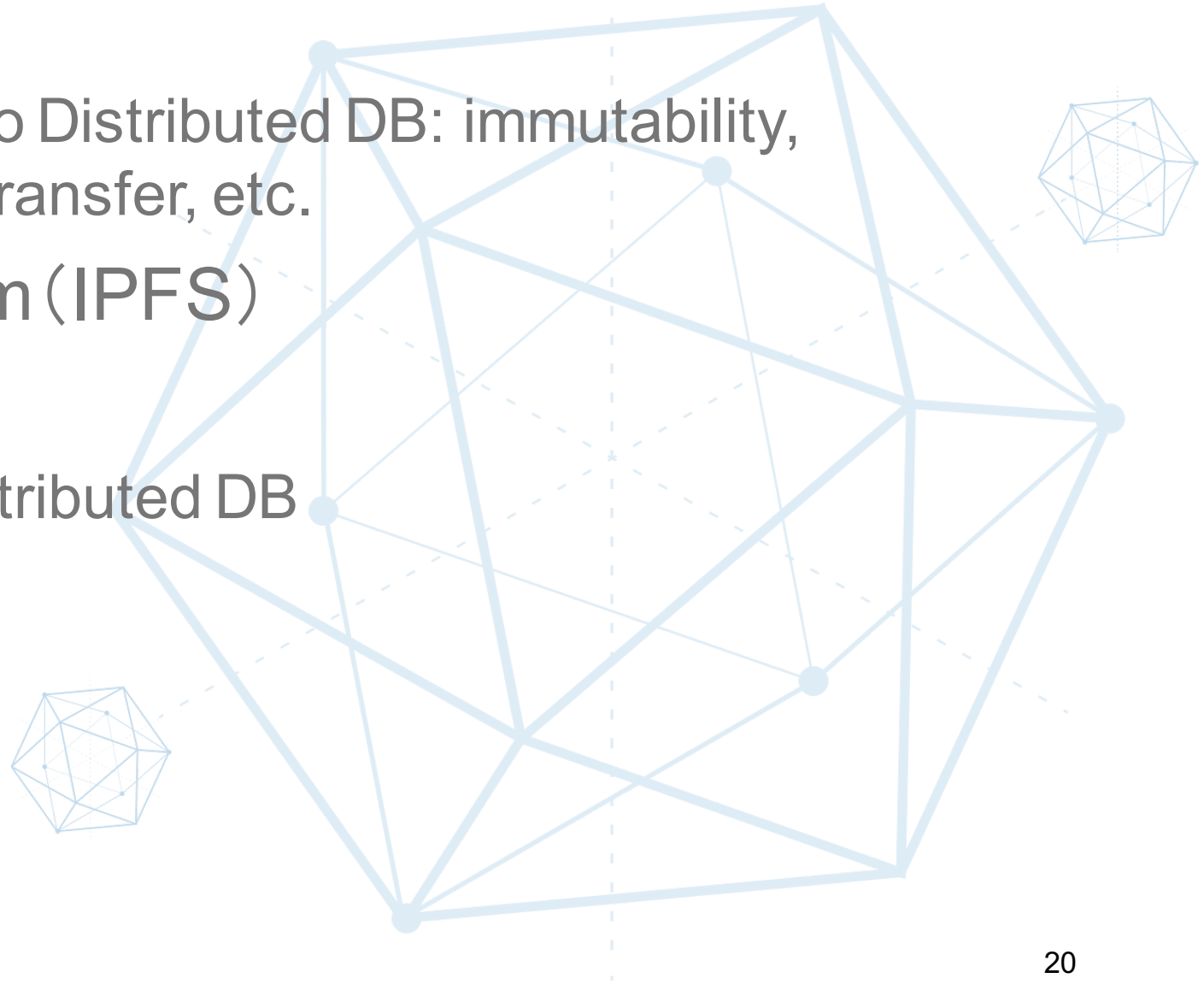
SAN FRANCISCO, Calif., Feb. 9, 2016 – The Linux Foundation, the nonprofit organization enabling mass innovation through open source, today is announcing new members from across the industry, a formal open governance structure and technical updates to the new Hyperledger Project.

Phase 4: Blockchain to Distributed Ledger

- Bitcoin
  - Focus on payment
  - Limit in simple smart contracts, performance…
- Ethereum
  - Improve performance
  - More smart contracts
- Hyperledger
  - Enterprise grade ledgers (IBM, Oracle, Intel, Cisco, DTCC, R3, NEC, JP Morgan, DAH, Accenture, SAP, Wanda, Huawei, CMB…)
  - Permission, more consensus, pluggable…
  - Smart contracts in Go, Java, and more

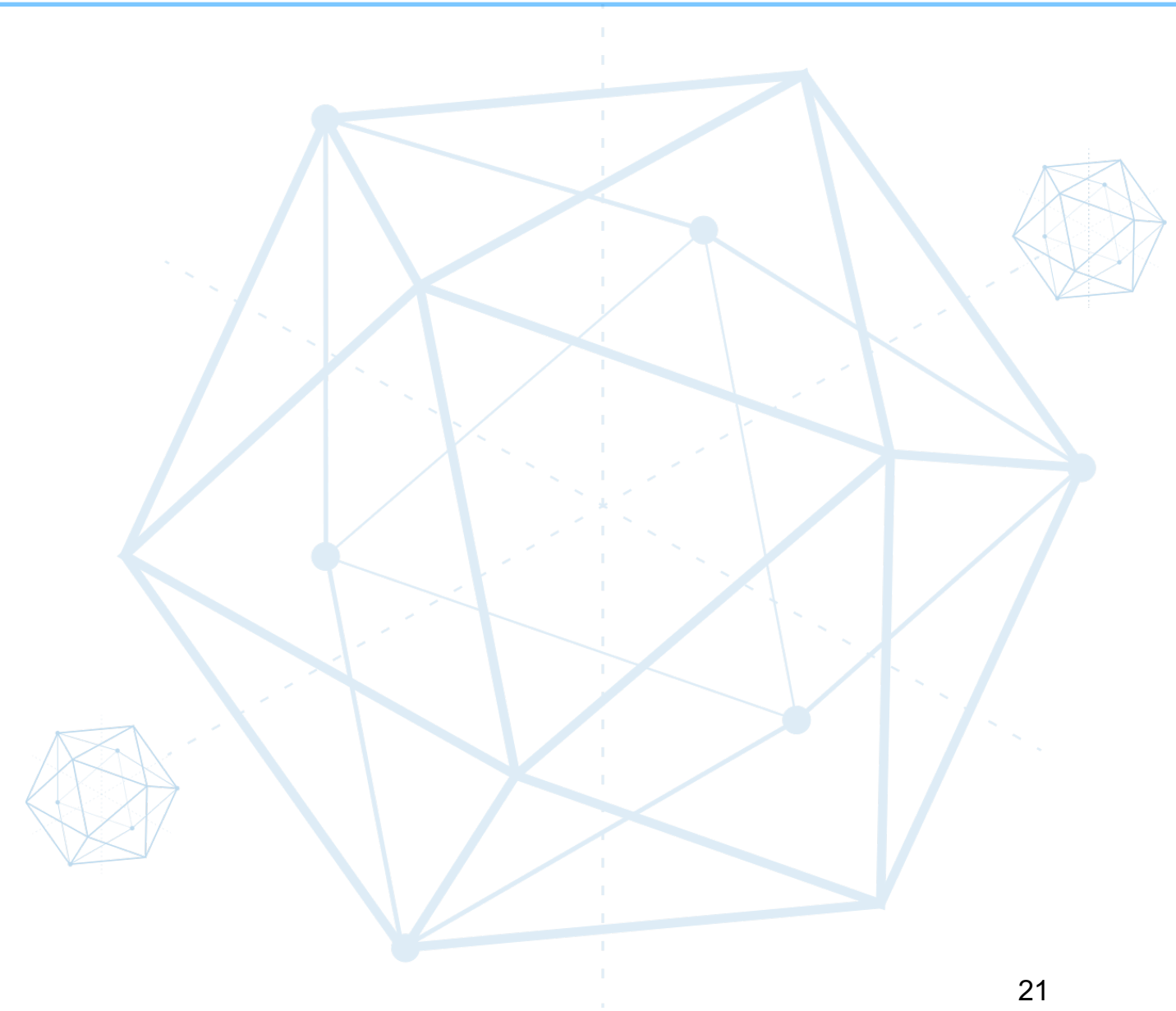
Other Related Projects

- BigChainDB
  - Bring Blockchain features into Distributed DB: immutability, decentralized control, asset transfer, etc.
- Inter Planetary File System（IPFS）
- Corda
  - Financial industry service distributed DB



