An Introduction to Hyperledger

Hyperledger Whitepaper Working Group

Abstract

The Hyperledger Project is a Linux Foundation sponsored initiative with the goal of building secure enterprise blockchain implementations. Hyperledger does not have a single blockchain codebase or a single blockchain project, but rather functions as an organization where projects that are accepted by the community can collaborate and share ideas, infrastructure, and even code. In this paper we explain the reasons behind the existence of Hyperledger and some of the governance choices we made and the design philosophy we bring to projects. We list some of the use cases and features that motivated our members to participate in Hyperledger. Additionally we outline the current state of Hyperledger in terms of the projects and development efforts that are currently ongoing, and provide directions for those looking to learn more about Hyperledger. This paper is not intended as a technical whitepaper but rather as an introduction to Hyperledger. However, we provide appropriate references for those interested in the technical details of various aspects of Hyperledger.

1 Introduction

Databases and database technology have played an important part in both business and society for decades. Databases began as simple, monolithic servers. As the need for more powerful functionalities grew, things like relational databases and query languages (i.e. SQL) were invented to deal with the growing need for improved efficiency and ease of use. As the world became more connected and global, distributed databases emerged, and things like consensus algorithms and fault tolerance became popular topics in both academia and business.

Now, the world has become so interconnected that many different people and entities need to be able to use the same database(s). Traditional distributed databases typically assumed that all users were honest, and errors were the result of poor network conditions or other faults that were not due to adversarial behavior. In today's world, however, people who have competitive or even adversarial relationships with one another, even within the same entity, may need to access or edit the same information in the same database. To solve this problem, distributed ledger technology and blockchain technology were developed. The basic idea is fairly simple: with clever applications of cryptography and distributed systems concepts to traditional databases, many more useful applications can be constructed in ways that do not require a central trusted authority or reduce the trust requirements on the participants. With this in mind, we can view both blockchain and distributed ledger technology as the emerging field at the intersection of databases, cryptography and distributed systems.

Historically, databases have focused on single party applications purely out of necessity. Since distributed databases allow for multiparty, shared database use, distributed ledgers can be equipped

with multi-party business logic, which is more commonly referred to as 'smart contracts. This allows distributed ledgers to be used for substantially more applications than traditional databases.

While there are many definitions of the terms *blockchain* and *distributed ledger*, we will define them here for clarity. For the purposes of this paper, we refer to a *blockchain* as a shared, append-only log of transactions (nothing can ever be erased or edited–only appends are allowed). We define a *distributed ledger* as a multi-party, distributed database where there is no central trusted authority. When transactions are processed in blocks according to the ordering of a blockchain, the result is a distributed ledger. In spite of our desire to clarify these terms, we will bow to popular press and use these terms interchangeably.

Hyperledger builds on this rich technology background to bring blockchain-based distributed ledgers into a broad class of enterprise usages. Broadly speaking, Hyperledger is an 'umbrella for open source distributed ledger platforms and related components and modules. The community of developers who participate in Hyperledger coordinate cross-industry, open source software development for projects that meet the diverse needs of those building and deploying distributed ledgers.

The most popular existing blockchains like Bitcoin [Nak08] and Ethereum [But13] utilize completely trustless networks. But most enterprise applications rely upon real world trust relationships that Hyperledger projects can leverage to gain efficiency, functionality, or both.

While supporting diversity of blockchain and distributed ledger technologies (necessary to meet the unique needs of enterprise applications) the consortium structure of Hyperledger also provides a means of bringing coordination from the chaos: identifying common components, avoiding duplication of effort, promoting interoperability and portability, and providing a diverse community for feedback.

In the remaining sections of the paper, we will explain what Hyperledger is and many of the design decisions and principles of the effort.

1.1 Outline

OUTLINE

2 Why Open Source

The concept of trust is indelibly woven into the very essence of blockchain technologies. It must be for the reason discussed above - blockchain technologies are used to enable direct, peer-to-peer transactions between parties that dont fully trust one another or have a trusted central authority. Consequently, trust in the blockchain technologies themselves is an essential prerequisite to their adoption.

We believe that an open source, collaborative approach that invites participation from all stakeholders is the most effective way to produce the necessary degree of trust in blockchain technologies for businesses to broadly and rapidly adopt them. The transparency of open source development facilitates audit and review from a diverse community of experts. This practice of open development and review is standard within the security and cryptography communities to ensure correctness of concept and implementation.

An effective open source project must have an open governance model, an open development model and an open review model. Hyperledger fully embraces the transparency and openness

common to Linux Foundation Projects, which provides the legal, governance, technical, logistical and promotional structure that all software initiatives need. Anyone can download the codebase and start contributing, and the positions of authority are determined in an open and democratic manner.

