HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

An Introduction to Hyperledger

Purpose of This Paper

This paper provides a high-level overview of Hyperledger: Why it was created, how it is governed, and what it hopes to achieve. The core of this paper presents five compelling uses for enterprise blockchain in different industries. It also describes the open source frameworks and tools that Hyperledger is developing to help enterprises around the world deliver on the promise of blockchain for more secure, more reliable, and more streamlined interactions.

This is not intended as a deep technical white paper, but an introduction to Hyperledger for a general business reader.

Intended Audience

We expect this paper will be read by business people from different backgrounds, including entrepreneurs, executives, IT managers, and software developers. Since the blockchain is so new, we expect different readers will be more or less familiar with certain blockchain terms and concepts. And since Hyperledger is a worldwide project, we expect this paper will be read by people around the world, many of whom do not have English as their first language.

Therefore, we tried to make this paper as clear and readable as possible. The **Further Resources** section at the end points to more introductory and more advanced materials you may want to explore.

ABOUT HYPERLEDGER

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in banking, finance, Internet of Things, manufacturing, supply chains, and technology. The Linux Foundation hosts Hyperledger under the foundation. To learn more, visit: hyperledger.org. Hyperledger does not promote a single blockchain codebase or a single blockchain project. Rather, it enables a worldwide developer community to work together and share ideas, infrastructure, and code.

V1.1 published August 2018.

Acknowledgements

The Hyperledger White Paper Working Group would like to thank all the following people for contributing to this paper:

Tamas Blummer, Sean Bohan, Mic Bowman, Christian Cachin, Nick Gaski, Nathan George, Gordon Graham, Daniel Hardman, Ram Jagadeesan, Travin Keith, Renat Khasanshyn, Murali Krishna, Tracy Kuhrt, Arnaud Le Hors, Jonathan Levi, Stanislav Liberman, Esther Mendez, Dan Middleton, Hart Montgomery, Dan O'Prey, Drummond Reed, Stefan Teis, Dave Voell, Greg Wallace, Baohua Yang.

We would also like to thank the Hyperledger Technical Steering and Marketing Committees for their valuable feedback throughout the writing of this paper.

1 Introduction

This section explains the basic concepts of blockchain as a new type of shared database or distributed ledger.

Databases are everywhere

Everyone has heard of "databases." We use them every day. For example, the contacts list on a phone is a simple database—an electronic version of a paper address book.

More elaborate databases include lists of customers, employees, patients, or voters, and their properties and relationships. Even more complex databases might contain lists of instructions or *programs* that can interact with one another.

In fact, you can think of a **database** as any organized set of information where you can find and possibly update items.

Ever since the computer revolution began in the 1950s, databases have played an important part in business and society. Databases began as simple applications with all the data arranged in flat files, like a list of contacts. Then they evolved to use hierarchies—more like org charts.

As companies called for more speed and power, databases became **relational** with all the information arranged as rows and columns in tables. You can **query** a relational database to pull out specific information, such as all your contacts called "Smith" who live in Oregon. You can't do that with a paper address book.

Many databases today are shared

By now, the world is so connected that different people often need to access the same data. To meet this need, **distributed databases** have emerged, where certain chunks of data can be accessed by more than one person at once.

For example, to make it simpler to set up or reschedule meetings, all the members of a workgroup can share their meetings on an online calendar. You can't do that with a paper calendar.

Of course, more elaborate shared databases are used in business. Consider a company's list of stock on hand, organized by SKU, and shared by the order desk at head office and by a sales rep with a laptop in the field.

Both the home office and the sales rep can query the database to see what's in stock, take orders, and allocate stock-on-hand to customers.

But shared databases raise questions

Once you start sharing a database with others, many questions arise:

- Who do you trust to share your data?
- How can you tell that someone is who they say they are online?
- What are they allowed to do to the database?
- What happens if both head office and the sales rep want to sell the same items?
- Who settles any conflicts or disputes?

Clearly, there are many practical issues with sharing a database. Over the years, people have tried many different solutions. One exciting new way to share databases that can help solve these problems is through *blockchain* technology.

Blockchain is the technology behind Bitcoin

The media is full of stories on Bitcoin and other **cryptocurrencies**. But most businesses don't care too much about cryptocurrencies. Most businesses are happy buying and selling with dollars, euros, pounds, yen, or any other accepted currency —perhaps even a cryptocurrency—as long as it works for them.

What's far more significant for enterprises is the technology behind cryptocurrencies, called blockchain.

"It's not Bitcoin, the still speculative asset, that should interest you," write Don and Alan Tapscott in their book *Blockchain Revolution*.[1] Instead, they point to "the power and potential of the underlying technological platform" as what will interest most business people.

Blockchain is a new form of shared database

A **blockchain** is a distributed database with no central authority and no point of trust. When you want to share a database, but you don't have a lot of trust in the other people who might use it, a blockchain can be very helpful.

In this context, **"trust"** could mean many things. Trust could mean trusting others to perform actions on the database properly. Trust could mean not trying to pry into each other's private information. Or trust could mean not degrading someone else's performance to gain a competitive advantage.

Discussing trust brings up the two main kinds of blockchain.

Most cryptocurrencies use **permissionless** blockchains where anyone can join and have full rights to use it. For example, anyone can buy Bitcoin or Ether because those use wide-open, permissionless blockchains.

On the other hand, business blockchains tend to be **permissioned**. This means a person needs to meet certain requirements to perform certain actions on the blockchain. Some permissioned blockchains restrict access to pre-verified users who have already proven they are who they say they are. Others allow anyone to join, but only let trusted identities verify transactions on the blockchain.

Remember our example of the database shared between head office and the field reps of a company. If a blockchain was used to manage that database, it would definitely be permissioned: Everyone accessing the blockchain would have to be an employee of the company or perhaps a trusted trading partner.

Blockchain permissions and consensus

In the database shared between head office and field reps, this question came up: What happens if two different reps want to sell the same items, but there aren't enough on hand to fill both orders?

If that database were managed with a permissioned blockchain, this problem could be solved through a process called **consensus**.

Blockchains use consensus systems to make sure the information in the database is always correct. For example, a consensus system would use pre-established rules to determine which field rep gets the limited items in stock.

Consensus systems take many different forms with different names.

For instance, Bitcoin uses a proof-of-work consensus, where the participants' computers solve difficult math problems. Other types of consensus are called proof of elapsed time and proof of stake. Many permissioned blockchains use something called Byzantine Fault-Tolerant consensus algorithms.

No matter how they're built, all blockchains rely on **cryptography**, the art and science of encoding information so that it's difficult to decode.

Basic identity management—proving you are who you say you are—usually involves digital signatures and a certificate authority. More advanced systems to manage privacy and permissions call for more advanced cryptography.

The good news is, you don't have to understand the intricate details of blockchains to understand how useful they can be.

Why blockchain matters to business people

With blockchains, many existing business processes in many industries can be streamlined to save time, save money, and reduce risk. And many entirely new processes—perhaps even whole new industries—can be invented.

As the Tapscott book explains, the first generation of the Internet was great for sharing information: things like e-mail, documents, photos, webpages, songs, and videos. But there was a problem. It was hard for anyone to prove they were who they said they are.

Every transaction that involved any value required a middleman, like a bank or credit card company, to confirm the buyer and seller and validate the transaction. That created friction, delay, and expense—and a central point of failure that hackers could attack.

Blockchain opens the door to a second generation of the Internet much better-suited for exchanging value, including valuable information.

With blockchains, people can establish who they are and then trade items like money, stocks and bonds, intellectual property, deeds, votes, loyalty points, and anything else that has value.

Even if the traders don't know or trust each other, they can trust the technology to record the transaction in a tamper-proof way. And the technology removes the need for any middleman, which saves time and cuts costs.

Hyperledger was created to further blockchain for enterprises

Hyperledger began in 2015 when many different companies interested in blockchain technology realized they could achieve more by working together than by working separately.

These firms decided to pool their resources and create open-source blockchain technology that anyone could use. These far-sighted companies are helping blockchain to become a more popular and industry-standard technology.

Hyperledger was put under the guardianship of the Linux Foundation (for a host of reasons that we'll talk about later) and has grown rapidly in the last few years.

As of publication date, Hyperledger has more than 230 organizations as members—from Airbus to VMware—as well as 10 projects with 3.6 million lines of code, 10 active working groups, and close to 28,000 participants who have come to 110+ meetups around the world. Through 2017, the project was mentioned in the press an average of 1,500 times a month.

Those of us involved with Hyperledger think the future of blockchain will involve modular, open-source platforms that are easy to use. With Hyperledger, we aim to create an environment that enables us to make this vision a reality.

2 Why Open Source for Blockchain?

"Proprietary software" refers to a commercial product licensed by a vendor, normally for a fee. No one but the original publisher is supposed to see or touch the code. On the other hand, open source is software that anyone can download, view, and change. This section explains why open source makes a lot of sense for enterprise blockchains.

Open source is popular and reliable

When properly designed, coded, and deployed, open source is a proven and effective choice.

For example, the **Linux** operating system runs 90% of the public cloud workload, more than 80% of the world's smartphones, and 99% of all supercomputers.[2]

The open source **Apache web server** has been the world's most popular web server for more than 20 years, and today supports more than 40% of all active websites.[3]

Other well-known open source software includes **mySQL**—the world's most popular database server—and the **Firefox** web browser.

Open source has some clear benefits

According to two recent surveys of executives and developers,[4] here are the key reasons why enterprises choose open source software:

- Competitive features and capabilities
- No vendor lock-in, so customers can easily switch
- High-quality solutions
- The ability to customize and fix bugs, through access to source code
- Lower total cost of ownership

In the early days of open source, its main attraction was that it was "free."