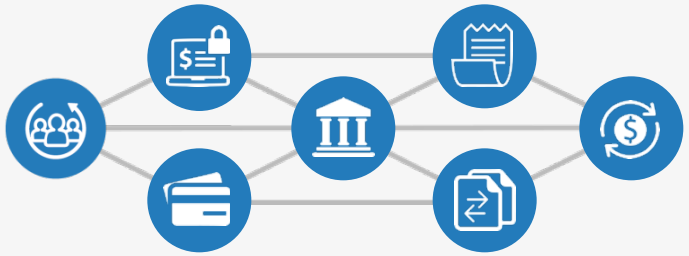
Outline

- Concepts
- History
- **Scenarios**
- Challenges
- Q&A



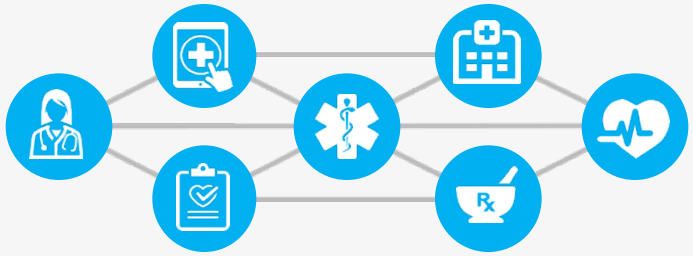
Shared Ledger Database

Blockchain allows multiple different parties to securely interact with the same universal source of truth



Finance

Streamlined settlement, improved liquidity, increased transparency and new products/markets



Healthcare

Unite disparate processes, increase data flow and liquidity, reduce costs and improve patient experience and outcomes

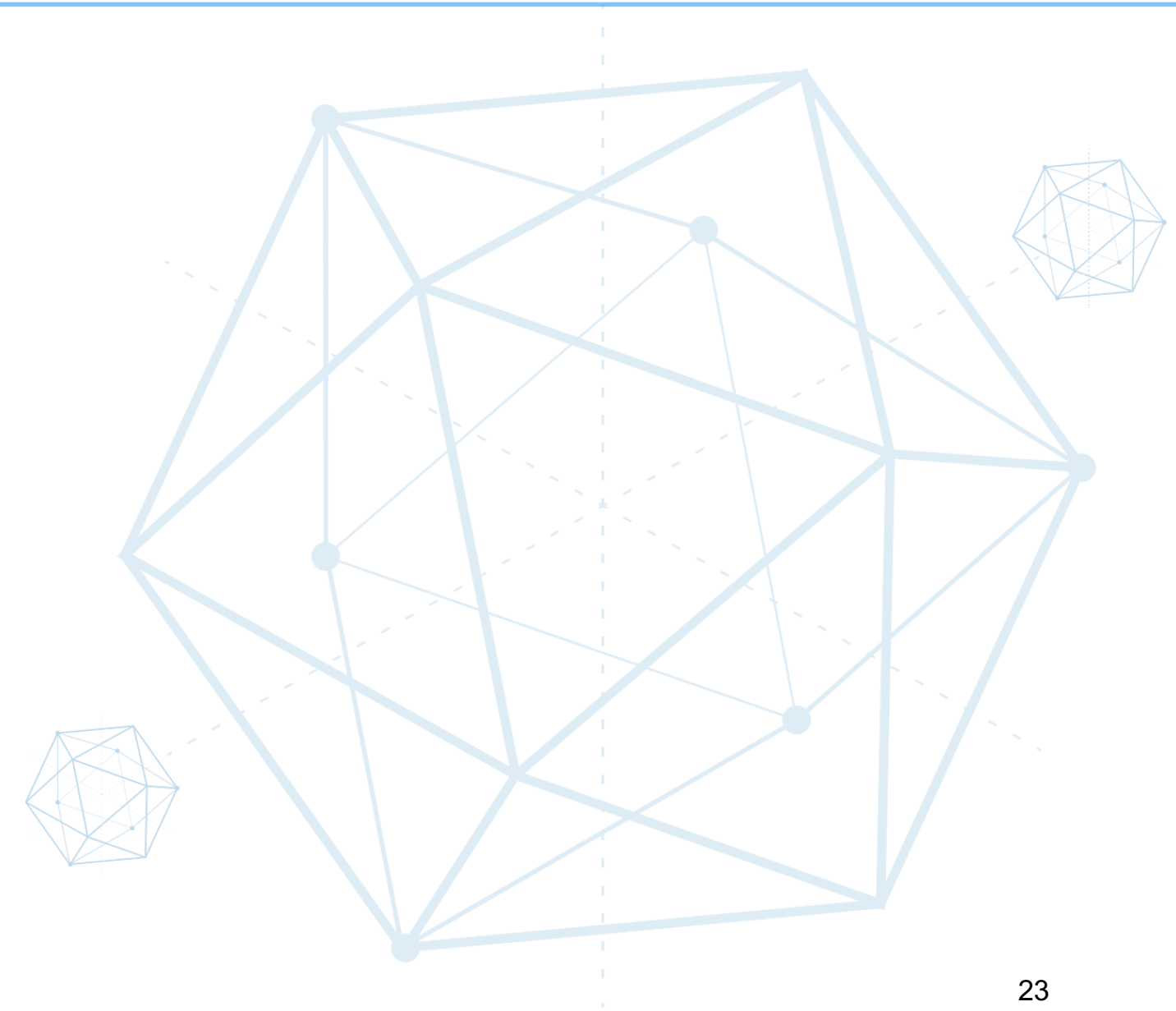
Supply Chain

Track parts and service provenance, ensure authenticity of goods, block counterfeits, reduce conflicts

Potential Scenarios Requirements

- Multiple Parties
- No Trust Base
- Smart Contract

- High Frequency?
- Very low latency?



Financial Service Industry

- Digital Currency
  - Europe, UK
  - Canada
  - Japan
  - China
- Payment
  - Bitwage, Circle, etc.
- Stock Exchange
  - Nasdaq Linq
- CrowdFunding

Cross-Border Payments

Transferring money across international borders is still complicated, time consuming and expensive. Payments routed abroad can take several days to get settled. Existing money transfer systems suffer furthermore from long lines, exchange rate losses, counter-party risks, bureaucracy and extensive paperwork. Cross-border payments have become a critical part of millions of lives as we moved towards a more globalized world and multicultural societies.

After months of work, a global team of developers have completed a cross-border POC built with Hyperledger Fabric. Designed to test whether moving member bank accounts to a distributed ledger could help the inter-bank payments platform Swift reconcile in real time, the blockchain trial is now ready for its next phase of testing with General members ANZ, BNP Paribas, BNY Mellon and Wells Fargo.

