DFIN | LedgerDomain

WHITE PAPER | BLOCKCHAIN

Global Enterprise and Real-Time Financial Computing

LedgerDomain's blockchain-based communal trust platform

Donnelley Financial Solutions (DFIN) partnered with LedgerDomain in June 2018 to bring the power and security of blockchain to clients globally. In this whitepaper, the team behind the blockchain startup explains why blockchain is the missing element in real-time fiscal calculations.

LedgerDomain was founded two years ago with a simple goal: the application of new blockchain technologies to enterprises the world over.

Since announcing their partnership in June 2018, DFIN and LedgerDomain are building secure, cloud-based applications for companies to collaborate on complex processes with critical regulatory and compliance dynamics. The enterprise blockchain solution is a multi-user database with cell-level encryption that automates workstreams performed by investment market teams.

“Regulatory disclosures and shareholder communications are manually intensive and complex, and involve multiple internal and external parties,” said Eric Johnson, president of Global Investment Markets at DFIN.

“Blockchain-based enterprise solutions address our clients’ pain points by attacking cost, complexity and operational risks to improve the overall client experience. As the trusted partner for 90 percent of the top 50 fund complexes, DFIN will be able to offer clients a next generation technology solution to streamline their most complex transactions.”

“We’re excited to combine LedgerDomain’s expertise in blockchain technology with DFIN’s digital regulatory and shareholder solutions,” said Ben Taylor, CEO of LedgerDomain. “We knew we needed a partner that could deliver actionable solutions. When we sat down with Eric and his team, we realized immediately that we shared a vision on technology and trust.”

The blockchain has garnered much praise, yet manwy implementation details remain vague. In this whitepaper, we provide some context for the history of financial computing. We also explain why blockchain is the missing element in real-time fiscal calculations.

Communal transactional computing is not new, of course: We all use a global network of ATM machines every day. We’re certainly accustomed to using a Chase ATM card in a Citibank ATM machine. This paper, however, proposes superior and structured choices for a community’s optimal level of network sharing.

We then review the infrastructure needed to attain those levels. Componentized, open-source platforms provide especially good value and flexibility. Consequently, LedgerDomain is standardized on Hyperledger Fabric, a Linux Foundation venture. It also makes substantial use of other open-source components.

Next, we explain some related facets of the project:

- Our code base, extending the Hyperledger infrastructure.
- Our Selvedge blockchain application server.
- Our smart contracts.
- Client applications purpose-built for our customers.

In essence, LedgerDomain delivers a highly robust and customized system, with capabilities at any scale.

Thanks in advance for your time and interest!

From all of us at DFIN and LedgerDomain

Essential terms

Cryptocurrency

When you think of blockchain, you probably think of its cryptocurrency applications. There are three main families of cryptocurrency:

1. Those associated with the Bitcoin platform.
2. Those tied to the Ethereum platform.
3. Independent forms.

In essence, anyone may purchase a "wallet" and then procure "coins" — which may then be transferred to others. These dealings occur in open networks where strangers trade incognito.[1] This ecosystem has been running for nearly a decade and remains surprisingly robust.[2]

Two points of immediate note:

1. Bitcoin is not a double-entry bookkeeping system (endeavoring to capture bitcoin movements with an attached memo field).
2. Bitcoin is a living system, with gradual improvements or changes occurring continuously.

Ethereum, as an alternative to bitcoin, is popular for hosting its own currency, known as "ether." It is also home to other currencies, CryptoKitties trading, and various proofs-of-concept. Ethereum has grand aspirations and — accordingly — has experienced growing pains.

In short, cryptocurrency platforms have created both a new type of computing and a new type of trust. They have generated a unique asset class from thin air. Whether any of these coins will have value in the future, only time will tell. Thus far, we can declare that the underlying technology has been stress-tested — and preserves genuine worth.

Blockchain

Blockchain is not a database, but rather sits atop a database. It is a time-stamped data organization, often implemented with cell-level encryption. That encryption allows many participants to access their own cells — and not the cells of other users.