The open source structure has been the driving force of the growing number of distinct software projects, contributors, meet-up groups, hackfests, and corporate members, all under the Hyperledger umbrella. Companies deploying blockchain internally, and those building products and services based on Hyperledger projects tell us that their trust and confidence comes from knowing that Hyperledger technologies are built in the open, with and by an extremely broad consortium of users and vendors regularly reviewing and checking the code to ensure that it is of the highest standard.

The open source nature of Hyperledger technologies also ensures no surprises when it comes to integration and interoperability between various blockchains - something we believe will be very common in the poly-chain future we expect. We expect that achieving needed interaction across proprietary chains would otherwise be much more difficult. In addition to interoperability between different chains, the open source nature of Hyperledger will enable more application portability between various blockchain implementations, hopefully leading to easier application creation for developers.

Economics is also powerfully on the side of a collaborative development effort like Hyperledger. Businesses as diverse as banks, car and plane makers, healthcare companies and a broad ecosystem of vendors, all need robust, feature-rich, modular blockchain platforms that they can tailor to meet their exact needs. When all these different users and vendors collaborate to co-create common platform technologies, the investment required from each is a fraction of what it would be if each created their own.

3 The Umbrella Organization

While blockchain is a powerful piece of technology, it is not a one-size-fits-all solution. Modifications and special features are needed in order for it to operate at an optimal level, or even operate at all for its intended purpose. Customized functionality and features are essential to making blockchain technology the appropriate solution for the organization that uses it. Since organizations have varying needs, it can be assumed that there will be multiple blockchains customized with different features for a wide-range of solutions instead of a single standard blockchain.

Because of this development of multiple systems, collaboration plays a larger role in order to help reduce the overall resources consumed with these efforts. For example, navigating through various developments in an open source environment can be daunting and subsequently cause organizations to forego keeping up with the changes or starting at all due to significant costs. Hyperledger fills this organizational need and makes the coordination process more effective by creating a collaborative environment that streamlines project development and communication. With this environment, keeping up with the various developments in the blockchain industry is simplified. This also makes it easier for newer participants that join the umbrella organization to catch up with the latest developments as information is properly structured to ensure that new participants have an easy way of joining the collaborative effort.

The umbrella organization structure also allows for specialization among the participants. Specialization has historically proven to be a driving factor in global economic development and the same benefits can be realized with participants specializing in various areas of the technology.

Outside an umbrella organization, such would still be possible in an open source environment, but would be much more difficult. As communication and collaboration is streamlined, implementation of these developments and access to necessary information can be done with ease across various projects for the benefit of the entire ecosystem. However, unlike most cases, participants that specialize in similar areas wont be competing against each other. With an umbrella organization, joint research efforts are not only possible, but also encouraged in order to prevent duplicate efforts, which have a stronger negative effect in a relatively new industry where the development pool is not yet deep..

The umbrella organization facilitates more collaboration between industry participants than would otherwise occur. This can streamline the development of newer projects and avoid duplicative efforts by allowing for the creation of common components that benefit the entire community. Interoperability between ledgers, similar or not, also becomes much more of a possibility, not just because of a better understanding of the other ledger projects, but also because of the collaborative environment. The governing structure provided by Hyperledger also helps solve potential interoperability disputes that may arise.

The structure enforces quality control by having a technical governing committee review all projects throughout their life cycles. For new projects, this provides a chance to be critiqued and gain knowledge from members of all existing projects. Cross-project exposure increases the likelihood of collaboration, which can potentially mitigate duplicated efforts. Additionally, existing project members may discover innovations and developments introduced by the new projects, and implement them in their own projects. This structure also fosters potential interoperability between new and old projects.

Consistency of licenses and handling of intellectual property is another value provided by the umbrella organization. In particular, Hyperledger operates under an Apache 2.0 license for code and Creative Commons Attribution 4.0 International license for content. These licenses are known to be particularly enterprise friendly. A single, consistent approach to intellectual property removes the need for expensive and complex development relationships amongst the members. Expectations for participants are clearly communicated and those building and using Hyperledger technologies can participate without fear of hidden legal encumbrances.

4 Design Philosophy

At Hyperledger, all projects follow a design philosophy that includes a modular extensible approach, interoperability, emphasis on highly secure solutions, a token agnostic approach with no native cryptocurrency and the development of a rich and easy-to-use Application Program Interface (API).

Distributed ledgers for different use cases can have vastly different requirements. For instance, in use cases where participants have high trust between one another, such as many financial applications, blockchains can use rapid network consensus systems and short block confirmation times before being added to the chain. However, other applications where there is minimal trust between participants may tolerate slower processing times.