Hyperledger Fabric enables real-time visibility on the liquidity of Nostro accounts, easing reconciliation and allowing liquidity savings while meeting key industry requirements such as governance, data privacy, standardisation, and identity.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

SWIFT ANZ WELLS FARGO

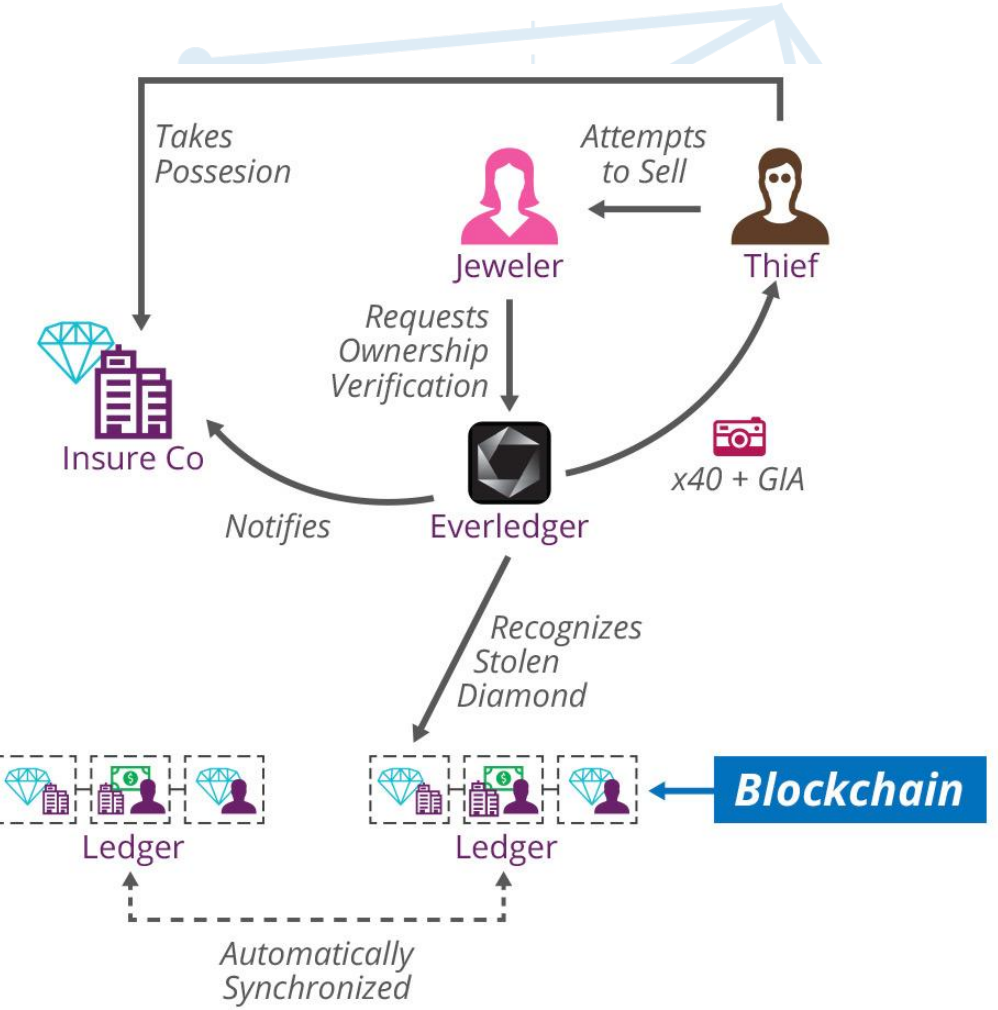
BNY MELLON BNP PARIBAS

Read about the POC in Coindesk.

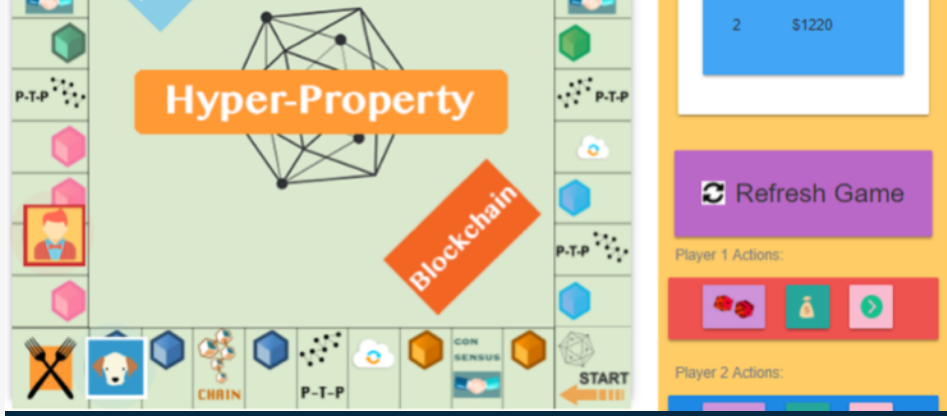
Hear about the collaboration in the ANZ Community Spotlight video.

Digital Asset Management

- Factom
- Everledger
- Food Safety
- Healthcare Records
- MIT Education Certificate



Real Estate Transactions



In the 1990s and 2000s, many international organizations put pressure on emerging countries to digitize land titles to guarantee citizens' legal rights to their properties. In some cases of corruption, the move to government-owned centralized databases backfired, and digital histories of land titles were eradicated, properties seized and handed over to oil companies.

Decentralizing databases and turning to distributed ledger technologies to keep track of land titles could keep governments accountable and create a more trustworthy system, even in instances where the individual actors may not be trusted.

Every transaction such as when a property is sold from one party to another or when a loan is taken out against a property, would be recorded on the public ledger. Financial firms would reference the distributed ledger to decide whether or not to extend the loan to someone looking to buy a property. This permissioned-based, shared system of record will increase trust overall and protect homeowners.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

The winning team at the Consensus 2017: Building Blocks Hackathon, built an online property banking and acquisition game utilizing Hyperledger Fabric with IBM Bluemix.

***HyperProperty* shows that Hyperledger Fabric can be used to guarantee who owns what properties. Lessons from *HyperProperty* can be applied to any tokenized economy where assets are represented by tokens on a blockchain. When assets need to be traded, trade participants can exchange value for the token and make transactions without a middleman. This has the potential to facilitate more efficient and less costly real estate transactions.**

Play HyperProperty.

Healthcare Records

Blockchain may offer a way to get the healthcare industry to commit to an information sharing platform in which pointers to personal health data could be stored on a secure, permissioned chain and shared back and forth quickly like email.

Hyperledger Composer offers a set of APIs, a modeling language and a programming model to quickly define and deploy business networks and applications that allow participants to send transactions that exchange assets.

Say, for example, a patient's x-ray sits on a cloud site and insurers can request the password to access it. Password requests get stored on a chain, and a set of smart contracts allow the doctor to share the pointers to the x-ray with the insurance company. The patient has a wallet noting which chains their records are stored on. When those pointers are shared, they're recorded as auditable events in the healthcare system, allowing patients to have complete visibility into their data and ultimately the ability to mediate and approve who their records are shared with.

Join the Hyperledger Healthcare Working Group (HLHC) to help bring commercial blockchain adoption to the healthcare industry.

CHANGE HEALTHCARE

Gem

HASHED HEALTH

HEALTHCARE BLOCKCHAIN INNOVATION

KAISER PERMANENTE®

patientory

Together we can create a blockchain system that disenfranchises the most vulnerable.

Lean more here.

Interstate Medical Licensing

Associate Hyperledger Member State of Illinois has implemented a pilot program in collaboration with General member Hashed Health using Hyperledger Fabric to reduce complexity of interstate medical licensing, as well as to improve the veracity of provider directories and claims adjudication processes.

The Hyperledger Fabric pilot program will identify opportunities to improve the efficiency and accuracy of the medical credentialing process in the state of Illinois. The concept will utilize a blockchain-based registry to streamline the sharing of smart contracts and medical credential data to automate workflow associated with interstate and multistate licensure.

In the short-term they anticipate this pilot will show how distributed ledger technology can help reduce the complexity of interstate licensing processes in Illinois. In the long-term, they see this as a secure, privacy-enhancing way in which state licensure boards can efficiently manage credentialing at national scale, while also presenting health payers and provider networks a 'single source-of-truth' to improve the veracity of provider directories and claims adjudication processes.

HASHED HEALTH

HEALTHCARE BLOCKCHAIN INNOVATION

The Illinois BLOCKCHAIN Initiative

Read the full announcement.

Music and Media Rights

Dot Blockchain Media (dotBC) is building a music content rights registry that will help musicians express their rights and wishes for commercializing their art in an interoperable file format. Data is maintained across a distributed network that utilizes Hyperledger Sawtooth.

dotBC's blockchain implementation is a foundation for music and media rights expression into the works themselves. It creates a fair and transparent method for music composers, artists, publishers and rights holders to express their rights and wishes for commercializing their art into a modern and interoperable file format. dotBC maintains partnerships and connections in the music and wider media industries to enable seamless data exchanges between more than 63 million globally recorded works from independent and major label artists and the dotBC ecosystem.