Each event within the blockchain occurs when parties agree to e-sign a transaction. The agreement, in turn, follows an associated "smart contract." A contract makes each transaction both binding and irrevocable. If a transaction is struck between two parties, each will have keyed access — as might a regulator, auditor or lender.

Blockchains need not include a cryptocurrency. By way of example, Hyperledger, an open-source blockchain platform sponsored by the Linux Foundation, is designed to support deals without a cryptocurrency component.[3]

1 The **original bitcoin white paper**, written by Satoshi Nakamoto, has never been bettered.

2 To our knowledge, neither wallet owners nor traders on the platform have encountered problems.

3 IBM recently published a **path-breaking paper** which detailed its many features.

Smart contracts

Smart contracts, whose history actually pre-dates bitcoin, were brought to fruition by **Nick Szabo**. They are pieces of code dictating the contractual terms of a transaction upon the blockchain. As they have grown in syntactical power, smart contracts can now mediate the kinds of basic financial relationships we encounter every day.

Financial computing

Financial computing consists of three elements:

1. Financial planning and analysis.
2. Price discovery, contracting, and binding.
3. Settlement and netting.

At LedgerDomain, our mission is to help enterprises use blockchain. We strive for frictionless commerce – in monetary transactions and elsewhere. Further details on how blockchain is key to the history of **financial computing** are detailed below.

Non-monetary transactions on blockchain

Many of life's transactions are perceived to be valuable, yet remain unquantifiable in any monetary sense. They range from marriage contracts to "track and trace" in a supply chain — one might even include the sharing of personal medical information. Smart contracts model all those dealings; the blockchain both captures and stores them.

Personal medical information is highly regulated (**HIPAA** in the US, **GDPR** in the EU, etc.). Blockchain makes possible the sharing of anonymized compliant datasets.

While the immutability of blockchain data is difficult to reconcile with the GDPR "right to be forgotten," LedgerDomain is on the forefront of GDPR-compliant blockchain development.

Unique identifiers

Over time, most blockchain applications and systems will interface with real-world objects. For blockchain to perform properly, these objects must have unique identifiers: 2D barcodes, RFID tags, machine-readable labels, etc. Such systems are affordable; general-purpose input devices like iPhones can read them.

Why blockchain unlocks the fourth wave of financial computing

As noted, blockchain's cryptographic safeguards have enabled cryptocurrencies like bitcoin to be transferred by strangers — globally. These same techniques will allow global enterprises to transact with zero friction across firewalls and borders. Moreover, blockchain's structure lets users analyze their own granular, historical data confidentially.

This so-called "one and done" approach equates to a contract:

- A day journal entry for the first party.
- A day journal entry for the second party.
- An audit-confirm for each of their auditors.
- And potential proof to any third-party authority. (for regulatory compliance or taxation.)

A perfect day journal is by no means a complete accounting system, but it's an amazing start.

To understand the implications of all this, we need to appreciate how financial computing has evolved within human economies. Financial computing is the art and science of recording events with a common unit of account (bitcoins, dollars, gold); a common unit of time; and more than one financial agent. In turn, these events can be integrated into "stocks" (like your bank balance) and differentiated into "flows" (like your annual W-2 earnings).

In a structurally comparable way, financial computing consists of three disciplines:

- Accounting (concerned with the past)
- Contractual matching and binding (present)
- Financial modeling (focused on the future)

The first wave of this financial computing paradigm emerged with writing, numbers and money in ancient Babylon. It was perfected in 1500 with the dawn of modern accounting. It then scaled in 1900 with the cost accounting and tabulating machines that enabled truly global enterprises. A fourth wave (1958-2028?) is currently moving towards real-time practices. Blockchain is required to drive both real-time and closed-loop financial computing.

The rise of artificial intelligence (AI) and the Internet of Things (IoT) could nudge that final stage towards "financial singularity." It might realize a dream that started with the earliest of settled societies. En route to that desired goal, both a communal trust platform and advanced algorithmic workflows are essential. Enter LedgerDomain.