Hyperledger embraces the full spectrum of these uses cases, especially enterprise scenarios with widely varied requirements for decentralization, trust, continuity, confirmation times, etc. Each represents a potentially unique optimization point for the technology. To address this, Hyperledger is developing modular, extensible frameworks that allow the re-use of common building blocks, while enabling experimentation and evolution with DLT components. This modular approach enables

extensibility and flexibility by defining common functional modules and the interfaces between them. This allows components to be changed independently without affecting the rest of the system. We are in the early stages in the evolution of DLT systems, and by taking a modular approach we will be able to experiment with different approaches to functional components. A modular approach allows us to develop optimal components which may be combined to compose DLT solutions that are best suited to different sets of requirements. Another advantage of the modular approach is that it allows a diverse community of developers to work independently on different modules, and allows the re-use of common modules across multiple projects. We define modules and interfaces for consensus, ledger storage, smart contract, communication, identity and policy and crypto functions[1].

Security is a key consideration for distributed ledgers, as many use cases may involve high value transactions or otherwise sensitive data. Securing a blockchain is quite a difficult task: distributed ledger components must be secure against online, persistent adversaries while still containing a large, feature-rich set of functionalities. The large codebase and open, networked nature of distributed ledgers make them prime targets for attackers.

In Hyperledger we view security and robustness as key aspects of Enterprise class blockchains and DLTs, which will evolve into critical infrastructure for next generation business networks. This includes embracing security by design and following best practices as specified by the Linux Foundations Core Infrastructure Initiative, and ensuring that the algorithms, protocols and crypto are reviewed and audited by security experts.

Interoperability and portability are key aspects for the work done under the Hyperledger umbrella. We envision that there will be many interconnected blockchain networks which will need to communicate and interact with each other to form potentially complicated networks. It is also highly desirable that smart contracts and applications be portable across different instances of blockchain/DLT networks in order to make development easier.

Hyperledger is independent and agnostic of currency and tokens. In Hyperledger we do not require a native token either as a means to provide incentives to operate the network or for resource management.The explicit focus on managing digital objects (which may represent currencies) removes the requirement for intrinsic crypto-currencies and native tokens.

Hyperledger projects will also supports a well defined set of APIs and SDKs that allows external clients and applications to interface with core DLT infrastructure. These APIs will enable a rich developer ecosystem that is needed to be successful in proliferating blockchain and DLT solutions across a diverse set of markets and use cases.

5 Relevant Use Cases

5.1 Applying for a Loan

Financial institutions want to lend, but only if a borrower is a good risk. This motivates them to gather detailed, personally-identifying information (PII) from each applicant. Regulation may demand that certain PII be shared (e.g., to prevent money laundering); on the other hand, holding too much information exposes them to risks from privacy regulation and hacking.

Loans arent fun for the borrower, either. Theyd like to know which financial institution offers the best terms, but the application process is arduous and intrusive, and each new application they submit multiplies the effort and the risk that their data will be abused.

[1]The architecture working group rocks!

The identity solution offered by Hyperledger Indy is transformative here. Applicants can share just the information that the financial institution needs to make a proposal, and they can do it in a way that guarantees truth, builds lender confidence, and satisfies regulatory pressures. They can do this with a hundred different potential lenders at a time, in milliseconds, all without creating correlation risk or placing sensitive personal info in a hackable database with custodians of uncertain reputation. Instead of disclosing their birthdate, annual income, and government ID number to enable a credit score, they can generate zero-knowledge proofs that they are over 21, that their gross income on last years taxes exceeded a certain threshold, that they possess a valid government ID number, and that their credit score exceeded a certain threshold within the past week.

Strong, distributed ledger-based identity establishes a global source of truth in this use case, and this delivers value to many parties. Applicants can give consent, and everyone can agree on when and with what conditions it was given; lenders can demonstrate equal opportunity conformance with an immutable audit trail; the marketplace operates more efficiently.

This use case only gets more compelling when the goodness of other Hyperledger projects is added. Hyperledger Burrow could turn loan applications into contracts, and attach them to strong identities as a seamless next step. A membership system based on Hyperledger Fabric could link to the pre-existing and self-sovereign identity of the application, allowing them to service loans and be a responsible customer of the lender without painful onboarding. And so forth.

5.2 Supply Chain: Tracking Fish from Ocean to Table

Oceanic fishing represents more than $ 100B in economic impact worldwide. In spite of its impact, the industry is fraught with problems. Estimates suggest that nearly 20% of fish are caught illegally. In addition to the environmental impact of illegal fishing, the integrity of the industry is also affected; a recent study based on DNA testing found that nearly $\frac{1}{3}$ of all fish was mislabeled including 87% of snapper and 57% of tuna (95% of all sushi restaurants were found to serve mislabeled fish).