"Hyperledger Sawtooth will enable us to scale rapidly and customize transaction processors specifically for ingesting rights data. We look forward to delivering a strong and lasting solution, anchored on a sophisticated and secure blockchain foundation, for the music and media industries with Intel."

– Benji Rogers, dotBC CEO

dot blockchain media

Although not a member of Hyperledger, dotBC is able to leverage the open source Hyperledger Sawtooth platform for recording its content rights registry for the media industries.

Read the full story in *Crypto Ninjas*.

Trade&Supply-chains

- International Trading
  - Different Currency
  - Lack of Trust
  - Time Cost
- Supply Chain
  - Many Participants
  - Complicated Process
  - Lots of Documentation/Proof

Diamond Supply Chain

In 2003, the Kimberley Process Certification Scheme (KPCS) was established to prevent conflict diamonds. Purchased diamonds now come with a certificate to prove the distributor did not obtain the diamond from rebels, that the mine has been audited, etc. The idea is that paperwork can confirm provenance; however, the process is lengthy and there is a history of fraud from missing paperwork.

To keep blood diamonds from entering the supply chain Hyperledger Premier member SAP Ariba is collaborating with Everledger to pilot a distributed ledger diamond track and trace system using Hyperledger Fabric v1.0 that everyone in the industry can write to from miners, to distributors, to retailers.

Holding a diamond to light creates a unique pattern that may be used to create an ID. When a bag of diamonds changes hands in the supply chain, it forms two entries in the chain: the diamond IDs present upon sending and receipt. Once a diamond ID number is inside the system it provides integrity as any stakeholder can then query and instantaneously verify a diamond's provenance.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

SAP everledger

This system is empowering whistleblowers, governments, mining companies, retailers, journalists, and human rights organizations to get specific on tracking where conflict diamonds are entering the supply chain and preventing them from entering the market.

Read about the Hyperledger Fabric pilot in *International Business Times.*

Green Assets Management

General Hyperledger member Energy Blockchain Labs partnered with Premier member IBM on the world's first blockchain-based green assets management platform based on Hyperledger Fabric. In production use by the carbon asset market in China, it allows enterprises to generate carbon assets more efficiently, helping to build a green, low-carbon and environmentally-friendly future in China.

Blockchain technology is expected to become an important means for effective control of carbon emissions, which is of great significance to China, the world's largest source of carbon emissions. Carbon asset development, also known as CER (Carbon Emission Reduction) quota issuing, is one of the most popular ways of encouraging enterprises to decrease emissions and use low carbon emission technology.

The platform is estimated to significantly shorten the carbon assets development cycle and reduce the cost of carbon assets development by 20-30 percent just in the pilot stage of the platform, enabling cost-effective development of a large number of carbon assets.

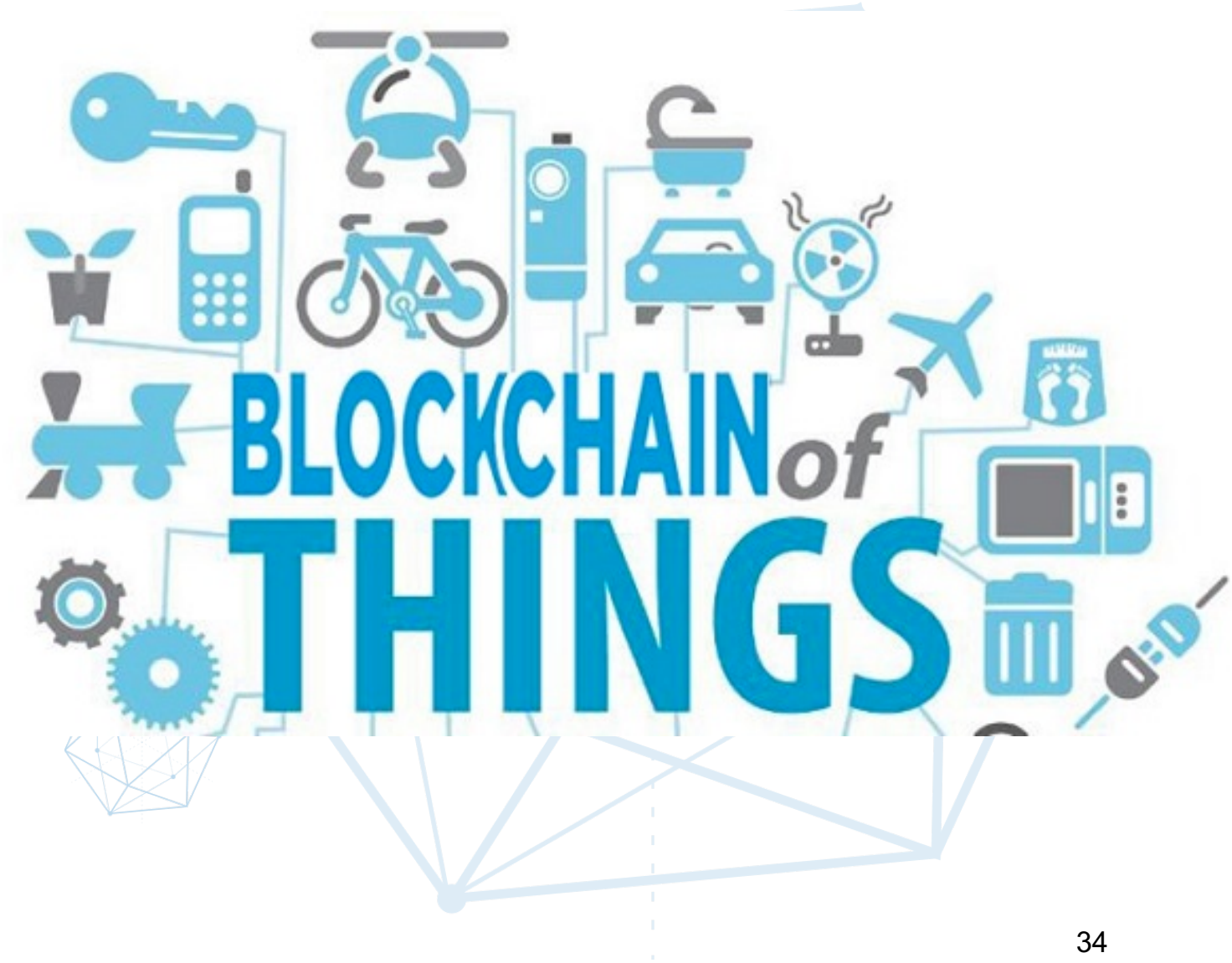
ENERGY BLOCKCHAIN LABS

IBM

Learn more about Energy Blockchain Labs in their Hyperledger Community Spotlight video.

Internet of Things, AI?

- Imagine, billions of smart devices connect to each other automatically.



Ethical Seafood Movement

Blockchain technologies are being used in the fishing industry to drive fish catch towards more ethical practices, obstructing pirate fisherman and fish that are caught outside of legal fishing areas from being sold.

Hyperledger Premier member Intel is collaborating with the Hyperledger community to implement a modern approach to seafood traceability. Leveraging the Hyperledger Sawtooth framework, the seafood journey can now be recorded from ocean to table.

IoT sensors can be attached to any object (like fish) that is entrusted to someone else for transport, with trackable ownership, possession, and telemetry parameters such as location, temperature, humidity, motion, shock and title. The final buyer can access a complete record of information and trust that the information is accurate and complete.