Communal applications, permissioned blockchains and Hyperledger

The sponsors or system owners of blockchain-style communal applications might share the following models among peer organizations and/or their members:

1. a data model in which everyone agrees to use the same data fields and formats, yet has their own clients and blockchain backends;
2. client sharing in which all sites use the same client, while blockchain backends differ;
3. fully-shared open blockchain systems with encrypted data (e.g. Bitcoin or Ethereum);
4. fully-shared and permissioned blockchain systems with encrypted data; or
5. fully-shared and permissioned blockchain systems with encrypted data and partitioning.

And that gives us the following scenarios:

1. In the open blockchain's vanilla form, members can see/decrypt only their own data.
2. In the permissioned blockchain's vanilla form, only permissioned members can see/decrypt only their own data.
3. In permissioned and partitioned blockchains, each member may use private channels to transact with trading partners. Likewise, others may possess their own channels.

In the Hyperledger architecture, this partitioning is called a (private) channel. While provisioning them is a chore, organizations will appreciate the additional privacy and security.

All five strategies have merit — and all will probably find their devotees. Even modest standardization, such as the shared data model, can direct considerable benefits towards traders. That said, LedgerDomain is focused on certain variants of shared-permission blockchain-based systems. We use Hyperledger Fabric components as a scaffolding for our client sponsors.

Blockchain types	Strengths	Weaknesses	Opportunities	Threats
1. Shared data model	Key partnership	Hard to change	Future-proof	
2. Shared client and data model	Site efficiency	Maintainability		Viral infection
3. Shared open system	TCO	Platform control	Lightning?	Security model
4. Shared permissioned system	Industry control	Less flexible	Upgradability	
5. Shared permissioned and partitioned system	Gold standard	Expensive	Upgradability	

4 See the documentation on Hyperledger channels.

Hyperledger

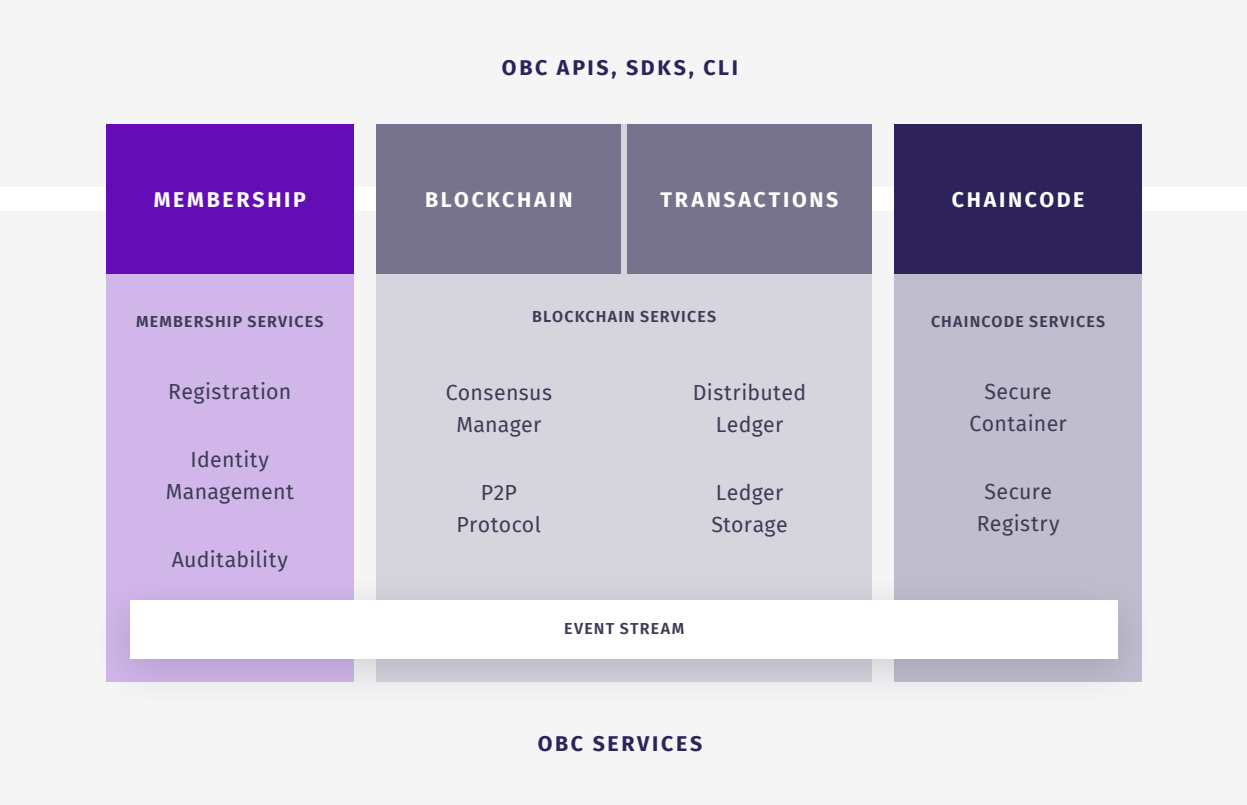
Hyperledger is an umbrella organization under the aegis of the Linux Foundation. It currently has over 150 members. Hyperledger products are licensed under the **Apache License Version 2.0 Software**. LedgerDomain has been a proud member of Hyperledger since 2016.