Traceability and provenance are managed in several limited domains such as Maine lobster and Maryland crab. However, the complexity of the ecosystem (see the figure below) and its relatively primitive use of technology limit the impact (see this article for more information on efforts to enable traceability more broadly). Problems identified by FishWise in a 2012 study include:

Many different paths from ocean to table Lake of global authority for tracing Existing proprietary tracing systems unscalable Most existing processes are paper-based

Oceana 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.”

The supply chain through which fish are delivered is extremely complex (see Figure 1) and involves diverse industries and regulatory controls that cross national boundaries. The diversity of participants in the supply chain and the complex relationships between them makes this a perfect opportunity of the use of blockchain technologies. A team at Intel is using the Hyperledger Sawtooth blockchain technology to build a traceability prototype that combines the distributed ledger, IoT sensors, and advanced communication technology to track telemetry parameters such as location, temperature and humidity throughout capture, processing, and transit. Sensors attached to the fish when it is caught record ownership and information about the location of the catch in the ledger. Transactions on the ledger reflect interesting events in the processing of the fish: ownership changes,

Figure 1: Source: `https://www.fishwise.org/images/fishwise_traceability_white_paper_august_2012.pdf`

transportation company, storage temperature range, etc. Further, analytics on the ledger can be used for both regulatory enforcement and for scientific analysis of fish harvesting and consumption.

The prototype highlights the benefits of Hyperledger Sawtooth as a platform for asset traceability. The lightweight, highly decentralized consensus protocol in Sawtooth ("proof of elapsed time") is particularly well suited to the diverse, physically and organizationally distributed ecosystem where potentially thousands of validating nodes are required. Broad participation in the ledger reflects the cross-industry nature of the supply chain. Additionally, asset tracking brings in a number of issues not generally seen in ledgers that focus on financial products. For example, asset tracking requires handling of diverse data types such as the composite format required for telemetry and environmental sensing. Transaction families in Sawtooth accommodate domain-specific data and the transactions that operate on it, including enforcement of data specific constraints (such as verification of the calibration of a sensor)

The use of blockchain technologies provides a number of benefits for cross-industry traceability. Most importantly, blockchain technologies provide a means of establishing a public (to the community of participants) and authoritative record of provenance. Its decentralized nature and resiliency to faults enable updates from fishing boats, trucks, cold storage facilities and restaurants. Beyond traceability, the digitization of assets (fish in this case) opens the doors for completely new markets that might include, for example, monetization of provenance.

5.3 Financial Services: Post Trade Activities

The primary drivers for adoption of blockchain in financial service industry are considerations for privacy, confidentiality, and accountability. Compliance guidelines like Anti Money Laundering and Know Your Customer demand that users/customers are known and have been given clearance by their bank and/or the market infrastructure provider. These requirements drive the adoption of primarily permissioned and private blockchains as public blockchains still carry the risk of compromising participants' confidentiality and privacy. These considerations together with large volumes of transactions are the primary reasons that consortium blockchains are gaining momentum in adoption of distributed ledger technology by the financial services industry.

Among various use cases in financial services, and especially in capital markets, post trade activities is one of the prime areas, which can benefit from adoption of blockchain.

Post trade processing comprises all activities after the completion of a trade transaction. This general description is valid for all types of trading - OTC (over-the-counter)[2] trading as well as trades executed at exchanges.

On a high level post-trade-processing comprises of the following operational steps:

Trade validation - activities taking place following the trade execution, mainly validation and confirmation of the actual transactions amongst the trade participants or through exchange.

Clearing - alignment and matching of the actual trade instructions and confirmations across the different counterparties as well as potential netting activities. In case the counterparties have agreed on bilateral margining or the transactions are cleared through a clearing house, the counterparty/settlement risk arising between the time of concluding the trade and the time of settlement (typically 2 - 3 days) is mitigated.

[2]OTC trading takes place when the trade counterparties interact directly or via brokerage services.

Settlement - the (legal) realization of the actual contractual obligations to reach the finality of the transaction. This includes support processes like the notification of all relevant entities affected by the transaction.

Custody activities - custodians are responsible for the safekeeping of securities. As such the positions held by the trade counterparties have to be adjusted.

Besides these operational steps, post-trade-processing typically contains reporting requirements regarding the business transaction under consideration. Amongst these are counterparty internal risk reporting[3] and regulatory reporting.

The operational steps as well as the reporting activities are in todays setup typically a fragmented process chain spanning across a variety of departments of the respective counterparties, spread across a variety of entities, such as trade counterparties, brokers, settlement agents, central security depositories, clearing houses, thus resulting in a variety of interfaces. This consequently can result in a variety of reconciliation efforts along the process chain, between the trade counterparties as well as other entities/service providers involved, introducing inefficiencies in post trade processing.