Today, however, enterprises choose open source to reduce risk, gain speed-to-market, and get a competitive edge. Organizations want their programmers to focus on strategic projects that add significant value—such as building industry-specific enhancements on top of a proven platform—rather than re-inventing the wheel.

All these benefits are heightened when an enterprise confronts any profoundly new or challenging concept—like the web in years past—and like blockchain today. Rather than develop an entire infrastructure and engineer all of its own solutions, enterprises can "stand on the shoulders" of others who already did pioneering work and freely shared it with the world.

Open source builds trust

Blockchain represents a perfect opportunity to benefit from open source, since the concept of trust is woven deeply into all blockchain technologies.

Blockchain systems are engineered to enable direct, peer-to-peer transactions between parties who don't fully trust one another, or don't trust any central authority to validate transactions or settle disputes. Therefore, it's essential for these parties to trust in blockchain technologies.

We believe that an open, collaborative approach that invites participation from all stakeholders is the most effective way to build trust for enterprises—enough trust for them to widely and rapidly adopt blockchain technologies.

Open governance

Open governance means that technical decisions—such as which features to add, how to add them, and when to add them—are made by a group of community-elected developers drawn from a pool of active participants. Anyone can participate in Hyperledger by becoming a contributor and/or maintainer.

Becoming a developer or maintainer translates into one thing: trust. You know how decisions will be made and how people will be selected to make these decisions. Hyperledger is vendor-neutral and technical contributions are based on meritocracy.

Companies deploying blockchain internally, and those building products and services based on Hyperledger projects, tell us they trust Hyperledger because our technologies are built in the open by a broad community.

Open source promotes interoperability

"Interoperable" means that a program can work with other programs—even those from other organizations—to quickly and easily perform a function. In today's connected world, this is a must-have. And in the future, we believe that many blockchains will support many business processes for many organizations.

Hyperledger eases interactions between blockchains. The open source Hyperledger technologies are designed from the start to support interoperability across various blockchains. In particular, Hyperledger Quilt is expressly designed to support cross-chain transactions.

Open source makes sense for blockchain

Both economics and common sense are on the side of a collaborative effort like Hyperledger.

Enterprises need robust, feature-rich, modular blockchain platforms they can tailor to meet their requirements. Businesses as diverse as banks, car and airplane makers, and healthcare companies make a broad ecosystem of enterprises, all cooperating with the global Hyperledger developer community.

When many different users and vendors collaborate to co-create common technologies, everyone can enjoy the proven benefits including lower risk, higher quality, and faster time-to-market. We believe we can do more to advance blockchain technologies by working together than by working in isolation.

3 The Greenhouse for Enterprise Blockchain

Hyperledger serves as a “greenhouse” that brings together users, developers, and vendors from many different sectors and market spaces. All these participants have one thing in common: All are interested in learning about, developing, and using enterprise blockchains.

While blockchain is a powerful technology, it is not one-size-fits-all.

Every enterprise needs special features and modifications to help a blockchain achieve its intended purpose. Since different organizations have different needs, there will never be one single, standard blockchain. Instead, we expect to see many blockchains with different features that provide a wide range of solutions across many industries.

Hyperledger provides a greenhouse structure that can incubate new ideas, support each one with essential resources, and distribute the results widely. A greenhouse structure can support many different varieties while consuming far fewer resources.

As the greenhouse organization for open source blockchain development, Hyperledger provides these benefits:

- Help keeping up with developments
- Better productivity through specialization
- Collaboration to avoid duplicate efforts
- Better quality control of code
- Easier handling of intellectual property

Help keeping up with developments

Navigating through all the developments in an open source environment can be daunting. Due to the cost and complexity involved, some organizations may give up, or never get started at all.

Hyperledger reduces this research burden by creating a collaborative environment that streamlines communication. Better communication helps new participants to catch up, by gaining faster access to necessary information. As newer participants quickly join the collaborative effort, this speeds up development for the benefit of the entire community.

Better productivity through specialization

A basic premise of economics ever since Adam Smith is that **specialization**—also known as division of labor—leads to higher productivity. Instead of everyone doing a little bit of everything, specialization enables people to focus their energies on fewer tasks and become more expert at them. The benefits of specialization include more expertise, more value added, and ultimately more wealth created. This is why specialization has proven to be a driving factor in global economic development.

Participants can gain the same benefits—more expertise, more value added, and better all-around productivity—by specializing in certain areas of a new technology like blockchain. In an open source environment without any greenhouse organization, this would be far more difficult.

Hyperledger’s greenhouse structure encourages specialization, which yields better productivity. And participants who happen to specialize in similar areas aren’t competing against each other. In a greenhouse organization, specialists are encouraged to join forces to accelerate their research and development.

Collaboration to avoid duplicate efforts

In a siloed environment, many people can unwittingly duplicate each another’s efforts. Duplication of effort is especially negative in a new industry like blockchain, where the talent pool of seasoned developers is not yet deep.

In a greenhouse organization, collaboration between participants is highly encouraged. This can avoid duplication, streamline the development of new projects, and encourage the creation of common components that benefit the entire community.

Interoperability between various distributed ledgers is also enhanced by a better understanding of other projects. And the governing structure provided by Hyperledger can help solve any interoperability disputes that could potentially arise.

Better quality control of code

Open source software is recognized for its high quality, achieved through careful code reviews and significant debugging. Hyperledger promotes quality control by having a technical governing committee review all projects throughout their life cycles. This gives new projects a chance to be critiqued, so their developers can gain knowledge from all the existing projects. For their part, long-time project members may discover innovations in new projects which can enhance their own projects. This greenhouse structure also fosters interoperability between new and existing projects.

Easier handling of intellectual property

Another benefit provided by the greenhouse structure is easier, more consistent handling of intellectual property. Hyperledger operates under an Apache 2.0 license for code (see **apache.org/licenses/LICENSE-2.0**) and Creative Commons Attribution 4.0 International license for content (see **creativecommons.org/licenses/by/4.0/**). Both these licenses are known to be especially enterprise-friendly.

A single, consistent approach to intellectual property removes the need for complex and expensive contractual relationships among members. Since all participants have clearly communicated their expectations, anyone building and using Hyperledger technologies can participate without fear of running into hidden legal encumbrances.

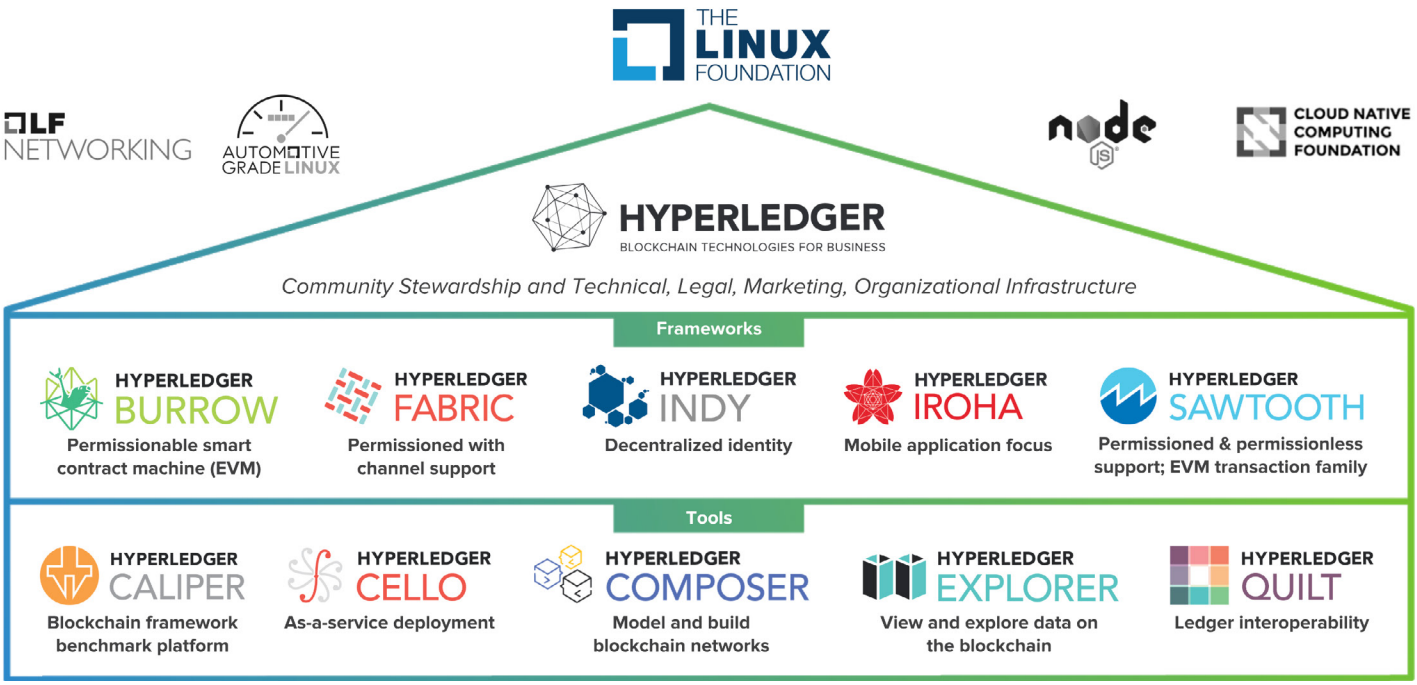

FIGURE 1: THE HYPERLEDGER GREENHOUSE STRUCTURE

4 Hyperledger Design Philosophy

Distributed ledgers can have vastly different requirements for different use cases. For instance, when participants share high levels of trust—such as between financial institutions with legal agreements—blockchains can add blocks to the chain with shorter confirmation times by using a more rapid consensus algrithm. On the other hand, when there is minimal trust between participants, they must tolerate slower processing for added security.