Hyperledger Fabric is the organization's most comprehensive and mature project. It is the platform upon which LedgerDomain remains focused. Currently in production mode, Hyperledger Fabric 1.3 is the stable release as of October 2018.

It should be emphasized, though, that Hyperledger Fabric is an empty vessel. The sponsor supplies the chaincode instructions, commonly termed "Smart Contracts," as well as the associated client software.

Hyperledger Fabric is componentized: Any of its eighteen or more elements may be substituted and replaced with other open-source or third-party equivalents.

Our whitepaper now turns to three additional foci of enduring significance: (1) membership and certificates; (2) application services and dev ops; and (3) notarization.



Memberships and certificates

The topic of membership may well be the most challenging. In an open blockchain such as bitcoin, every wallet is held by the wallet holder. The wallet holder is typically anonymous and the system maintains none of his/her attributes. If a wallet holder is presumed to owe taxes on a transaction, an honor system prevails; if another feels that they have been mistreated, remedies are pursued out of band.

With a permissioned blockchain system such as Hyperledger Fabric, a sponsor could of course replicate the open blockchain experience. He or she could simply invite a large number of random participants, yet the presumption is that sponsors will invite responsible organizations. They will have vetted one another and, in turn, will manage their members' participation.

As such, Hyperledger Fabric provides fine-grained controls emanating from a root server — through an organization to a defined and organizationally backed participant. Mapping and configuring these member relationships is far from trivial; care must be taken to set up members with appropriate privileges. Communities with many members joining and leaving need to resource their dev ops team appropriately.

Application services and dev ops

Hyperledger Fabric today is ready to support clients and server pairs — once components have been configured and the chain code launched. However, in order to perform adequately under load, the administrator must first provide a server environment supporting any and all clients. He or she must then provision appropriate system resources, all in a secure manner.

We liken this process to visiting an auto parts store, buying all the parts, going to the parking lot — and putting them all together before driving away. Our Dev Ops tools handle a range of non-trivial challenges that sponsors face, which include:

- defining the organizations in the network-to-be
- communicating crypto/configuration materials for network bootstrapping
- configuring, deploying, running and monitoring all services in the Fabric network
- creating the channel(s) and having orgs' peers join the desired channels

At LedgerDomain, we have also built a blockchain application server to both manage the original configuration and dynamically respond to environmental challenges. We call this Selvedge, appropriating another textile term. It's a self-finished edge of fabric that cannot unravel.

Notarization

Many students of blockchain are aware that in open platforms (like Bitcoin and Ethereum) the so-called "mining" is a critical security layer. The miners' role is to safeguard against double-spending and other malfeasance.

In permissioned blockchain systems, the security envelope is a little different: The permissioning allows for access control, while the Membership Service Provider (MSP) coordinates the certificate cascade. The administrator then works with the sponsor/organization to grant member-appropriate privileges. Notarization is also an important consideration for the sponsor. Hyperledger Fabric can be run with a variety of different notarization schemes, each with their own costs and benefits. Hyperledger Fabric is designed to be plug-compatible with newer schemes as/when they emerge.