Implementing post-trade-processing on blockchain is bound to lead to process efficiency gains as compared to the current implementation model. When settling via a blockchain system one could exploit the peer-to-peer property of a blockchain, i. e. one counterparty would insert the transaction details into the system and the other counterparty would verify and confirm. Thus the confirmation processes would be processed within the same system, rendering separate confirmation processes obsolete.

In todays world both parties would independently send their settlement instructions to a trusted 3rd party - the settlement agent - and this 3rd party would match both data sets and further process the settlement. Any mismatches in the initial instructions would lead to reconciliation efforts or even failed trades. In case of a blockchain solution, the network itself acts as an independent trusted 3rd party due to it's immutability and irrefutability of transactions.

The complexity of the multi-party interactions/interfaces is additionally reduced as all data from all from all process steps and actors resides on the blockchain and is accessible on a need-to-know basis. Therefore, the reconciliation processes should become obsolete altogether. Also the blockchain based system of record could serve as an efficient basis for reporting activities, e. g. regulatory transaction and trade reporting.

These efficiency gains have significant benefit to trade validation, clearing, both risk and regulatory reporting, as well as some aspects of the settlement phases of post trade processing[4].

When looking to apply blockchain to financial services, in addition to the commonly recognized properties of a tamper-proof irrefutable transaction log, a blockchain used for post trace activity would need to have several features, typically achievable with the use of permissioned distributed ledgers.

Distributed ledgers used for capital markets use cases would typically be expected to have immediate finality. Nakamoto-style consensus algorithms (such as proof of work, proof of stake, or proof of elapsed time) may result in temporary forks, leading to transaction rollback, which is not acceptable for post trade processing use case. It is therefore expected that the blockchain applied here will have the ability to use a consensus algorithm, which has immediate finality.

[3]The contribution of the transaction to the market and credit risk of the respective counterparts

[4]Using blockchain for near-time settlement may eliminate the netting (position offsetting) benefits to the counterparties derived from end-of-day processing, so its utility for the settlement portion of the post trade processing may be limited.

Post trade activity participants have the expectation of privacy and confidentiality of transactions. The clearing house recording the transaction must ensure that parties are not able to perceive each others position and trade information. Moreover, the existence of trades themselves, even if parties are anonymized, should not be revealed since it may make transactions susceptible to traffic analysis. Current generation of analysis tools may be able to compromise both identity of the participants and trading patterns, which could be correlated to the public market information.

As described above current post trade activities happen at the end of the business day, thus presenting a different set of performance requirements than a system based on a blockchain would have. The total number of transactions would increase given the participants' ability to learn their position with the clearing house in near real-time. So while the average transactions per second number would increase, the peak performance requirements would decrease significantly, since end-of-day reconciliation used to transmit the entire set of trade records for the day would have been made obsolete.

Hyperledger Fabric channels combined with separate endorser sets provide an excellent solution to the problems of privacy and confidentiality. Ability to restrict data replication to only permissioned parties brings the benefits of the blockchain for data integrity and non-repudiation of transactions without compromising the security of the data. Reporting requirements - both internal and external - can be satisfied by including a regulatory agency and other oversight entities as members of the channel. Furthermore, network segmentation enabled by Fabric's channels can help in supporting multiple jurisdictions and regulatory regimes.

Hyperledger Sawtooth transaction families provide a reliable and performant way to encapsulate the operations relevant to the post trade. The ability to build complex rules using a language of choice to expose the interface which only provides the functions permitted in the context, bring a higher level of trust for the financial services institutions by providing the smart contract functionality without the risk of ad-hoc deployable code.

Hyperledger Indy's unlinkable verifiable claims can be leveraged to report outstanding risk on a shared ledger without compromising the identity of the firm, and still allow a regulatory body to have a holistic view of the market, enabling it to prevent potential market crashes and major defaults. This feature can further alleviate the privacy concerns, by putting participants in control of their network identities and disclosed attributes.

5.4 Health Records: Credentialing

Blockchain technologies have the potential to ameliorate one of the great annoyances of modern medical practice: "credentialing". Credentialing is the process a hospital uses to ensure that its physicians are competent and worthy of the trust that patients put in them. In a sense, credentialing is the hospital's way of performing "due diligence" on a physician.

A physician who wishes to become affiliated with a hospital begins the process by first gathering copies of all of his or her professional credentials including, for example:

- Medical school diploma
- Certificates of any residencies and fellowships the physician completed
- Copies of any specialty medical boards that have certified the physician
- All state medical licenses held by the physician

- Evaluations from peers
- Proof that the physician is current on continuing medical education requirements
- Letters from hospitals with which the physician was previously affiliated, explaining the circumstances under which the affiliation ended
- Details of any malpractice actions against the physician

The hospital's credentialing office checks the physician's documentation for completeness, accuracy, and authenticity. This is an exacting task. Almost inevitably, they will find shortfalls, and will ask the physician to supply missing documents. In many cases, the hospital's credentialing office will verify some or all of the physician's submitted documentation, e.g., telephoning the physician's medical school to confirm that the physician did indeed graduate from there. It is not uncommon for weeks or months to elapse as the physician and credentialing office work to satisfy the hospital's requirements.