Hyperledger embraces the full spectrum of use cases. We recognize that different enterprise scenarios have different requirements for confirmation times, decentralization, trust, and other issues, and that each issue represents a potential "optimization point" for the technology.

To address this diversity, all Hyperledger projects follow the same design philosophy. All our projects must be:

- Modular
- Highly secure
- Interoperable
- Cryptocurrency-agnostic
- Complete with APIs

Modular

Hyperledger is developing modular, extensible frameworks with common building blocks that can be reused. This modular approach enables developers to experiment with different types of components as they evolve, and to change individual components without affecting the rest of the system. This helps developers to create components that can be combined to build distributed ledger solutions well-suited to different requirements.

This modular approach also means that a diverse community of developers can work independently on different modules, and re-use common modules across multiple projects.

The Hyperledger Architecture Working Group defines functional modules and interfaces for issues such as communication, consensus, cryptography, identity, ledger storage, smart contracts, and policy. To find out more, visit **wiki.hyperledger.org/groups/architecture/architecture-wg**.

Highly secure

Security is a key consideration for distributed ledgers, especially since many use cases involve high-value transactions or sensitive data. With large codebases, many networked nodes, and valuable data flows, distributed ledgers have become prime targets for online attackers. Securing a blockchain is quite a difficult task: Distributed ledgers must provide a large set of features and functions, while resisting persistent adversaries.

Security and robustness are the keys to enable enterprise-class blockchains to evolve, and provide the critical infrastructure for next-generation business networks.

Hyperledger projects embrace security by design and follow the best practices specified by the Linux Foundation's Core Infrastructure Initiative. To find out more, visit **coreinfrastructure.org/**.

As such, all Hyperledger algorithms, protocols, and cryptography are reviewed and audited by security experts, as well as the wider open source community, on a regular basis.

Interoperable

In the future, many different blockchain networks will need to communicate and exchange data to form more complex and powerful networks. At Hyperledger, we believe that most smart contracts and applications should be portable across many different blockchain

networks. This high degree of interoperability will help meet the increased adoption of blockchain and distributed ledger technologies.

Cryptocurrency-agnostic

Hyperledger projects are independent and agnostic of all alt-coins, cryptocurrencies, and tokens. Hyperledger will never issue its own cryptocurrency; this is decidedly not our purpose. Hyperledger exists to create blockchain software for enterprises, not to administer any cryptocurrency.

However, the design philosophy includes the capability to create a token used to manage digital objects, which may represent currencies, although this is not required for the network to operate.

Complete with APIs

All Hyperledger projects provide rich and easy-to-use APIs that support interoperability with other systems. A well-defined set of APIs enable external clients and applications to interface quickly and easily with Hyperledger's core distributed ledger infrastructure. These APIs support the growth of a rich developer ecosystem, and help blockchain and distributed ledger technologies proliferate across a wide range of industries and use cases.

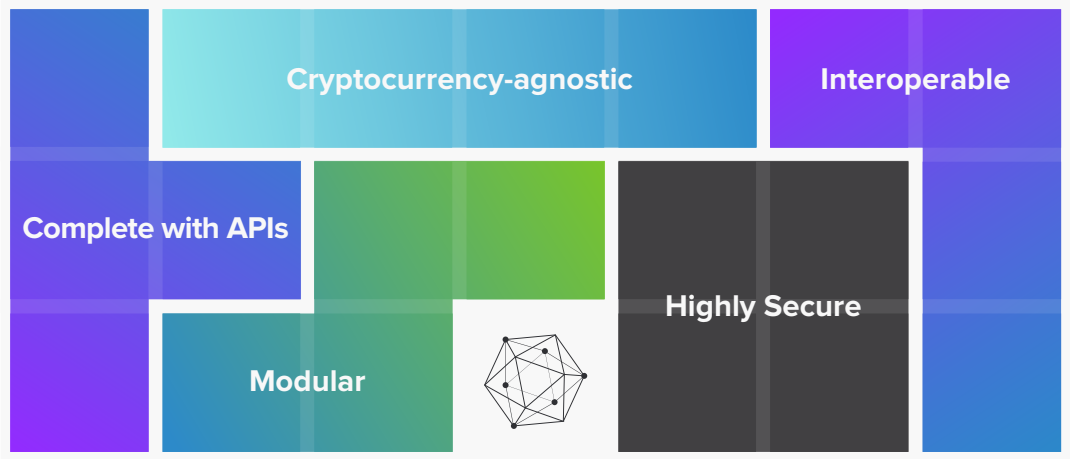

FIGURE 2: THE HYPERLEDGER DESIGN PHILOSOPHY

5 Some Compelling Use Cases

This section describes five concrete examples where blockchain has a clear and compelling use case.

These use cases are drawn from different domains and arranged in alphabetical order:

- Banking—applying for a loan
- Financial services—post-trade processing
- Healthcare—credentialing physicians
- IT—managing portable identities
- Supply chain management—tracking fish from ocean to table

In each case, Hyperledger has useful tools available; in some cases, a proof-of-concept has already been developed.

5.1 Banking: Applying for a Loan

Banks want to lend, but only to borrowers who are good risks. This motivates the banks to gather detailed, personally identifiable information (PII) from everyone who applies for a loan, such as date of birth, annual income, government ID or passport number, and so on.

Ultimately, the banks use this PII to access an applicant's credit rating. Regulations may demand that certain PII is shared with authorities, for example, to prevent money laundering. But retaining so much PII makes every bank a juicy target for hackers.

Seeking a loan isn't much fun for borrowers, either. The application process is intrusive, and it's hard to "shop around" for the best rates. Every new application multiplies the effort and increases the risk that the applicant's PII will be abused.

HYPERLEDGER INDY CAN STREAMLINE THIS PROCESS

Hyperledger Indy offers a transformative identity solution for this use case.

With Indy, applicants can share only the information the banks need to make a decision, in a way that guarantees truth, builds confidence in the lender, and satisfies pressures from regulators.

Anyone seeking a loan can apply to 100 different lenders in milliseconds, without placing any sensitive personal data into a hackable database.

Instead of disclosing any PII, loan applicants can generate zero-knowledge proofs that they are over 21, that their income on last year's taxes passed a certain threshold, that they hold a valid government ID number, and that their credit score met a certain threshold within the past week.

Strong, distributed ledger-based identity establishes a global source of truth, which delivers value to many parties. Applicants can give consent, and everyone can agree on when and how it was given. Lenders can conform with regulations and show an immutable audit trail.

As a result, the market can operate more efficiently: Banks can offer loans with confidence, while applicants can effectively safeguard their PII.

OTHER HYPERLEDGER PROJECTS ADD FURTHER STRENGTHS

This use case becomes even more compelling when you consider the added strengths of other Hyperledger projects.

For example, **Hyperledger Burrow** can turn loan applications into smart contracts, and attach them to strong identities as a seamless next step. And **Hyperledger Fabric** can drive a membership system by linking to the pre-existing, self-sovereign identity on the loan application.

5.2 Financial Services: Post-Trade Processing

The primary drivers for blockchain in today's financial services are privacy, confidentiality, and accountability.

Compliance guidelines like "Anti-Money Laundering" and "Know Your Customer" require that banks and service providers can verify a customer's legal identity and give them clearance to do transactions. These requirements drive the adoption of permissioned and private blockchains, since public blockchains can risk compromising a participant's privacy and confidentiality.

Together with the large volumes of transactions, these are the main reasons why consortium blockchains are gaining momentum in financial services. Among many possible use cases in this industry—especially in capital markets—post-trade processing can benefit from blockchain.

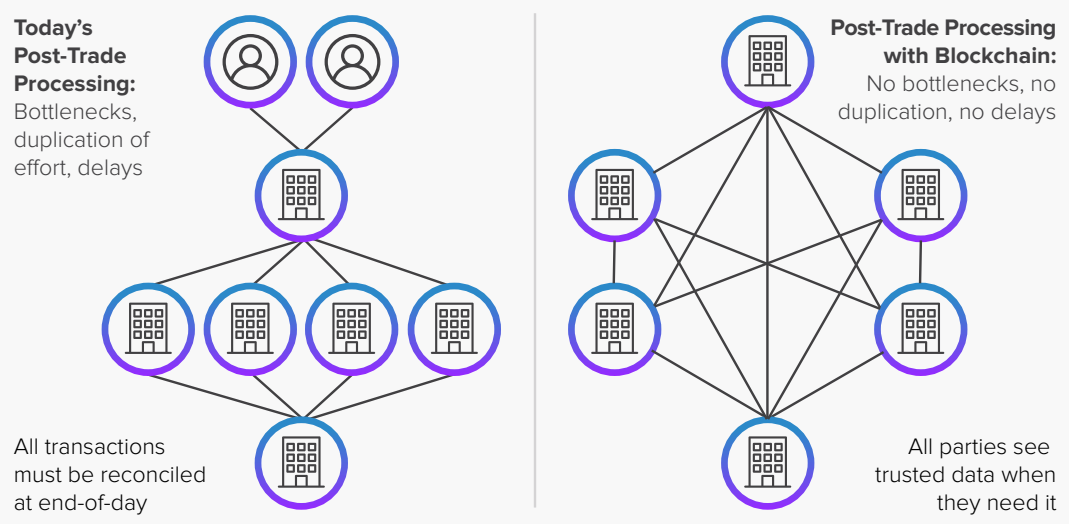

FIGURE 3: POST-TRADE PROCESSING, WITH AND WITHOUT BLOCKCHAIN

THE MANY STEPS IN POST-TRADE PROCESSING

Post-trade processing includes all the activities done after a trade is completed. This covers transactions done over-the-counter (OTC) or at an exchange.