The LedgerDomain Selvedge blockchain app server

Hyperledger Fabric is a rich, highly-configurable suite of software components from which blockchain systems can be built. A vanilla Fabric project is adequate for both pilots and live implementations targeted at workgroups. Nevertheless, larger blockchain implementations are undeniably compute-intensive. That brings us to Selvedge.

Selvedge is the world's first enterprise-class blockchain app platform. The brainchild of LedgerDomain chief software architect Dr. Victor Dods, it was handmade to meet the expectations of Web 2.0 enterprise companies and their Global 2000 peers around the world.

Selvedge mediates between client organizations and members. In other words, it is positioned between their private channels, respective public/private smart contracts and correlated chain code. Critically, Selvedge may be configured to operate in "lights-out" environments, wherein an administrator can orchestrate and provision without access to members' sensitive data.

Using the Hyperledger Fabric Peer Event Hub, Selvedge coordinates messaging to both members and peripheral enterprise systems. As such, it handles exception reporting and failed transactions with ease. Selvedge is comprised of multiple components. The backend is 100 percent Golang (a fast, statically compiled language). The configuration, deployment and administration tools are written in Python for the sake of flexibility.

Selvedge is also capable of auto-deployment seeded via SSH. Similar to a cloud-based machine image, complete with chaincode and versioning, this is the most secure and scalable solution for blockchain deployment on bare metal without the need for specialized local personnel.

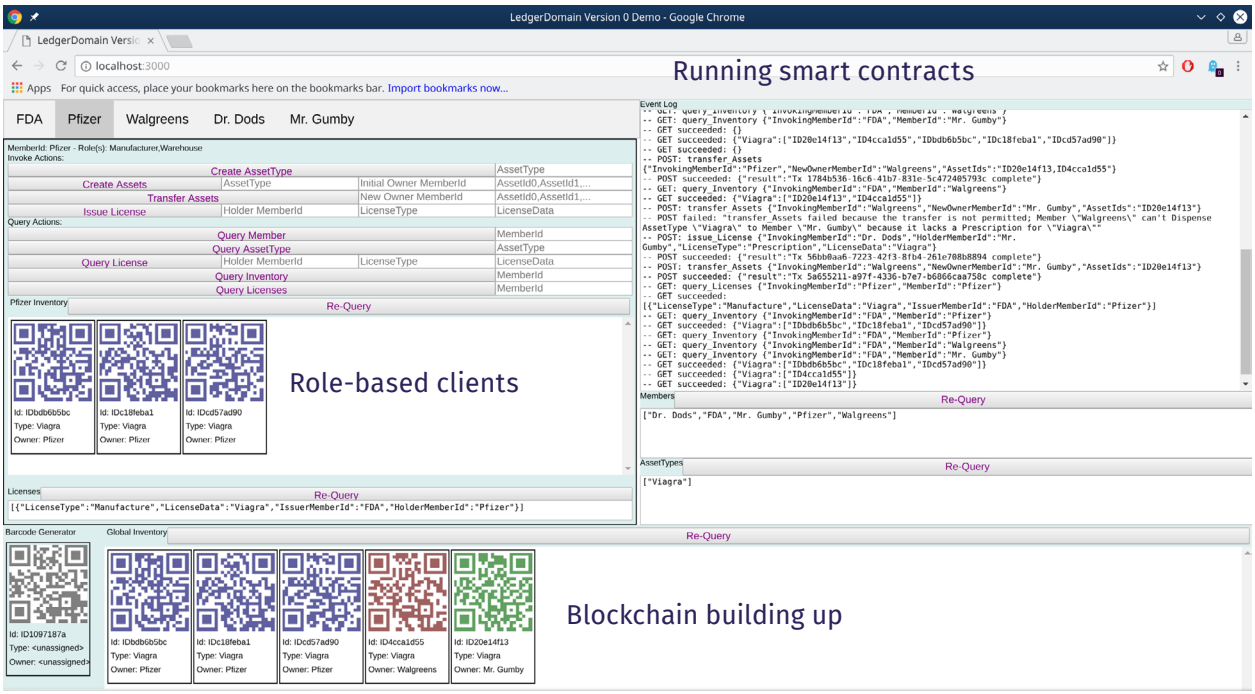
LedgerDomain tiered clients

System-integrity risks are inherently unequal; the same can be said of clients.