Once the documentation is determined to be complete, accurate and authentic, the hospital's credentialing committee, typically composed of both physicians and administrators, sits in judgment of the physician and decides whether or not to allow the physician to begin practicing in affiliation with the hospital.

When using blockchain technology in any solution, several key decisions must be made.

First, will content or pointers-to-content be placed on the blockchain? For credentialing solutions, it might be reasonable to place publically available information (such as state medical licensing) on the blockchain itself. However, private information (such as peer reviews) are better stored off the chain to guard against compromise of encryption keys and give users the ability to remove (but not edit) information, thereby increasing trust.

Second, what is the best way to manage the identities potentially of thousands of participants? For ambitious credentialing solutions, this might include every hospital, every physician, every provider of continuing medical education, and so on.

Third, what are the resource requirements, specifically storage? Credentialling solutions may provide service for decades. Persistent commitment of participation comes with a potentially significant contribution of resources for compute, communication, and storage. For example, what if, a few years from now, credentialing organizations want video testimony from peers?

Hyperledger Indy provides off-the-shelf solutions for what would otherwise require careful engineering of new software modules. Indy implements the proposed W3C standard for verifiable claims. This capability provides a method for pairwise exchange of selected credential attributes. For example, a physician could request a credential from their medical school that attests to their successful graduation. That credential could be provided by the physician to a hospital as verification of education. An important property of Indy and their implementation of verifiable claims is that the the credential for education can be verified by the hospital as graduation from an accredited university without the need to contact the medical school directly. The applying physician need only expose precisely what is required for credentialing at the hospital; no additional exposure is necessary.

6 Current Projects

6.1 Fabric

Hyperledger Fabric is a platform for distributed ledger solutions, underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability. It is designed to support pluggable implementations of different components, and accommodate the complexity and intricacies that exist across the economic ecosystem.

Where Hyperledger Fabric breaks from some other blockchain systems is that it is private and permissioned. Rather than allowing anyone to be part of the network by either participating in the Proof-of-Work consensus or receiving transferrable forms of data such as tokens over the blockchain, the members of a Hyperledger Fabric network enroll through a membership services provider.

Hyperledger Fabric also offers the ability to create channels, allowing a group of participants to create a separate ledger of transactions. This is an especially important option for networks where some participants might be competitors and not want every transaction they make, such as a special price theyre offering to some participants and not others, known to every participant in the network. If two participants form a channel, then only those participants, and no others, have copies of the ledger for that channel.

6.2 Sawtooth

The Sawtooth design philosophy targets keeping distributed ledgers distributed and making smart contracts safe - particularly for enterprise use.

In fitting with this enterprise focus, Sawtooth is also highly modular. This enables enterprises and consortia to make policy decisions that they are best equipped to make.

Originally, Sawtooth was designed to explore scalability, security, and privacy questions prompted by the original distributed ledgers. That mandated a certain modularity that was lacking at the time. Starting from scratch allowed us to employ lessons from those pioneering systems and branch into usages that the original currency ledgers werent intended to address. PoET, the new consensus hits scalability, while Transaction Families, our contract logic, narrow the attack surface for contracts while simultaneously broadening the functionality. We also have a keen interest in trusted execution environments and what role that can play in private transactions.

In branching into new business cases, we felt it was important that the system preserve certain tenants of a distributed ledger. That is, in an enterprise deployment, the concept of a distributed ledger shouldnt collapse into a replicated database. Enterprise participants need autonomy and they have the right to run their own nodes. The set of participants will also be dynamic and the system particularly consensus must accommodate that volatility. It is not clear, for example, whether an O(n2) protocol with fixed membership like PBFT can support the scale or volatility of a distributed ledger at production levels. Further it seems inadvisable to sidestep the challenges of providing Byzantine Fault Tolerance and operate on only a Crash Fault Tolerant consensus. Finally, we observed that, public and private define a spectrum of authorization policies not a binary option for a distributed ledger.

6.3 Iroha

Hyperledger Iroha joined Fabric and Sawtooth Lake to become the third distributed ledger platform under the Hyperledger umbrella in October, 2016. It was originally developed by Soramitsu in

Japan and was proposed to the Hyperledger Project by Soramitsu, Hitachi, NTT Data, and Colu.

Iroha takes a very different design philosophy from Fabric and Sawtooth Lake, in that it focuses on providing features that are helpful for creating applications for end-users.

6.4 Burrow

Hyperledger Burrow is a permissionable smart contract machine; it became the fourth distributed ledger platform under the Hyperledger umbrella in April, 2017. It was originally developed and proposed to Hyperledger by Monax.