On a high level, post-trade processing includes these steps:

1. **Trade validation**—Validating and confirming the transaction following the execution of the trade.
2. **Clearing**—Matching the trade instructions and confirmations across the different counterparties as well as the potential netting activities.[5]
3. **Settlement**—Legally realizing the contractual obligations to reach the finality of the transaction. This includes support processes such as notifying all entities affected by the transaction.
4. **Custody activities**—Adjusting the positions held with the custodians on behalf of the counterparties.
5. **Reporting**—Satisfying all reporting requirements for regulatory and internal risk, i.e., the transaction's contribution to the market and credit risk of each counterparty.

ISSUES WITH TODAY'S POST-TRADE PROCESSING

Today, all these steps are typically done through a fragmented workflow that spans numerous departments across different entities: brokers, central security depositories, clearing houses, exchanges, settlement agents, and so on. Every trade involves many different interfaces, processes, and reconciliation efforts.

For example, today both parties send separate settlement instructions to a trusted third party—the settlement agent—which matches both data sets and instructions. Any mismatches trigger prolonged reconciliation efforts or may even result in a failed trade.

All this duplication of effort introduces inefficiency and delays into post-trade processing.

BLOCKCHAIN CAN STREAMLINE POST-TRADE PROCESSING

Compared to the current model, doing post-trade processing on blockchain can be far more efficient.

Leveraging the peer-to-peer strength of a blockchain, one party can insert transaction details for the other party to verify. Doing both processes on the same system can significantly streamline the process, since the network itself can act as a trusted third party, enabled by the immutable and irrefutable nature of transactions on the blockchain.

The complexity can be further reduced, since all data from all steps and all actors can reside on the blockchain, accessible on a need-to-know basis. Any further reconciliation becomes unnecessary. And the blockchain system can also serve as an efficient basis for regulatory and trade reporting.

This means four of the five steps listed above—validation, clearing, settlement, and reporting—can be streamlined by using a blockchain for post-trade processing.[6]

SPECIAL FEATURES REQUIRED FOR POST-TRADE PROCESSING

Any permissioned distributed ledger can provide a tamper-proof, irrefutable transaction log. But to be effective for post-trade processing, a blockchain requires several added features, such as immediate finality, future-proof confidentiality, and streamlined performance.

Immediate finality: Any distributed ledger used for capital markets must offer immediate finality, so that the receiver can be assured that the transactions are valid and committed. Consensus algorithms such as proof of work (PoW), proof of stake (PoS), or proof of elapsed time (PoET) can cause temporary forks and even transaction rollbacks. These are unacceptable in post-trade processing. Any blockchain for this use case must use a consensus algorithm that provides immediate finality.

Future-proof confidentiality: Participants in any trade expect their transactions to remain private and confidential. The clearing house recording the transaction must ensure that parties can't see each other's position or trading information. Even with anonymized data, the existence of trades must not be revealed, since this can make transactions susceptible to traffic analysis. Correlated to public market information, this can compromise both a participant's identity and their trading patterns.

In the future, even more stringent requirements for ensuring confidentiality of ledger data may be required. In a typical blockchain where all data is stored on each participating computer, any compromise of the private key—or even worse, the cryptographic hash or encryption algorithm—can lead to the complete unveiling of all historic data for all participants.

Any distributed ledger used for financial services must ensure that all transactions will remain confidential for the foreseeable future.

Streamlined performance: Today, all post-trade activities happen at the end of the business day, which presents different requirements than most other use cases. When using a blockchain, it will not be necessary to transmit the entire day's set of trade records to be reconciled. All trades will be reconciled in near real-time.

Yet the total number of transactions will likely increase, since participants can learn their position with the clearing house in near real-time. This means that while the average number of transactions per second will likely increase, the peak performance requirements will decrease significantly. Overall, system throughput will be faster.

HYPERLEDGER PROJECTS CAN HELP

Several projects from Hyperledger provide features and functions that can help build effective blockchain solutions for post-trade processing.

The channels supported by **Hyperledger Fabric** can be deployed as fully disjoint networks with separate endorser sets and ordering nodes to provide privacy and confidentiality. Restricting data replication only to permissioned parties delivers the benefits of the blockchain for data integrity and non-repudiation of transactions, without compromising data security. Reporting requirements—both internal and external—can be satisfied by including a regulatory agency and other oversight entities as members of the channel. Network segmentation enabled by Fabric's channels can support multiple jurisdictions and regulatory regimes.

The transaction families in **Hyperledger Sawtooth** provide a reliable and powerful way to support post-trade activities. Building complex rules using a preferred language, and exposing only the functions appropriate to the context, enables safer smart contracts. And the option to prohibit deployment of ad-hoc smart contracts further reduces risks for financial institutions.

Hyperledger Indy's unlinkable verifiable claims can be leveraged to report outstanding risk on a shared ledger without compromising privacy. This still enables a regulatory body to take a holistic view of the market, and to help prevent potential market crashes and major defaults. This feature can also strengthen privacy, by putting participants in control of their network identities and any attributes they choose to disclose.

5.3 Healthcare: Credentialing Physicians

Blockchain technologies promise to reduce one of the great annoyances of modern medical practice: "credentialing". Hospitals use the credentialing process to make sure that its physicians are competent and trustworthy. In a sense, credentialing is the hospital's way of performing "due diligence" on a physician.

But today this process imposes a huge burden, both on the physician applying for affiliation and the hospital that must vet the applications.

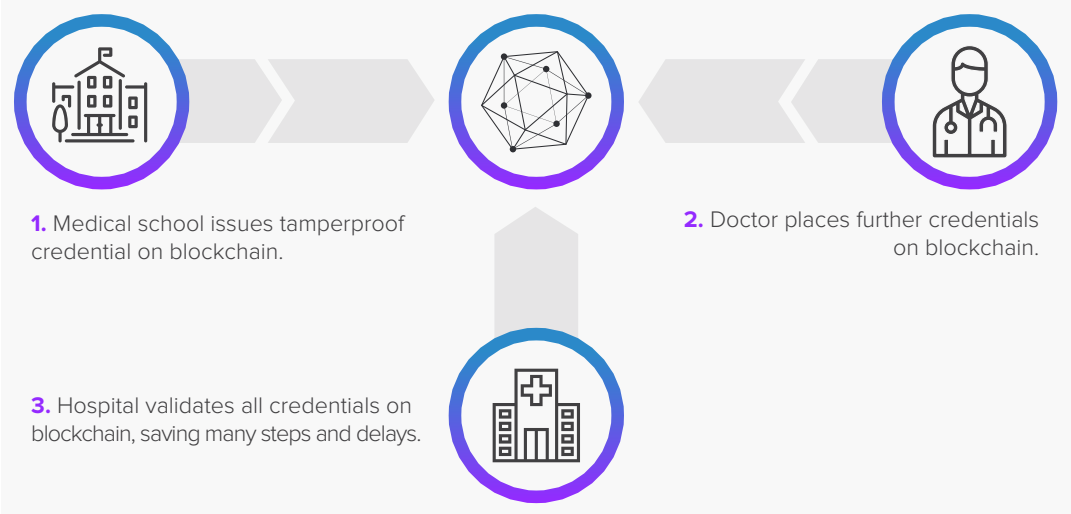

FIGURE 4: BLOCKCHAIN MAKES DOCTOR CREDENTIALING FASTER AND MORE SECURE

THE PHYSICIAN GATHERS CREDENTIALS, MANY ON PAPER

Any physician who wishes to become affiliated with a hospital begins the process by gathering copies of all their professional credentials, such as:

- Medical school diploma
- Certificates of any residencies and fellowships completed
- Certificates from any specialty medical boards
- All state medical licenses
- Evaluations from peers
- Proof of meeting requirements for continuing medical education
- Letters from hospitals where the physician was previously affiliated, explaining how and why the affiliation ended
- Details of any malpractice suits

THE HOSPITAL CHECKS CREDENTIALS AND CALLS A MEETING

On the hospital's side, the credentialing office checks the physician's documentation for completeness, accuracy, and authenticity. This is an exacting task. Almost inevitably, they find shortfalls and go back to the doctor for missing documents.

Then the credentialing office verifies some or all of the physician's documentation. For example, they may phone a medical school to confirm that the physician did indeed graduate from there. This is clearly a time-intensive process that is prone to errors.

Once the documentation is determined to be complete, accurate, and authentic, the hospital's credentialing committee—which typically includes physicians and administrators—meets to decide whether the physician can begin practicing in affiliation with the hospital.

The entire credentialing process is complex, low-trust, and time-consuming. And it can take weeks or even months until any physician is cleared to affiliate with a hospital.

THREE KEY QUESTIONS FOR ANY BLOCKCHAIN SOLUTION

An effective blockchain solution for medical credentialing must answer three key questions about content, identities, and resources.

1. **Will actual content or only pointers to content be placed on the blockchain?**
   Credentialing solutions might place public information (such as state medical licensing) on the blockchain itself. However, private information (such as peer reviews) might be better stored off the chain; this would guard against any loss of keys, and enable users to remove—but not change—private information.
2. **What's the best way to manage the identities of many participants?**
   An ambitious credentialing solution might include every hospital, every physician, every source of continuing medical education, and so on. This could eventually number thousands of participants. How will so many identities be efficiently and securely managed?
3. **What resources are required, especially for storage?**
   Credentialing solutions may be in service for decades, requiring significant resources for processing, communication, and storage. For example, what if at some point credentialing organizations want video testimony from peers? Storage requirements could skyrocket—and who would cover that added cost?

HYPERLEDGER CAN HELP STREAMLINE CREDENTIALING

Credentialing provides a good use case for blockchain technologies, which can simplify and streamline every step of the process.