A key initiative at LedgerDomain concerns our tiered clients. We grant a range of certificate authorities to organizational members, who in turn deputize individual members. We term this “role-based membership,” leading to purpose-built role-based clients.

Here we show clearly how these clients are stacked in administrative “G*d Mode.” Below is a screenshot of the US pharmaceutical supply chain, in which a hypothetical pharmaceutical company receives a certificate from a regulator to manufacture/distribute a hypothetical medicine. The company then transfers custody to a hypothetical drugstore company.

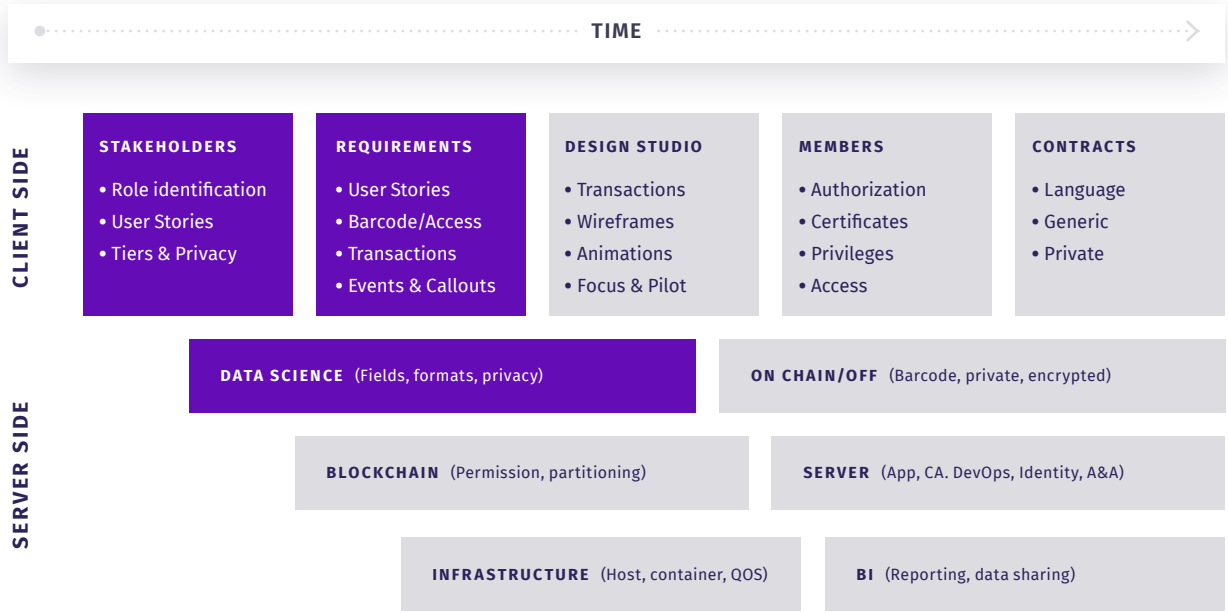
In this same model, a physician — Dr. Dods — prescribes for a patient, whom we shall call Mr. Gumby. Both invocations of and responses from the attendant smart contracts are seen to the right; unique identifiers for pill bottles are shown at the bottom of the image. Real-life blockchains at work!



LedgerDomain smart contracts

Smart contracts, or chaincodes, run on the blockchain network peers. They govern the community's transactions. Many basic dealings — such as chain of custody in the supply chain or value transfer in cryptocurrencies — require nothing more than compact sets of instructions.

Most modern enterprise ecosystems, however, are far from simple. The key to successful system performance is to engage key stakeholders in workshops. Design studios can correctly model desired roles and transactions. Everything is then translated to (1) tiered clients, (2) membership privileges and (3) smart contracts in an integrated fashion, using the appropriate data science model. The overall process is visualized below.