Burrow provides a modular blockchain client with a permissioned smart contract interpreter built to the specification of the Ethereum Virtual Machine (EVM). Burrow provides a strongly deterministic, smart contract focused, blockchain design to Hyperledger's overall effort. Users of Burrow are able to benefit from having an access control layer through the use of smart contracts and our secure natives based permission layer.

The major components of Burrow are as follows:

Consensus engine which is responsible for maintaining the networking stack between nodes and ordering transactions to be utilized 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 application builders with a strongly deterministic smart contract engine for operating complex industrial processes. Gateway provides programmatic interfaces for systems integrations and user interfaces

6.5 Indy

Hyperledger Indy uses distributed ledger technology to make identity independent of organizational silos; friends, competitors, and even antagonists can all rely on a shared source of truth that answers fundamental questions such as, Who am I dealing with? and How can I verify data about the other party in this interaction? Solid answers to these questions enable the sort of trusted interactions demanded everywhere.

Because Indy stores identity artifacts (public keys, proofs of existence, cryptographic accumulators that enable revocation) on a ledger with distributed ownership, identities can be self-sovereign– nobody external to the identity owner can manipulate them or take them away. Identity in Indy is also privacy-preserving by default, meaning that an identity owner can operate without creating correlation risk or breadcrumbs.

A core technology for Indy is verifiable claims. These attestations of an identitys attributes resemble credentials familiar to all of us: passports, drivers licenses, birth certificates, and so forth. But they can be combined and transformed in powerful ways, using zero-knowledge proofs to enable selective disclosure of just those pieces of data that a particular context demands.

This combination of self-sovereignty, privacy, and verifiable claims is synergistic. Bulk troves of sensitive data vanish or become useless. The economics of hacking transform. The competing demands of privacy-preserving and strongly identifying regulations are satisfied. Individuals and organizations are free to seek mutual benefit from rich interaction; the identity ecosystem gains the innovation and dynamism of a free market.

Despite the advanced crypto under the hood, Indys API is simple and straightforward. It consists of about 50 C-callable functions, with idomatic wrappers for many mainstream programming languages,

6.6 Cello

Hyperledger Cello is an open framework to help people adopt blockchain technologies efficiently and easily, by providing automatic ways in blockchain provision and operational management.

It brings the on-demand "as-a-service" deployment model to the blockchain ecosystem to reduce the effort required for maintaining the lifecycle of the Hyperledger blockchain frameworks. It provides a multi-tenant chain service efficiently and automatically on top of various infrastructures, including baremetal, virtual machine, Cloud platforms like AWS, and container platforms like Docker Swarm and Kubernetes, overall helping provide "Blockchain as a Service" efficiently. It also helps with maintainance through a dashboard where users can watch the statistics/status of the blockchain system (e.g., system utilization, blockchain events, chaincode performance), and manage the blockchains (e.g., create, config and delete) and chaincode (e.g., deploy and upload private chaincode) in real-time.

Hyperledger Cello currently has supported Hyperledger Fabric 1.0 as the main blockchain implementation, while it has plans to support more blockchain types like sawtooth. The architecture follows the micro-service style, with pluggable implementations for most components. The main programing languages are Python and JavaScript.

6.7 Composer

Hyperledger Composer is an extensive, open development toolset and framework to make developing blockchain applications easier. Our primary goal is to accelerate time to value and make it easier to integrate your blockchain applications with the existing business systems. You can use Hyperledger Composer to rapidly develop use cases and deploy a blockchain solution in weeks rather than months. It also allows you to model your business network and integrate existing systems and data with your blockchain applications.

You can use Hyperledger Composer to quickly model your current business network, containing your existing assets, such as tangible or intangible goods, services, or property, and the transactions related to them. As part of your business network model, you define the transactions which can interact with assets. Business networks also include the participants who interact with them, each of which can be associated with a unique identity across multiple business networks.

Hyperledger Composer supports the existing Hyperledger Fabric blockchain infrastructure and runtime, which supports pluggable blockchain consensus protocols to ensure that transactions are validated according to policy by the designated business network participants.

6.8 Explorer

Blockchain explorer provides a dashboard for viewing information about transactions, blocks, node logs, statistics, and smart contracts available on the network. Users will be able to query for specific blocks or transactions and view the complete details. Blockchain explorer can also be integrated with any authentication/authorization platforms (commercial/open source) and will provided appropriate functionality based on the privileges available to the user. Goals of the project are listed below. To implement a generic Blockchain explorer web application which is easy to install and can be used with different Blockchain platforms. Use latest tools and technologies that make the explorer easy to implement, maintain and extend. Easily installable package available through standard package managers for most popular platforms.