Revolutionizing the seafood supply chain is just one example of the many ways Hyperledger Sawtooth can have real world benefits.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

intel

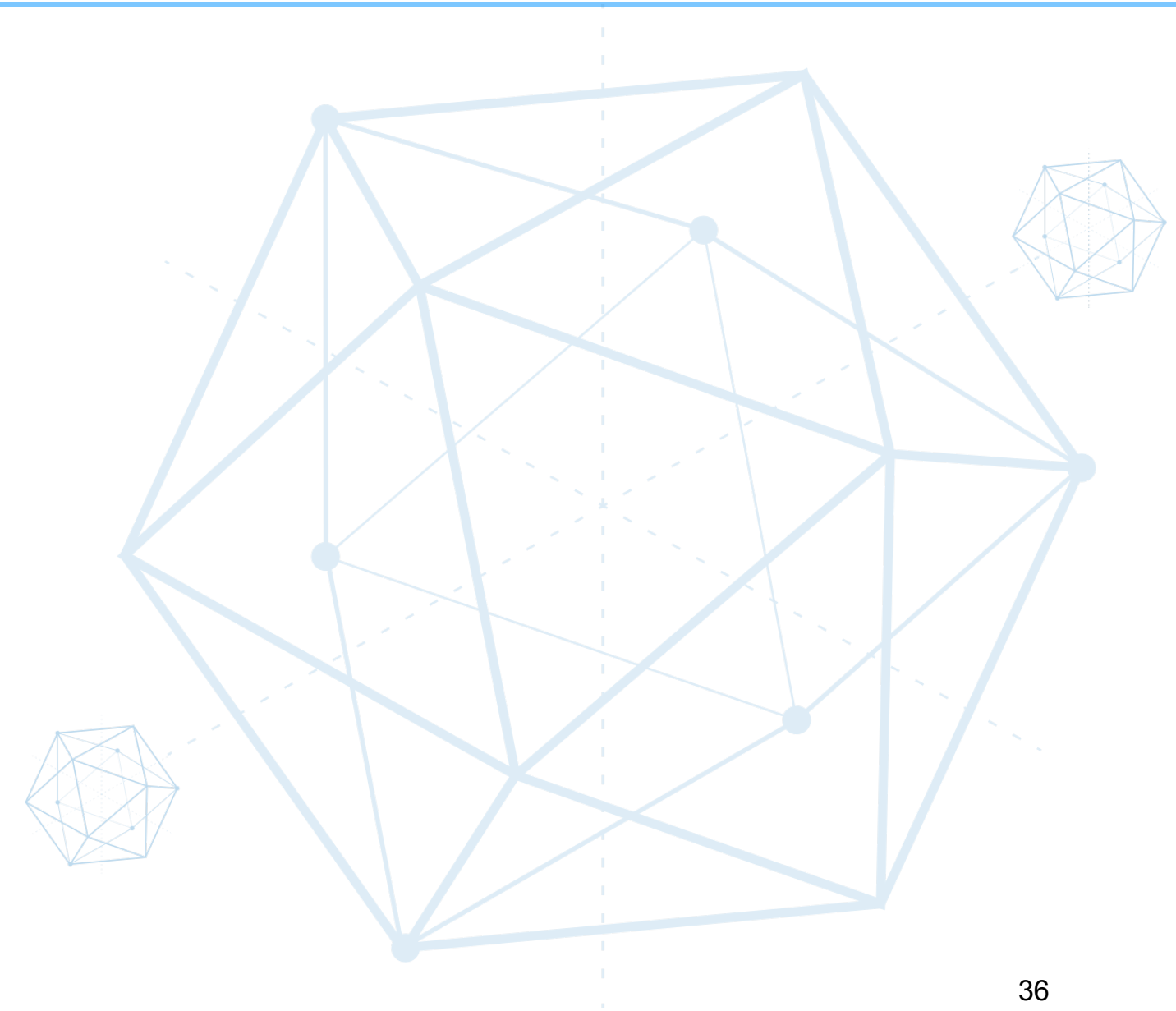
Intel has revealed a public demo that finds it showcasing how a seafood supply chain can be built using Hyperledger Sawtooth.

Watch the explainer video and read the full case study on the Hyperledger Sawtooth project page.

Read about the demo in CoinDesk.