Hyperledger Indy provides off-the-shelf solutions that would otherwise require architecting and developing new software. One significant feature: Indy implements the proposed W3C standard for verifiable claims, supporting the pairwise exchange of selected credentials. In practice, this can work as follows:

1. A physician requests proof of graduation from their medical school.
2. After creating a pairwise relationship with the physician, the medical school sends the physician a credential, including proof of graduation and any additional data defined. This credential is stored in the physician's edge device. No data from the credential is stored on the ledger. The ledger simply holds credential definitions, public DIDs, revocation registries, and schemas.
3. The physician can share attributes from the credential (such as proof of graduation) as a proof for any hospital. Since all attributes in the proof are signed by the medical school, the hospital can use the blockchain to verify the source, integrity, and revocation status of any attribute.
4. The physician, if they choose, can use zero knowledge proofs and selective disclosure to share only the specific data points the hospital requires, and nothing more.

This implementation of verifiable credentials safeguards the physician's privacy, prevents correlation, keeps personal data off the ledger, and saves time and effort for everyone involved. At last: a better way to handle medical (or any other) credentialing.

5.4 IT: Managing Portable Identities

One of the most exciting applications of blockchain is for self-sovereign identity: the idea that an individual owns their own "identity" and controls the data around it. This has profound implications for enterprise IT.

INDY EXTENDS TRADITIONAL IDENTITY SYSTEMS

Hyperledger Indy is a distributed ledger with a primary focus on self-sovereign identity. Indy shares some features with traditional enterprise identity systems such as 2FA, IDPs, LDAP, OAuth, and so on, namely:

- Industrial-strength cryptography
- Rich metadata about identities
- Sophisticated access control and policy

But there is a profound difference: Indy identities are shared, not siloed and federated. An Indy identity is portable, so you can bring it with you wherever the distributed ledger is accepted.

This means that 10 systems that support Indy identities don't create 10 separate identities for John Q. Public. Instead, all 10 systems access John's pre-existing identity on the blockchain. John can simply show up and use his identity. An organization can cancel John's access, but never his identity, because John owns it himself. And John—not the places that accept John's identity—controls access to his data.

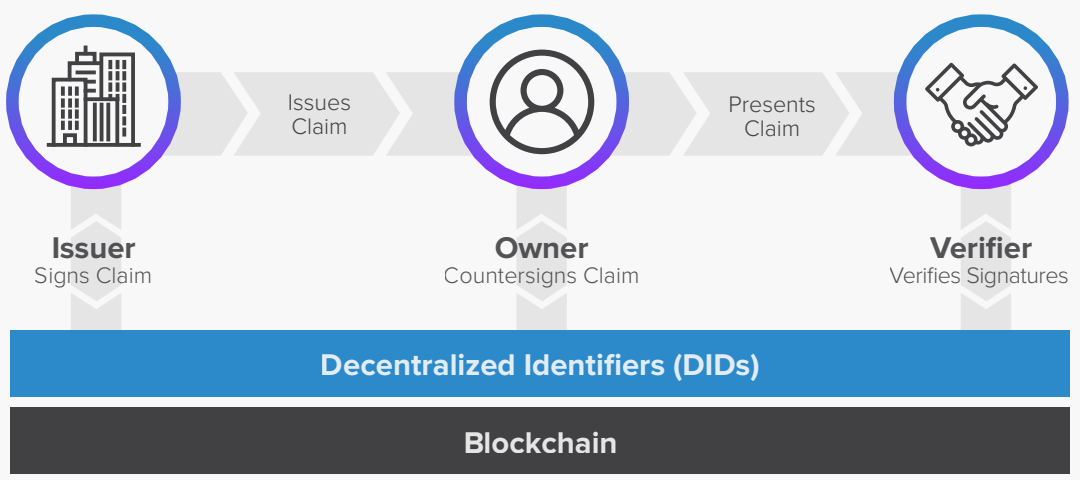

FIGURE 5: MANAGING PORTABLE IDENTITIES WITH BLOCKCHAIN

INDY FITS ENTERPRISE IT BETTER

Indy also shares some features with blockchain-based identity solutions such as Blockstack (**blockstack.org/**) and Uport (**uport.me/**). All these technologies store identity on a distributed ledger to promote security and personal freedom.

However, Blockstack depends on Bitcoin and and Uport on Ethereum. These proof-of-work (PoW) ecosystems impose a high cost on transactions, so that every new persona, pairwise relationship, published attribute, or public key rotation becomes a tangible expense. This creates a disincentive to pairwise relationships, which undermines privacy.

Also, these ecosystems are global and public. They can't be special-purposed for a less-than-fully-global context.

Indy, on the other hand, does not use PoW, so that transactions are free. And different instances of Indy can scale to fit whatever context is convenient. That makes Indy more flexible, more cost-effective, and more practical for managing identities through an enterprise blockchain.

5.5 Supply Chain Management: Tracking Fish from Ocean to Table

Ocean fishing represents more than $70B in worldwide trade.[7] But the industry faces many problems.

For example, estimates suggest at least 20% of all fish are caught illegally—yet only a tiny fraction are ever inspected.[8]

A recent study based on DNA testing found that nearly one in three fish were mislabeled by sellers.[9] And a detailed sampling from 674 outlets across the United States found that 87% of snapper and 59% of tuna were mislabelled—and worse, 95% of all sushi restaurants were serving mislabeled fish.[10]

These issues create health risks for consumers, hurt vulnerable fish stocks, rob nations of taxes, and damage the integrity of the whole industry.

MANY CHALLENGES IN SEAFOOD TRACEABILITY

Traceability and provenance are well-managed for certain local catches such as Maine lobster and Maryland crab. But as shown in Figure 6, the complexity of the ecosystem makes it challenging to achieve better traceability.

A recent study by the non-profit sustainable seafood organization FishWise[11] identified these key problems:

- Many different paths from ocean to table
- Lack of global authority for tracing
- Proprietary tracing systems do not scale
- Most existing processes are paper-based

The supply chain that delivers fish from ocean to table is extremely complex and opaque. It includes many participants from different industries, and regulatory controls that cross national boundaries. That makes this supply chain a perfect opportunity for blockchain technologies.

Oceana, an NGO devoted to protecting the oceans, postulated that a shared platform for traceability would help to improve the accuracy of labeling and reduce pirate fishing: “Despite formidable challenges, seafood traceability is well within reach. Simply by keeping track of where our seafood comes from at every step of the supply chain, we can make progress against pirate fishing.”[12]

A SEAFOOD SUPPLY CHAIN PROTOTYPE

A team at Intel is using **Hyperledger Sawtooth** to build a traceability prototype that combines the distributed ledger, IoT sensors, and advanced communications to track telemetry parameters throughout capture, processing, and transit.

Sensors are attached to the fish when it is caught to record data such as location, temperature, and humidity. This data is recorded in the ledger, along with further events in the processing of the fish: ownership changes, storage temperature range, transport company, and so on. The ledger can also provide analytics for both regulatory enforcement and scientific analysis of fish harvesting and consumption.

This prototype highlights the benefits of Hyperledger Sawtooth as a platform for tracing assets. The lightweight, highly decentralized consensus protocol in Sawtooth (proof of elapsed time or PoET) is particularly well-suited to a diverse, distributed ecosystem where thousands of validating nodes may be required. Broad participation in the ledger reflects the cross-industry nature of the seafood supply chain.