Please refer to the project proposal document on the wiki (`https://wiki.hyperledger.org/projects/explorer`) page to understand more about the project.

7 Highlighted Features

7.1 Identity

Indy shares some features with traditional enterprise identity solutions–the world of LDAP, OAuth, 2FA, IDPs, and similar tech. Both approaches use industrial-strength crypto. Both enable capturing and sharing rich metadata about an identity. Both facilitate sophisticated access control and policy. But there is a profound difference: Indy identities are shared instead of siloed and federated. An Indy identity is portable–you can bring it with you wherever the distributed ledger is accepted. Ten orgs or systems that each support Indy identities dont create ten separate identities for John Q. Public; John simply shows up with his pre-existing identity and uses it. Organizations can cancel Johns access, but never his identity, because John owns it. John, not the places that accept Johns identity, controls access to his data.

Indy also shares some features with blockchain-based identity solutions such as Blockstack and Uport. All of these technologies store identity on a distributed ledger and thus promote security and personal freedom. However, Blockstack and Uport depend on Bitcoin and Ethereum, respectively. These are proof-of-work ecosystems that impose a non-trivial cost on transactions; every new persona, public key rotation, published attribute, or pairwise relationship is a tangible expense. This creates a disincentive to pairwise relationships, which undermines privacy. Also, these ecosystems are global and public; they cannot be special-purposed for a less-than-fully-global context. Indy, on the other hand, does not use proof-of-work–transactions are free. And instances of it can be used in whatever context is convenient.

8 Long-Term Vision

We already live in a highly interconnected world. In the future, we believe that the world will become even more closely tied together: more data sharing, more communication, and more digital content, will become the norm in both our business and personal lives. This will necessitate careful management of security, privacy, and trust. We view distributed ledger technology as the solution to the problem where someone needs a distributed database for which there is no single owner that is trusted by all of the users. Thus, as interconnection increases, we believe that blockchain technology and DLT as a whole will become quite prevalent in society as distributed ledgers replace some, but not all, traditional databases where viable.

This prevalence of distributed ledgers will not come about without difficulty, however. Nothing in this space is "for free". For instance, if you want a great deal of security and privacy features in a blockchain, you will often pay the price in terms of performance. This implies that we will need to have a large variety of different blockchains–no one blockchain will work for all applications–that can communicate and interact seamlessly.

Thus, our long-term vision for Hyperledger is driven by two main architectural concerns: modularity and interoperability. We hope that, eventually, Hyperledger consists of lots of modules for various different blockchain components that can be put together by a non-expert into a cohesive, functional, and secure distributed ledger. All of these modules would be interchangeable with other

modules of the same time, and able to communicate with other modules of different types (or the same type if involved in communication between separate blockchains). This would ideally enable a non-expert to set up an interoperable and secure blockchain quickly, easily, and efficiently.

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 diverse blockchains and we hope that other developers consider interoperability with Hyperledger projects. We do not intend for Hyperledger to be a single stack. Instead, we hope that it becomes a collection of tools purpose built with interoperability and modularity in mind. Any individual can use one, some, or all of the Hyperledger projects to 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 necessitate a good community, strong industrial support, and solid design principles. As we have hopefully illustrated in this paper, we have structured Hyperledger with these tenets in mind. It is now up to us to go out and accomplish this.

9 Conclusion

In this paper, we have explained the rationale behind the creation of Hyperledger and what our goals were (and still are for the project). We outlined why we think an open-source, umbrella project seems to be the optimal governing arrangement for a general blockchain consortium. We proposed some of the use cases that inspired our members to found and develop Hyperledger and delineated some of the features that result from building blockchain for some of these interesting use cases. In addition, we briefly summarized all of the main Hyperledger projects and their statuses.

We hope that this is just the beginning for many readers. While this paper is not intended to be technical, we note that there is a wealth of technical information on the Hyperledger wiki. Each of the main projects has quite a bit of documentation, getting-started guides, and help available here[5]. In addition, some of the working groups have great technical resources. The architecture working group has a substantial amount of documentation on permissioned blockchain fundamentals and is a great resource for those looking to explore technical details. There are also application-specific working groups that are 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. We encourage readers to look to these places for more information on topics that they find interesting.

We hope that this paper is just the beginning of the Hyperledger experience for many. We acknowledge that there is a lot of work left to be done, and that Hyperledger will almost always be a work in progress. But we think our organization is solid and believe that, maybe with your help, we can build secure, efficient, and reliable blockchain solutions.

References

[But13] Vitalik Buterin. Ethereum white paper: a next generation smart contract & decentralized application platform. *www3. ethereum. org Nick Szabo, Formalizing and Securing Relationships on Public Networks, http://szabo. best. vwh. net/formalize. html*, 2013.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[5]If this isn't true, it should be!