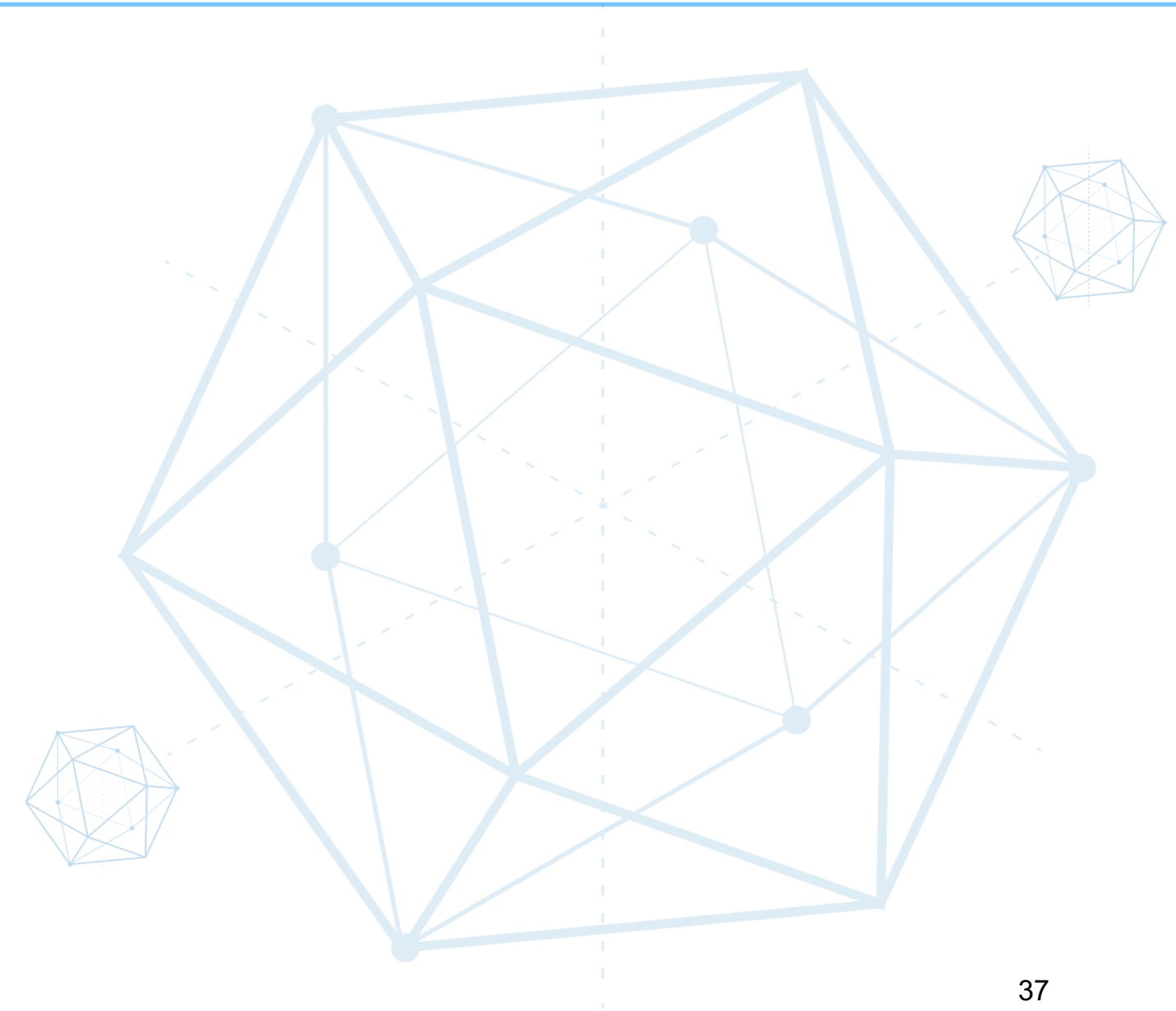
Outline

- Concepts
- History
- Scenarios
- **Challenges**
- Q&A



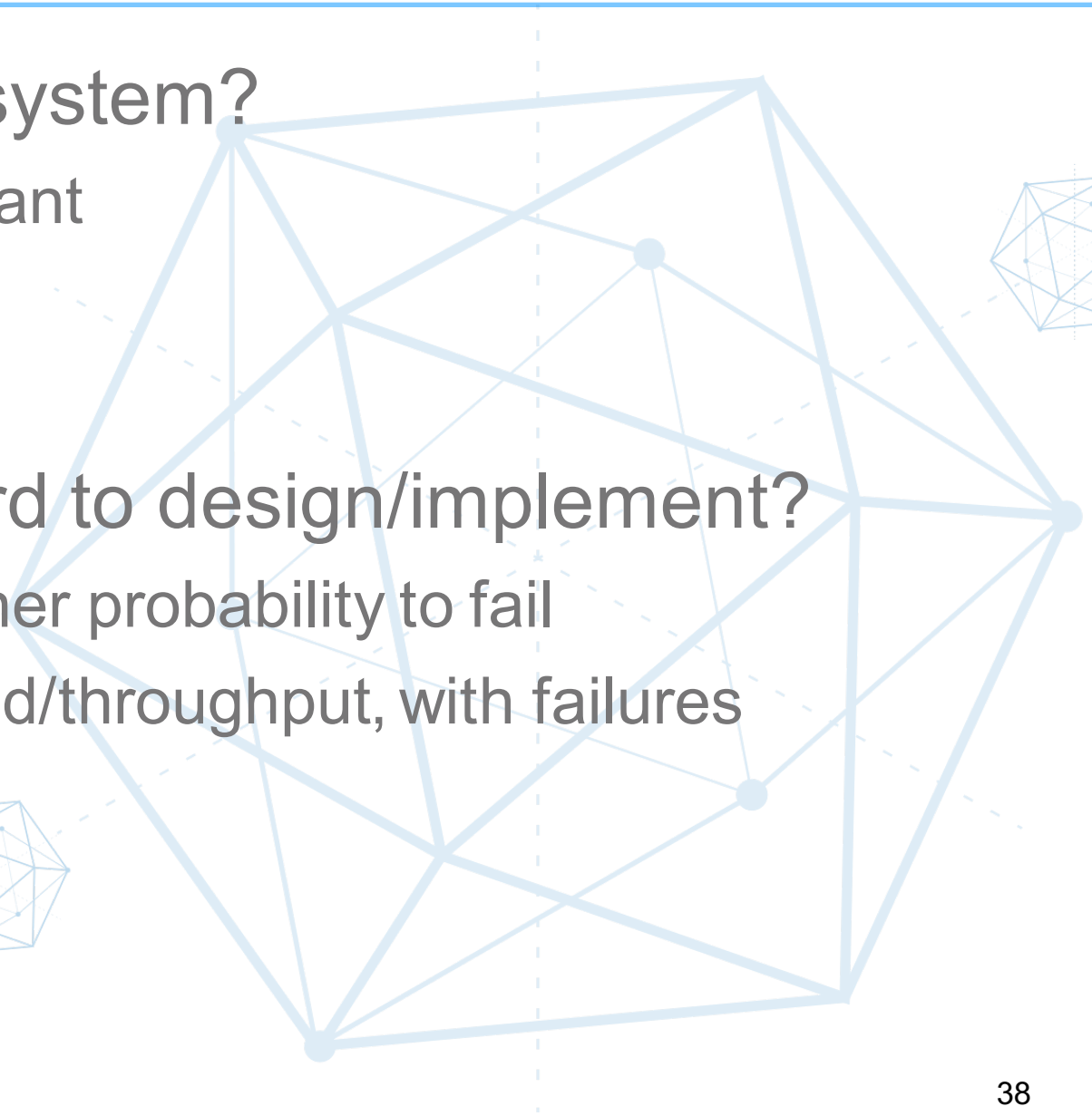
Technical Challenges in Distributed Ledger

- Distributed System
- Security
- Performance
- Inter-operability

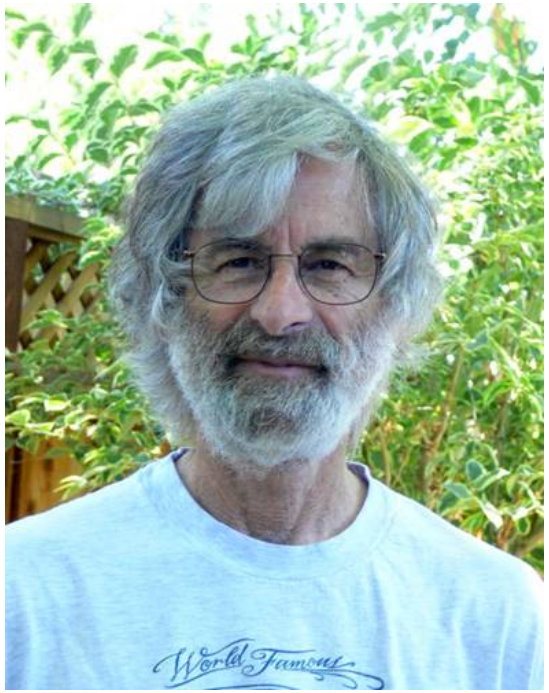


Challenges: Distributed System

- Why do we need distributed system?
  - Single node cannot be fault-tolerant
  - Performance limit
- Why distributed system is hard to design/implement?
  - The larger the system is, the higher probability to fail
  - Communication is limited in speed/throughput, with failures
  - Relative time/space