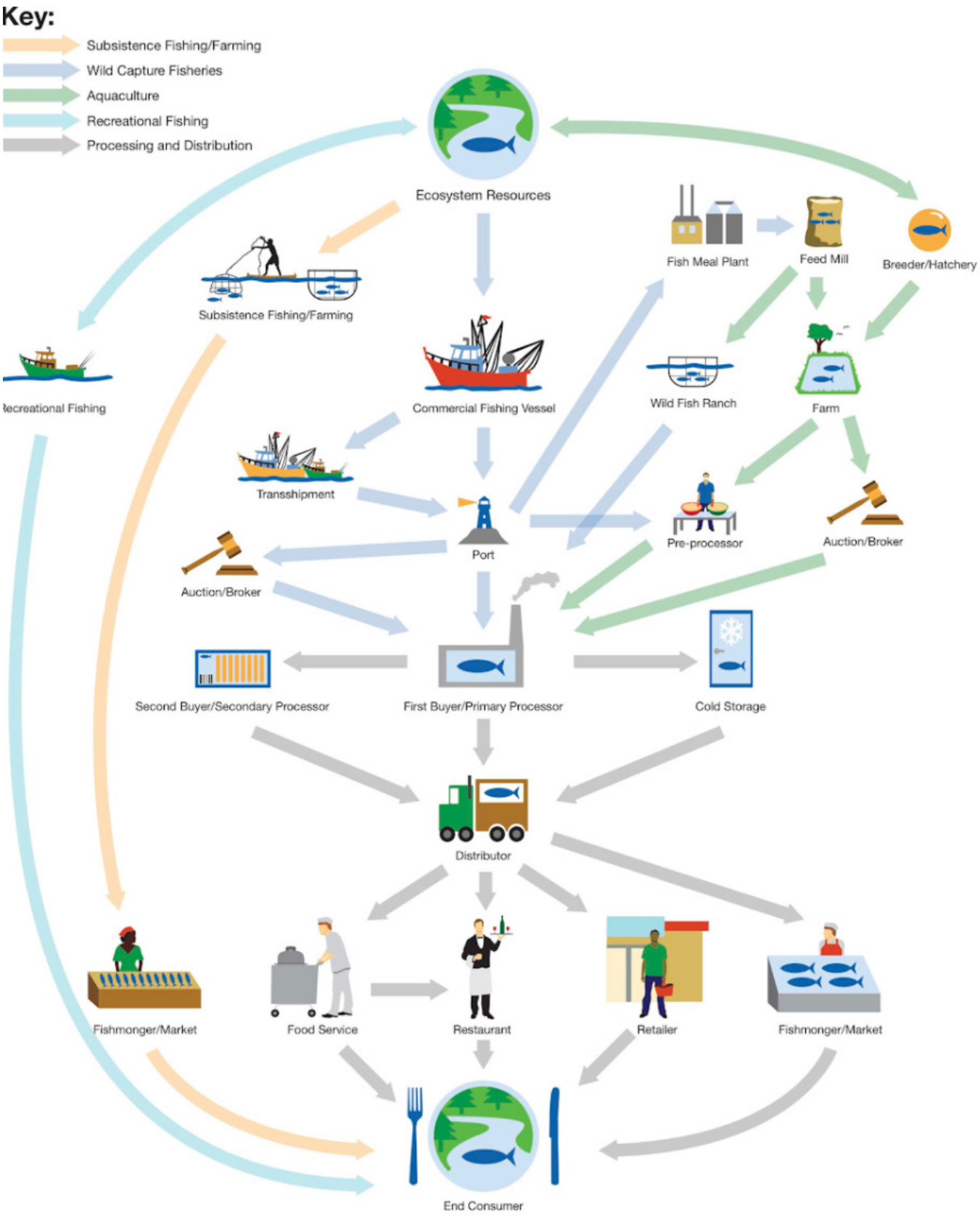

FIGURE 6: THE COMPLEXITY OF THE SEAFOOD SUPPLY CHAIN

Source: Advancing Traceability in the Seafood Industry, FishWise

ASSET TRACKING TOUCHES ON DIFFERENT ISSUES

Asset tracking touches on several issues not generally seen in ledgers for financial products For example, asset tracking requires handling diverse data types, such as the composite format required for telemetry and environmental sensing.

Sawtooth accommodates both domain-specific data and the transaction families that operate on it, including data constraints such as verifying the calibration of a sensor.

Blockchain promises a number of benefits for cross-industry traceability. Most of all, these technologies can help establish a community of participants and an authoritative record of provenance. The blockchain's decentralized fault-tolerance enables updates from a wide range of nodes, including fishing boats, trucks, cold-storage facilities, retail stores, and restaurants.

Beyond traceability, digitizing assets opens the door for completely new markets such as, for example, monetization of provenance.

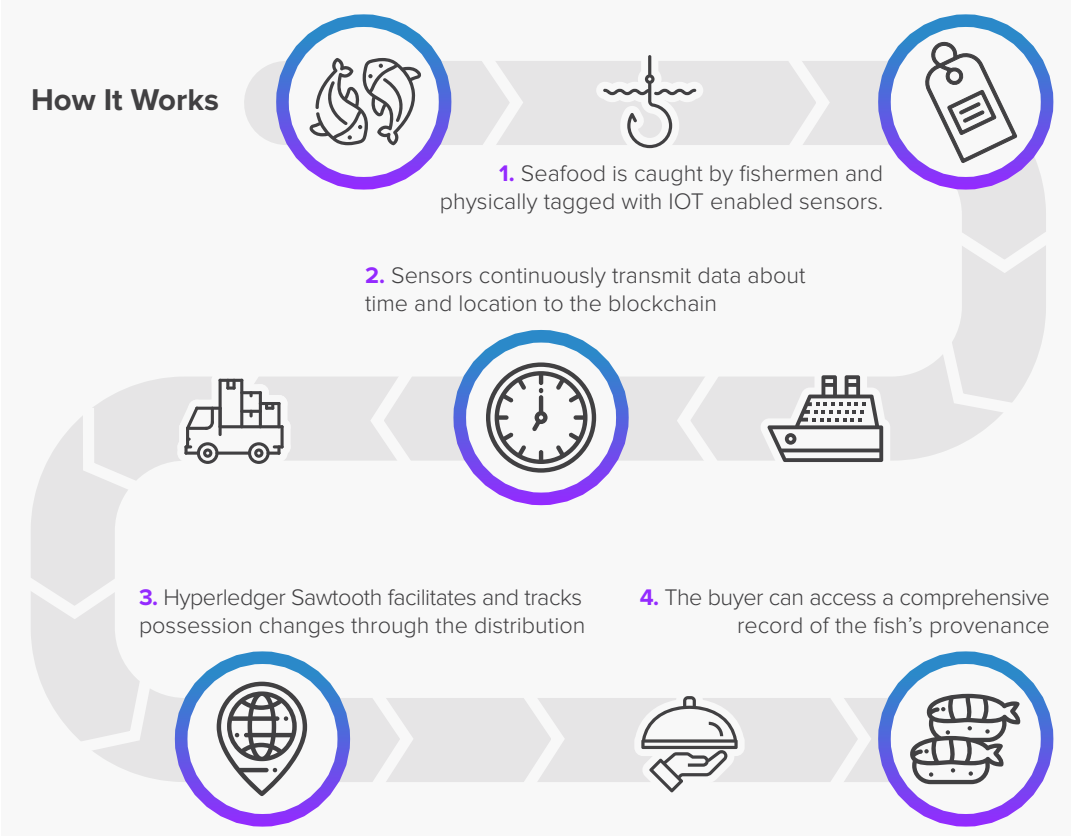

FIGURE 7: OCEAN TO TABLE FLOWCHART USING HYPERLEDGER SAWTOOTH

6 Current Projects: Frameworks

Hyperledger incubates and promotes a range of business blockchain technologies, including:

- Distributed ledger frameworks
- Smart contract engines
- Client libraries
- Graphical interfaces
- Utility libraries
- Sample applications

The Hyperledger strategy encourages the re-use of common building blocks, enables rapid innovation of components, and promotes interoperability between projects.

Table 1 sums up all the current distributed ledger frameworks in alphabetical order. The rest of this section sums up each framework briefly, and shows where to find more information.

Section 7 describes the current Hyperledger tools and utilities.

Table 1: Summary of Hyperledger Frameworks

HYPERLEDGER BURROW	A modular blockchain client with a permissioned smart contract interpreter developed in part to the specifications of the Ethereum Virtual Machine (EVM).	Covered in **Section 6.1**
HYPERLEDGER FABRIC	A platform for building distributed ledger solutions with a modular architecture that delivers a high degree of confidentiality, flexibility, resiliency, and scalability. This enables solutions developed with Fabric to be adapted for any industry.	Covered in **Section 6.2**
HYPERLEDGER INDY	A distributed ledger that provides tools, libraries, and reusable components purpose-built for decentralized identity.	Covered in **Section 6.3**
HYPERLEDGER IROHA	A blockchain framework designed to be simple and easy to incorporate into enterprise infrastructure projects.	Covered in **Section 6.4**
HYPERLEDGER SAWTOOTH	A modular platform for building, deploying, and running distributed ledgers. Sawtooth features a new type of consensus, proof of elapsed time (PoET) which consumes far fewer resources than proof of work (PoW).	Covered in **Section 6.5**

6.1 Hyperledger Burrow

Hyperledger Burrow provides a modular blockchain client with a permissioned smart contract interpreter developed partly to the specifications of the Ethereum Virtual Machine (EVM). In short, Burrow is a permissionable smart contract machine.

Burrow became the fourth distributed ledger platform within Hyperledger in April, 2017. It was originally developed and proposed to Hyperledger by Monax.

Burrow provides a strongly deterministic, smart contract-focused blockchain design. Burrow users benefit from an access control layer through the use of smart contracts and Äúsecure natives-based permission layer.

Burrow includes all the following components:

- **Consensus engine**—Maintains the networking stack between nodes and ordering transactions to be used by the application engine.
- **Application Blockchain Interface (ABCI)**—Provides the interface specification for the consensus engine and application engine to connect.
- **Smart contract application engine**—Provides developers with a strongly deterministic smart contract engine for operating complex industrial processes.
- **Gateway**—Provides programmatic interfaces for system integrations and user interfaces.

To find out more about Hyperledger Burrow, see **hyperledger.org/projects/hyperledger-burrow**.

6.2 Hyperledger Fabric

Hyperledger Fabric is a platform for building distributed ledger solutions, with a modular architecture that delivers high degrees of confidentiality, flexibility, resiliency, and scalability. This enables solutions developed with Fabric to be adapted for any industry.

Fabric allows components, such as consensus and membership services, to be plug-and-play. It leverages container technology to host smart contracts called "chaincode" that contain the business rules of the system. And it's designed to support various pluggable components, and to accommodate the complexity that exists across the entire economy.

Starting from the premise that there are no "one-size-fits-all'' solutions, Fabric is an extensible blockchain platform for running distributed applications. It supports various consensus protocols, so it can be tailored to different use cases and trust models.

Fabric runs distributed applications written in general-purpose programming languages without depending on any native cryptocurrency.

This stands in sharp contrast to most other blockchain platforms for running smart contracts, which either require code to be written in a domain-specific language or else rely on a cryptocurrency.

Furthermore, Fabric uses a portable notion of membership for the permissioned model, which can be integrated with industry-standard identity management. To support such flexibility, Fabric takes a novel architectural approach and revamps the way blockchains cope with non-determinism, resource exhaustion, and performance attacks.

Fabric also can also create channels, which enable a group of participants to create a separate ledger of transactions. This is especially important for networks where some participants might be competitors who don't want every transaction—such as a special price offered to some but not all—known to every participant in the network. If a group of participants form a channel, only those participants and no others have copies of the ledger for that channel.

To find out more about Hyperledger Fabric, see **hyperledger.org/projects/fabric**.

6.3 Hyperledger Indy

Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. Indy provides tools, libraries, and reusable components for creating and using independent digital identities rooted on blockchains or other distributed ledgers.

These identities are interoperable across administrative domains, applications, and any other organizational silo. That means friends, competitors, and even antagonists can all rely on a shared source of truth.

Indy answers fundamental questions such as, "Who am I dealing with?" and "How can I verify any data about the other party in this interaction?" Solid answers to these questions enable the trusted interactions that enterprises need.