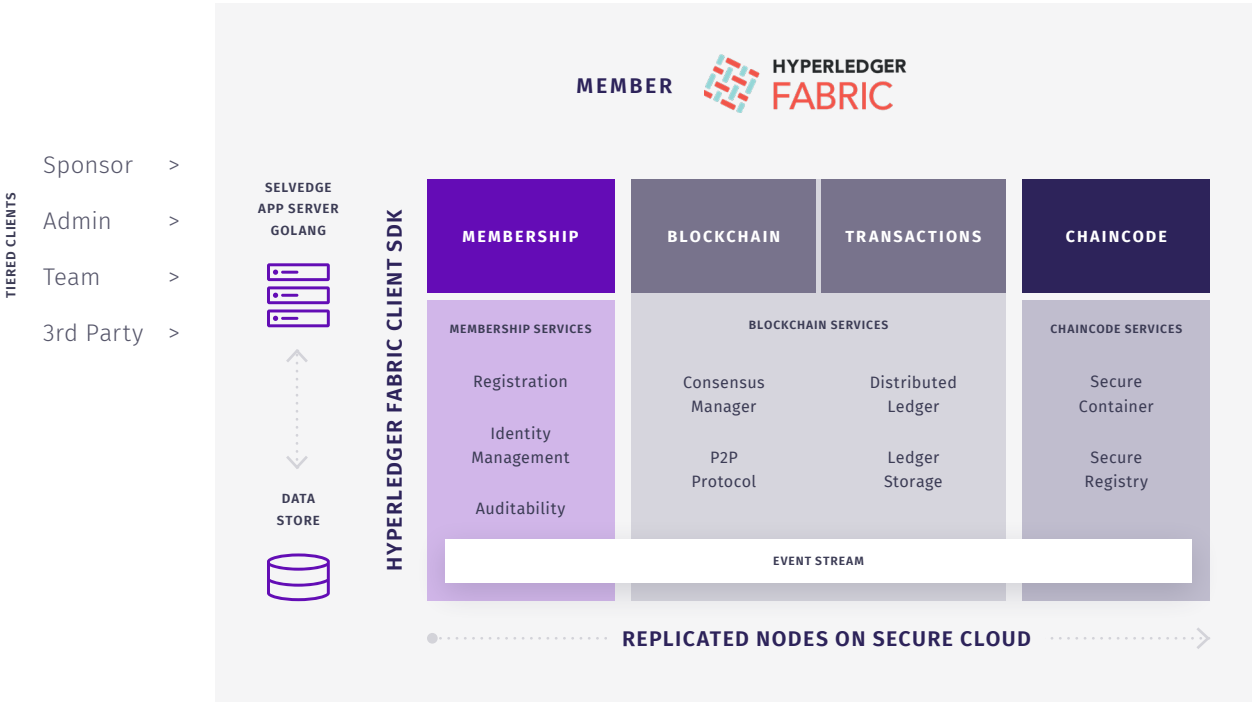


The smart contracts dictate all transactions on the system, either at the global level or within channels maintained by a subset of member organizations.[5]

5 The LedgerDomain chain code (smart contract) library is implemented in Golang. This enhances readability, reduces ambiguity, and provides either memory or computational efficiency. Selvedge's run-time components and the Sponsor's smart contracts are compiled, maintained, and QA'd together.

The LedgerDomain stack

Now that we've seen all the individual pieces, LedgerDomain's stack looks like this:



Our system typically runs on hosts such as Amazon Web Services, although certain clients opt to run their own nodes independently, either for compliance or policy reasons. IBM and Oracle provide hosting services as Hyperledger members.

The instances are configured with a variety of specialized replicated nodes, customized based on factors such as (1) the number of clients, (2) the peak load of transactions per second, (3) the geographic spread, (4) the average transaction file size, (5) regulatory stipulations and (6) the notarization scheme. Our Dev Ops team tunes each network so your Selvedge server can optimize system performance on the fly.

Thus we reach the leading edge of blockchain technology. Everything is secure and cross-organizational, and works in real time. You're ready to bring a truly disruptive technology to your own ecosystem with a fellow blockchain thought-leader at LedgerDomain.