Challenges: Distributed System

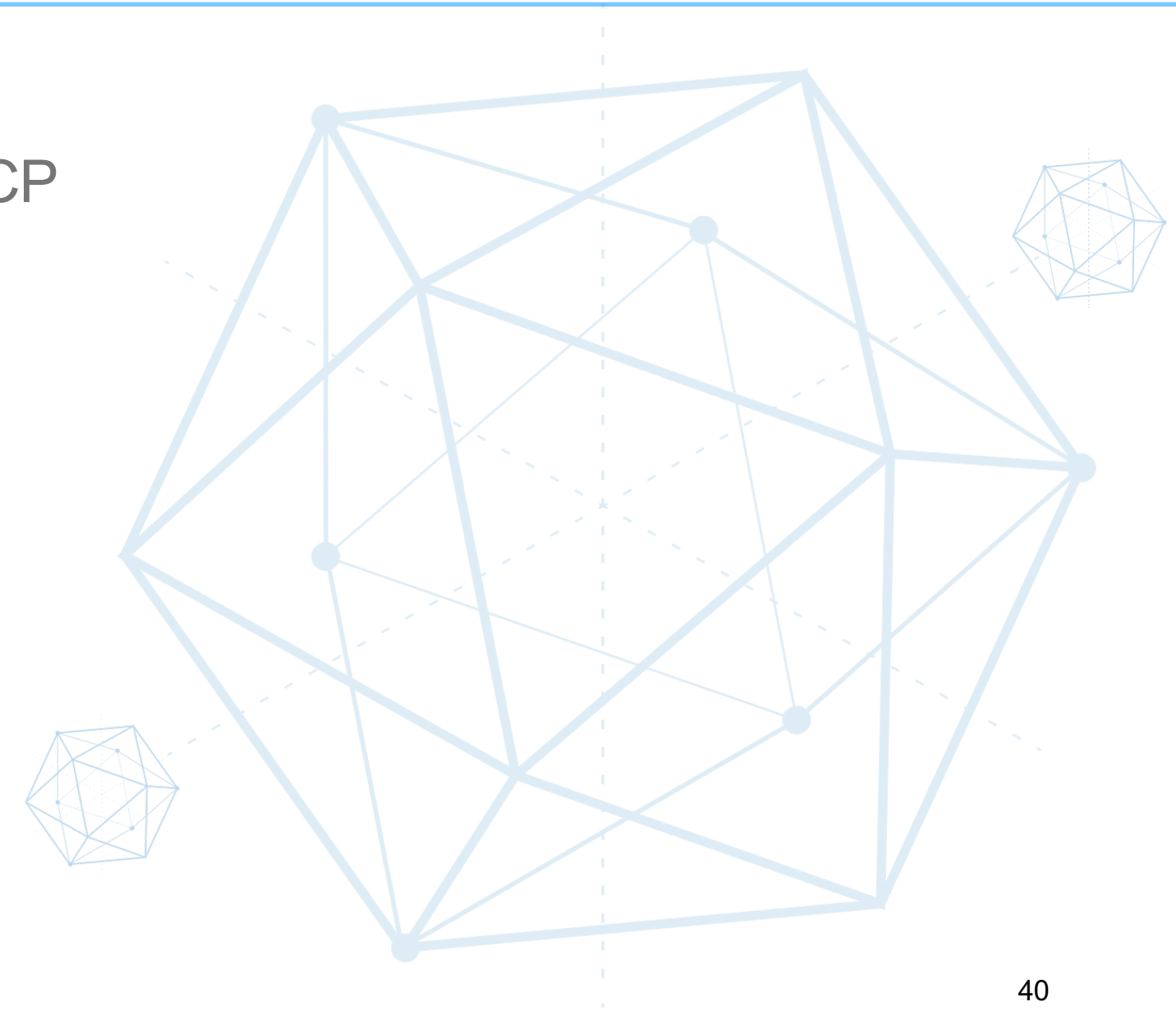


Leslie Lamport, Turing Award 2013

Barbara Liskov, Turing Award 2008

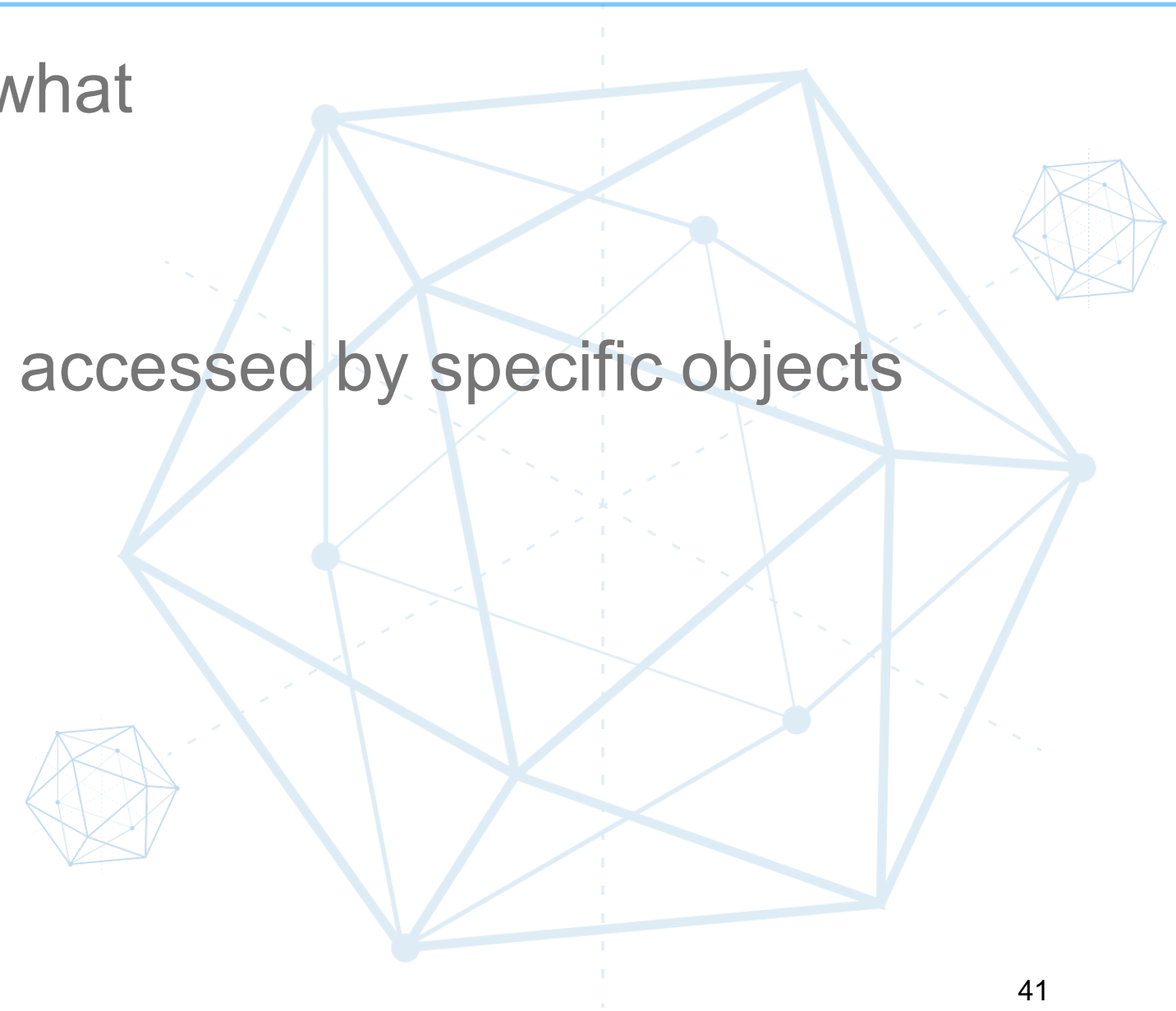
Challenges: Distributed System

- Networking
  - Protocols: gRPC, HTTP2, TCP
  - P2P algorithm
- Consensus Service
- Storage



Challenges: Security

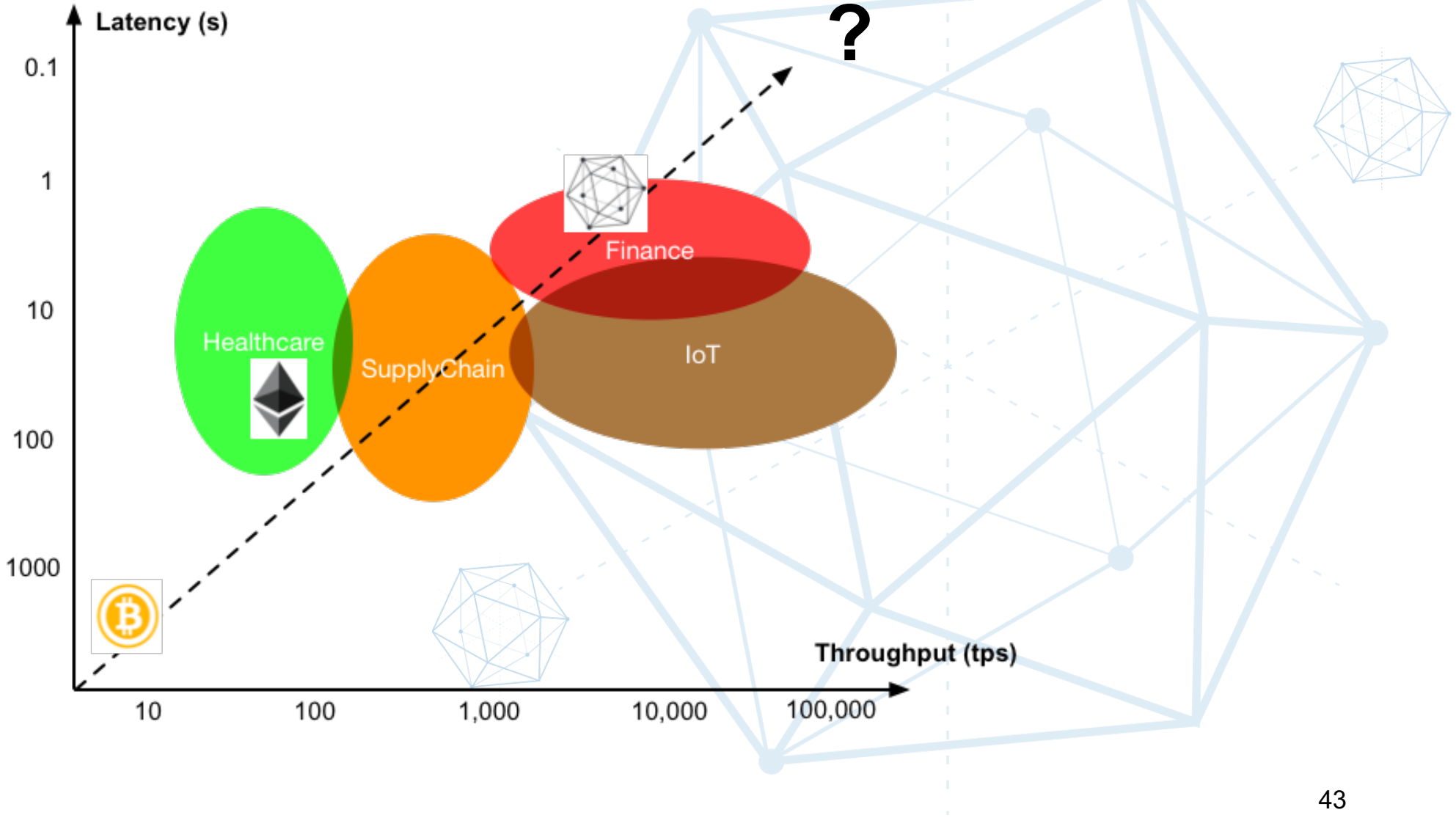
- Permission: Who can do what
  - Consortium, Organization
  - Admin, Member, Audit
- Privacy: Data can only be accessed by specific objects
  - Modern Encryption
  - Hashing
  - Zero Knowledge
- Quantum Computing