KEY FEATURES OF INDY

- **Self-sovereignity**—Indy stores identity artifacts on a ledger with distributed ownership. These artifacts can include public keys, proofs of existence, cryptographic accumulators that enable revocation, and so on. No one but the true owner can change or remove an identity.
- **Privacy**—By default, Indy preserves privacy, since every identity owner can operate without creating any correlation risk or breadcrumbs.
- **Verifiable claims**—Identity claims can resemble familiar credentials such as birth certificates, driver's licenses, passports, and so on. But these can be combined and transformed in powerful ways, using zero-knowledge proofs to enable selective disclosure of only the data required by any particular context.

MANY POWERFUL BENEFITS

This combination of self-sovereignty, privacy, and verifiable claims is extremely powerful. Consider the many potential benefits.

Bulk troves of sensitive data can vanish or become useless. The economics of hacking can be transformed, since less personally identifiable information (PII) is held by each business partner. The competing demands of preserving privacy and meeting regulations can be satisfied. Individuals and organizations can benefit from richer and more secure interactions. And the identity ecosystem can gain the innovation and dynamism of a free market.

Despite the advanced cryptography under the hood, Indy's API is simple and straightforward. This API includes about 50 C-callable functions, with idiomatic wrappers for many mainstream programming languages.

To find out more about Hyperledger Indy, see **hyperledger.org/projects/hyperledger-indy**.

6.4 Hyperledger Iroha

Hyperledger Iroha is a blockchain framework designed to be simple and easy to incorporate into infrastructure projects that require distributed ledger technology.

Iroha joined Fabric and Sawtooth to become the third distributed ledger platform under Hyperledger in October, 2016. It was originally developed by Soramitsu in Japan and was proposed to Hyperledger by Soramitsu, Hitachi, NTT Data, and Colu.

KEY FEATURES OF IROHA:

- A simple structure
- Modern, domain-driven C++ design
- Emphasis on mobile application development
- A new, chain-based Byzantine Fault-Tolerant consensus algorithm, called Sumeragi

Iroha takes a different approach from Fabric and Sawtooth by providing features that are helpful for creating applications for end users.

To find out more about Hyperledger Iroha, see **hyperledger.org/projects/iroha**.

6.5 Hyperledger Sawtooth

Hyperledger Sawtooth is a modular platform for building, deploying, and running distributed ledgers. Distributed ledgers provide a digital record (such as asset ownership) that is maintained without a central authority or implementation. Sawtooth aims to keep distributed ledgers distributed and to make smart contracts safe for enterprise use. In fitting with this enterprise focus, Sawtooth is highly modular. This enables enterprises and consortiums to make decisions about their blockchain applications for themselves.

TECHNICAL INNOVATIONS IN SAWTOOTH

Sawtooth contains several technical innovations, including:

- **Dynamic consensus**—Going beyond compile-time pluggable consensus, this allows a consortium to change consensus algorithms on a running blockchain simply by issuing a transaction.

- **Proof of elapsed time (PoET)**—A consensus algorithm with the scalability of proof of work but without the drawback of high power consumption.
- **Transaction families**—A smart contract abstraction that enables users to write smart contract logic in the language of their choosing.
- **Compatability with Ethereum contracts**—Transaction families can also integrate other smart contract interpreters including Hyperledger Burrow's Ethereum Virtual Machine. Sawtooth features like permissioning and un-pluggable consensus enable Ethereum to be configured appropriately for an enterprise.
- **Parallel transaction execution**—Most blockchains require transactions to be executed in series to guarantee consistent ordering at each peer. Sawtooth includes an advanced parallel scheduler that splits blocks into parallel flows. Parallelism allows for faster block processing to partially address the performance drawback of blockchains compared to traditional databases.
- **Private transactions**—Clusters of Sawtooth nodes can be easily deployed with separate permissioning. This provides privacy and confidentiality among participants of that distinct chain. No centralized service leak transaction patterns or other confidential information. However, an intermediary such as **Hyperledger Quilt** is required to connect separate chains. In the future, Sawtooth plans to provide additional privacy and confidentiality features on top of trusted execution environments and/or zero knowledge primitives.

SAWTOOTH EXTENDS EARLIER DISTRIBUTED LEDGERS

Originally, Sawtooth was designed to explore scalability, security, and privacy questions prompted by the earliest distributed ledgers. That required a modular design that was lacking at the time. Starting from scratch enabled the project to draw lessons from those pioneering systems, and then extend into further use cases that the original currency ledgers weren't intended to address.

The consensus model PoET boosts scalability. Transaction families broaden the scope of smart contracts, while narrowing the potential attack surface. The Sawtooth designers are also exploring trusted execution environments and the role those can play in private transactions.

SAWTOOTH FOR ENTERPRISES

Even when branching into new business cases, certain key features of a distributed ledger must be preserved. In an enterprise deployment, the distributed ledger must not devolve into nothing more than a replicated database.

Enterprise participants need autonomy and have the right to run their own nodes. This interaction, with each member operating nodes in their own self-interest, provides the integrity of a blockchain.

To realize that integrity, blockchains must meet three challenging requirements:

1. Provide security against malicious actors inside the network
2. Manage a large population
3. Manage a dynamic population

Many consensus algorithms used in conventional replicated databases are not designed to handle these blockchain requirements.

Sawtooth and PoET are designed for truly decentralized blockchain applications; that is, applications where there are many participants in the consensus process that are administratively and physically distributed.

PoET provides security against bad actors and is designed to manage the arrival and departure of nodes in a large network.

Furthermore, Sawtooth provides on-chain governance to upgrade the consensus and other business rules the consortium agrees to over the life of the network. This means that a consortium can change consensus on-the-fly using transactions only.

Users can even start with a constrained consensus and then change to a consensus like PoET that affords the secure, dynamic, and scalable characteristics required by a production network.

To find out more about Hyperledger Sawtooth, visit **hyperledger.org/projects/sawtooth**.

7 Current Projects: Tools

Hyperledger incubates and promotes a range of business blockchain technologies, including tools and utility libraries.

The Hyperledger strategy encourages the re-use of common building blocks, enables rapid innovation of components, and promotes interoperability between projects.

Table 2 sums up all the current Hyperledger blockchain tools in alphabetical order.

The rest of this section sums up each tool briefly, and shows where to find more information.

Table 2: Summary of Hyperledger Tools

HYPERLEDGER CALIPER	A blockchain benchmark tool that measures the performance of any blockchain by using a set of predefined use cases.	Covered in **Section 7.1**
HYPERLEDGER CELLO	A set of tools to bring the on-demand deployment model to the blockchain ecosystem with automated ways to provision and manage blockchain operations that reduce effort.	Covered in **Section 7.2**
HYPERLEDGER COMPOSER	An open development toolset and framework to make developing blockchain applications easier.	Covered in **Section 7.3**
HYPERLEDGER EXPLORER	A dashboard for viewing information on the network, including blocks, node logs, statistics, smart contracts, and transactions.	Covered in **Section 7.4**
HYPERLEDGER QUILT	A set of tools that offer interoperability by implementing ILP, which is primarily a payments protocol designed to transfer value across distributed and non-distributed ledgers.	Covered in **Section 7.5**

7.1 Hyperledger Caliper

Hyperledger Caliper is a blockchain benchmark tool that measures the performance of any blockchain implementation by using a set of predefined use cases.

Caliper produces reports that show a number of performance indicators, such as:

- Resource utilization
- Transaction latency
- Transactions Per Second (TPS)
- Others to be defined

Until Caliper, there has not been any general tool that provides performance evaluations for different blockchain solutions, based on a set of neutral and commonly accepted rules.

Caliper will not publish benchmark results. The idea is to use Caliper as an in-house reference to help choose the blockchain implementation best-suited for a company's specific needs.

Hyperledger Caliper provides a functioning benchmark tool that can run against many Hyperledger frameworks. The community will continue to define further performance indicators and benchmark use cases. The success of the project will depend on many community members using it as the benchmark tool.

To see more about Hyperledger Caliper, see **hyperledger.org/projects/caliper**.

7.2 Hyperledger Cello

Hyperledger Cello is a blockchain module toolkit that aims to bring the on-demand deployment model to the blockchain ecosystem. The goal is to help enterprises quickly and easily adopt blockchain technologies, by providing automated ways to create, manage, and terminate blockchains.

Cello provides an efficient and automated multi-tenant chain service on top of various infrastructures, including bare metal, virtual machines, cloud platforms like Amazon Web Services (AWS), and container platforms like Docker Swarm and Kubernetes. All in all, this helps boost the efficiency of "Blockchain as a Service (BaaS)."

Cello also provides a real-time dashboard where users can:

- View the status of the blockchain system
- See statistics such as blockchain events, chaincode performance, and system utilization
- Manage blockchains by creating, configuring, and deleting them
- Manage chaincode by deploying and uploading private chaincode

Hyperledger Cello currently supports **Hyperledger Fabric** as the main blockchain implementation. The project plans to support **Hyperledger Sawtooth** and other types of blockchains.

The architecture follows the micro-service style, with pluggable implementations for most components. The main programming languages used are Python and JavaScript.

To find out more about Cello, see **hyperledger.org/projects/cello**.

7.3 Hyperledger Composer

Hyperledger Composer is an open development toolset to make it simple and fast to create smart contracts and blockchain applications to solve business problems. The main goal is to make it easier to integrate blockchain applications with existing business systems, and thus accelerate time-to-value.

Composer can help develop use cases and deploy a blockchain solution in weeks, rather than months.

Composer also enables users to quickly model an existing business network, and integrate existing systems and data with blockchain applications. A network can contain assets—such as tangible or intangible goods, services, or property—and transactions related to them. As part of the model, users can define how transactions can interact with assets.

Business networks include the participants who interact with them. And each participant can be associated with a unique identity across several different business networks.