Challenges: Performance

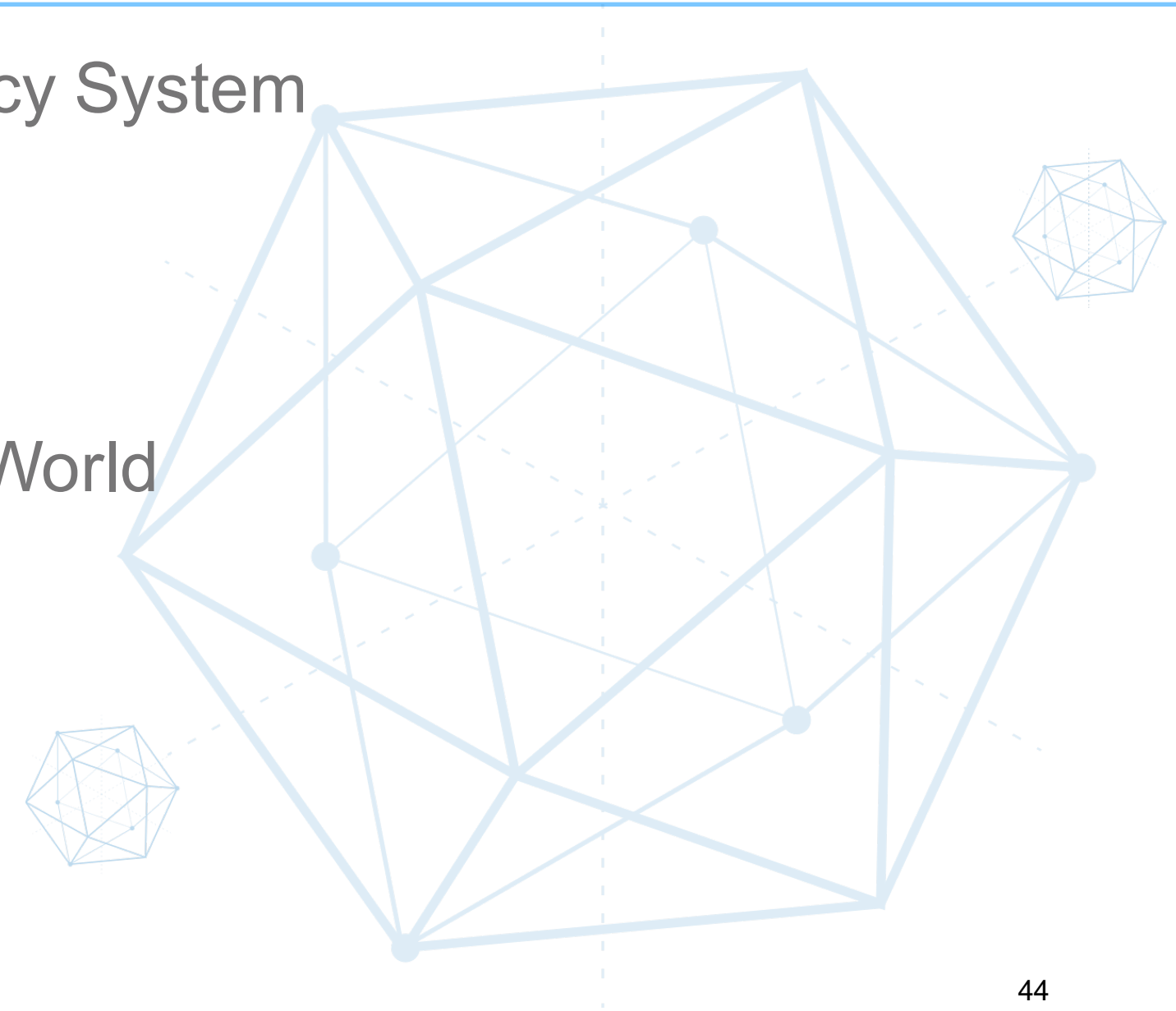
- Public Blockchains
  - 1~100 tps
  - 10s ~ mins
- Permissioned Blockchain
  - 1k~10k tps
  - 1~10s
- Communication & Computing & Storage

Performance? It depends!



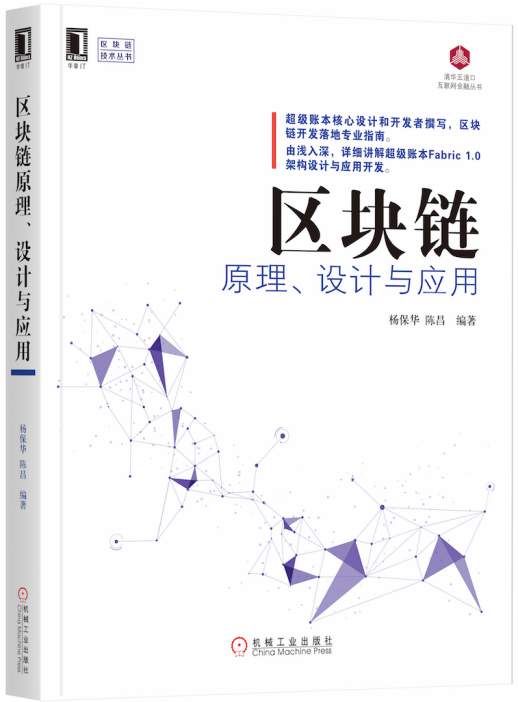
Challenges: Interoperability

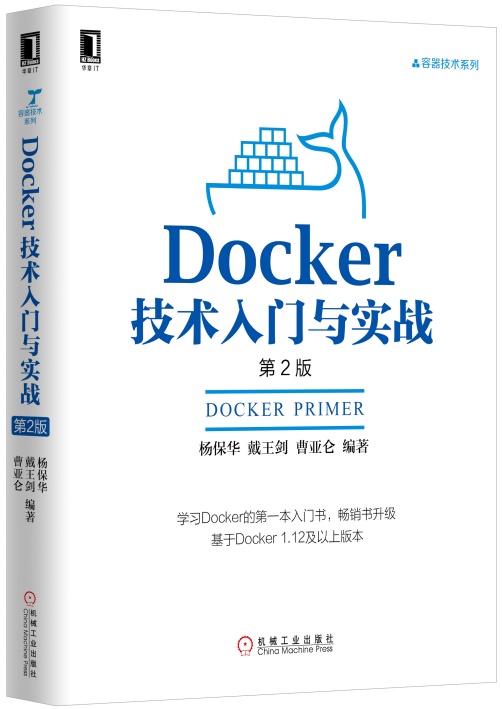
- Interoperability with Legacy System
  - DataStore
  - BI
- Interaction with Physical World
  - Legal
  - Law
  - Business Entity



Reference

- Hyperledger Project
- Hyperledger Wiki
- 《区块链原理设计与应用》
- 《Docker 技术入门与实战》
- github.com/yeasy/blockchain_guide
- github.com/yeasy/docker_practice





HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Questions?

Thank You!
@baohua

Slides available at github.com/yeasy/seminar-talk#hyperledger