Hyperledger Composer supports the existing **Hyperledger Fabric** blockchain infrastructure and runtime. Since Fabric supports pluggable consensus protocols, this ensures that transactions can be validated according to the appropriate policy of the network participants.

To find out more about Hyperledger Composer, see **hyperledger.org/projects/composer**.

7.4 Hyperledger Explorer

Hyperledger Explorer provides a dashboard for viewing information about blocks, node logs, statistics, smart contracts, transactions, and any other information stored in the blockchain. Users can query for specific blocks or transactions to view the complete details.

Explorer can be integrated with any authentication or authorization platforms, either commercial or open source, to provide the functions appropriate to a user's privileges.

The goals of the Explorer project include:

- To create a generic web-based blockchain explorer that's easy to install and use with different blockchain platforms
- To use the latest tools and technologies to make Explorer easy to implement, maintain, and extend
- To support the standard package managers on most popular platforms to ensure the Explorer is quick and easy to install

Hyperledger Explorer currently supports the **Hyperledger Fabric** framework.

To find out more about Hyperledger Explorer, see **hyperledger.org/projects/explorer**.

7.5 Hyperledger Quilt

Hyperledger Quilt offers interoperability between ledger systems by implementing the Interledger Protocol (ILP) in Java. ILP is a simple, open source protocol that establishes a global namespace for accounts to help make transactions across ledgers.

MORE ABOUT THE ILP

Payment networks today are siloed and disconnected. While payments are relatively easy within one country, or if both the sender and recipient have accounts on the same network or ledger, sending from one system or ledger to another is often impossible. Where connections do exist, they are manual, slow, or expensive.

The ILP is based on concepts dating back to the 1970s. It took the advent of Bitcoin and the global blockchain movement to make the world realize that money and value transfers could be reinvented with Internet-based technologies. With ILP, money and other forms of value can be packetized, routed, and delivered over payment networks and ledgers.

ILP is a payments protocol designed to transfer value across both distributed and non-distributed ledgers. This provides for routing payments across different digital asset ledgers, while isolating senders and receivers from the risk of intermediary failures. Secure multi-hop payments and automatic routing enable a global network of networks for different types of value that can connect any sender with any receiver.

AN INTEROPERABILITY SOLUTION

Hyperledger Quilt is an enterprise-grade implementation of the ILP protocol, developed in Java. Quilt provides libraries and reference implementations of the core Interledger components.

The idea is that Quilt will become a ledger interoperability solution for Hyperledger projects. This will enable the distributed ledger solutions from Hyperledger members, the private ledgers from financial institutions, the wallets from IoT companies, and supply chain systems to connect with one another to perform distributed atomic transactions.

By implementing the ILP, Quilt provides:

- A set of rules for enabling ledger interoperability with basic escrow semantics
- A standard for a ledger-independent address format and data packet
- A framework for designing higher-level protocols for specific use cases

To find out more about ILP, visit **interledger.org/rfcs/0003-interledger-protocol/**.

To see more about Hyperledger Quilt, visit **hyperledger.org/projects/quilt**.

8 Long-Term Vision

We live in a highly interconnected world. In the future, the world will no doubt become even more closely tied together. In both our business and personal lives, more data, more digital content, more communication, and more sharing will be the norm. All this will require careful management of our security, privacy, and trust.

A common problem, and a sensible solution

We expect to see a common problem: Many people will want to share data in a distributed database, but no single owner will be trusted by every user.

The solution is distributed ledger technology (DLT). As data sharing increases, we expect blockchain technology and DLT to become more and more common.

But reaching widespread use of distributed ledgers will not be simple. For instance, gaining security and privacy with a blockchain often means sacrificing performance. This suggests that we'll need a variety of different blockchains that can all communicate and interact seamlessly. No one blockchain will work best for all applications.

The long-term vision for Hyperledger is driven by two main concerns: that the architecture must be modular and interoperable.

Interchangeable modules

We hope that eventually Hyperledger consists of many modules that can be assembled into a cohesive, functional, and secure distributed ledger. All these modules will ideally be interchangeable with other modules of the same type. All these modules will ideally be able to communicate with other modules of the same or different types. And ideally, even a non-expert will be able to use them to set up a secure, interoperable blockchain quickly, easily, and efficiently.

Many blockchains that work together

We want to specifically point out that we do not believe any Hyperledger blockchain should be the "one distributed ledger to rule them all.'' The Hyperledger community sees merit in many different blockchains. We hope that other developers consider interoperability with Hyperledger projects.

Not a single stack, but a collection of tools

The goal for Hyperledger is not to become a single software stack. Instead, we want to create a collection of tools built with modularity and interoperability in mind. Then, any individual can use one, some, or all of the Hyperledger projects to create a distributed ledger to suit their needs.

In the future, we hope that Hyperledger can solve most of the common problems in the distributed ledger space. This will require a good community of developers, strong support from business and industry, and solid design principles. As shown in this paper, we have structured Hyperledger with all these in mind.

9 Conclusions

In this paper, we explained the rationale behind the creation of Hyperledger and our goals for the project. We outlined why we think an open source greenhouse structure seems to be the optimal governing arrangement for a general blockchain consortium. We showcased some of the many use cases that inspired our members to join and work on Hyperledger. We described some of the features required to build effective blockchains for some of these use cases. And we briefly summed up all the Hyperledger projects and where they stand at publication date.

We hope reading this paper is just the beginning of the Hyperledger experience for you.

We know there's a lot of work left to be done. We realize that Hyperledger will probably always be a work-in-progress. But—perhaps with your help—we can all work together to build secure, efficient, and reliable blockchain solutions that make a difference to everyone's future.

Introductory sources on blockchain

Blockchain Basics: Glossary and use cases. IBM developer-Works. Updated August 21, 2017. A solid explanation of blockchain terms aimed at developers new to the space.

Blockchain Basics: A Non-Technical Introduction in 25 Steps. Daniel Drescher. Apress. March 2017. Explains blockchain concepts with analogies, metaphors, and pictures, not mathematical formulas or program code.

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Don Tapscott and Alan Tapscott. Portfolio—Penguin. May 2016. Less about the technology and more about the implications of blockchain for business. The authors also have basic videos available on YouTube.

Blockchain Technology Overview. National Institute of Standards and Technology, U.S. Department of Commerce. January 2018. One of the best introductions to blockchain we have seen, written in plain English while maintaining nuances. Includes glossary of terms and acronyms.

Further resources from Hyperledger

We encourage you to use the Hyperledger resources to find more information on any blockchain-related topics you find interesting. Here are some further resources to get you started.

The Hyperledger Vision is a slide deck that sums up some blockchain 101-type information and the founding vision for Hyperledger, available at **hyperledger.org/resources/publications**.

The Hyperledger Wiki contains a wealth of technical information, available at **wiki.hyperledger.org/start**.

You can find further information on each of the current Hyperledger frameworks at these links:

- **Burrow**—**hyperledger.org/projects/hyperledger-burrow**
- **Fabric**—**hyperledger.org/projects/fabric**
- **Iroha**—**hyperledger.org/projects/iroha**
- **Indy**—**hyperledger.org/projects/hyperledger-indy**
- **Sawtooth**—**hyperledger.org/projects/sawtooth**

You can find further information on each of the current Hyperledger tools at these links:

- **Caliper**—**hyperledger.org/projects/caliper**
- **Cello**—**hyperledger.org/projects/cello**
- **Composer**—**hyperledger.org/projects/composer**

- **Explorer**—**hyperledger.org/projects/explorer**
- **Quilt**—**hyperledger.org/projects/quilt**

The Hyperledger Working Groups have many great technical resources, and are open to anyone with an interest in their subjects. For example, the Architecture Working Group has substantial documentation on the fundamentals of permissioned blockchain. If you're looking to explore technical details, that group is a great resource.

The application-specific working groups are also great places to learn. For instance, the Identity Working Group has spent a lot of time discussing and documenting how blockchain can enable identity solutions.

Notes

1. Don Tapscott and Alan Tapscott. ***Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.*** Portfolio-Penguin. 2016. p9
2. 2017 State of Linux Kernel Development. **linuxfoundation.org/2017-linux-kernel-report-landing-page/**
3. April 2018 Web Server Survey. Netcraft. **news.netcraft.com/archives/2018/04/26/april-2018-web-server-survey.html**
4. The 10th Annual Future of Open Source Survey. North Bridge and Black Duck Software. 2016. **blackducksoftware.com/2016-future-of-open-source**
5. Note that the counterparty risk arising between concluding and settling a trade, typically two or three days, can be reduced if the counterparties have agreed on bilateral margining or if the transactions are cleared through a clearing house.
6. The usefulness of blockchain for post-trade settlement may be limited, since near real-time settlement may eliminate the netting benefits (position offsetting) of end-of-day processing.
7. Food and Agriculture Organization, United Nations. 2016. ***The State of World Fisheries and Aquaculture 2016.*** **fao.org/3/a-i5555e.pdf**
8. ***Stolen Seafood: The Impact of Pirate Fishing on Our Oceans.*** Oceana. 2013. **oceana.org/sites/default/files/reports/Oceana_StolenSeafood.pdf**
9. Miguel Ángel Pardo, Elisa Jiménez, Begoña Pérez-Villarreal. ***Misdescription incidents in seafood sector.*** 2016. Food Control 62 pages 277–283.
10. Oceana Study Reveals Seafood Fraud Nationwide. 2013. **oceana.org/sites/default/files/reports/National_Seafood_Fraud_Testing_Results_FINAL.pdf**
11. FishWise. 2017. ***Advancing Traceability in the Seafood Industry: Assessing Challenges and Opportunities.*** **https://fishwise.org/wp-content/uploads/2018/04/2018.02.22_Trace-WP_February-2018-Update-1.pdf**
12. Oceana. 2014 Annual Report. **oceana.org/sites/default/files/2014_annual_report.pdf**