Implementing blockchains and distributed infrastructure

Building a better working world

1. Introduction

Blockchain and distributed ledger technology is quickly gaining traction in the financial services industry. Both incumbents and start-ups are actively looking to apply the technology to reduce costs or improve efficiency. The technology's potential to make ledgers more transparent, trustworthy and efficient leads to suggestions that it can possibly revolutionize financial services and other industries.

Applying the blockchain within each firm's context is complicated, however: despite companies' enthusiasm and its rapid evolution, the technology is still in its infancy. It is as yet unclear what business needs, if any, the blockchain will truly resolve, and some question whether this technology is "looking for a solution." While it may take years for its potential benefits to crystallize, firms understandably aim to experiment with the technology to uncover valuable applications.

To help firms understand the technology and how its power can be harnessed, this article explains the blockchain's potential to change financial services, explores possible applications and describes the issues worth considering when applying the technology.

2. What are blockchain distributed ledger and distributed infrastructure technologies?

Distributed ledger technology, of which blockchain is the most widely known example, allows for the sharing of a ledger of activity — such as arbitrary data or tokens to which value is assigned — between multiple parties.

A distributed ledger can take over many of the functions performed by central third parties, by enabling the network itself to be the intermediary (see figure 1). This is particularly relevant for financial services, a field in which reputable third parties are widely used to create trust and decrease risk.

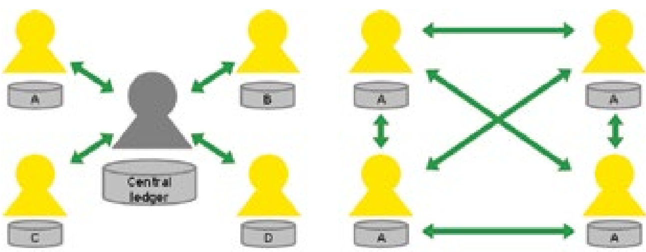


Figure 1 — In a traditional setup, a central third party controls the flows of information in its central ledger, and each connected party has its own copy of its individual activity. A distributed setup allows each connected party to interact with one another using the same distributed ledger.

Distributed ledgers can be enhanced by smart contracts, which are small computer programs that behave according to predefined logic. Once created, smart contracts are able to operate autonomously — independently of any party in the system, including its creator — and consequently thought to be capable of replacing legal contracts. That is, these smart contracts can be used to model the terms of a real-world contract and automatically enforce its clauses as contractual conditions are met. Despite the name, smart contracts' capabilities are not limited to legal contracts and can be arbitrarily complex: that is, complete software applications can be placed on a distributed ledger to operate autonomously.

Consequently, distributed ledgers enabled with smart contracts could become capable of performing trusted database operations in a distributed environment that today would require a centralized infrastructure. Given this potential for distributed ledger technology and smart contracts to allow the distribution of any centralized computing infrastructure, we consider this overall field to be distributed infrastructure.

It is no surprise that the blockchain is being tested as a means to improve business areas that today are considered unreliable, expensive or inefficient because of current infrastructure or business models.

3. The spectrum of (de)centralization

The term distributed infrastructure implies that firms that consider applying the technology should be willing to share control over the infrastructure they wish to distribute. The extent to which the infrastructure is shared can be plotted along a spectrum that ranges from fully centralized to fully decentralized — we call this the spectrum of (de)centralization. Typically, the level of centralization results in a trade-off: the more decentralized the infrastructure, the less trust is required between participants. However, this leads to less efficiency in computing power because additional verification is required. Each position on the spectrum impacts who is allowed to do what on the infrastructure. These user rights can be divided into three types:

1. Read (view the history of activity of the ledger)
2. Write (commit activity to the ledger)
3. Validate (validate authorized transactions and prevent incorporation of unauthorized transactions)

The three main positions along the (de)centralization spectrum, as well as their pros and cons, are described below.

Centralized

A centralized configuration reflects the current status quo: one party controls the infrastructure. This central party alone is able to perform and validate data transactions. Other parties may be provided with read-only rights to review the ledger history on their distributed copy, for example, for auditing or regulatory purposes.

The advantage of such a system lies in its cost-effectiveness. It requires no consensus mechanism and provides full control over the transactions that take place within the chain. This, however, requires participants to trust the central party. Another disadvantage is that the central party is a single point of failure, resulting in a system that is vulnerable to malicious attacks or fraud.

Hybrid

Between a fully centralized and fully decentralized infrastructure sits a permissioned ledger. In this structure, control over a ledger is distributed across a group of trusted peers. Through a consensus mechanism, parties with the right to validate new transactions can update the ledger. Because this group may be small, the involvement of a malicious party could expose the network to the risk of tampering. This risk can be partially mitigated via due diligence procedures regarding the selection of peers who are allowed to join the network. A group of banks that wish to transact with one another could opt for a permissioned ledger, with each or

part of the group being allowed to validate the transactions. Viewing rights could be provided to regulators or other third parties for real-time reporting.

Permissioned ledgers allow semi-trusted parties to share infrastructure among themselves and interact directly with each other, without requiring the establishment of a single trusted party or a separate, distinct infrastructure to coordinate between them. Trading partners in certain markets, or distinct legal entities among conglomerates or joint ventures, could benefit by using this technology: while there is a sufficient level of trust to engage with each other in mutually beneficial trade, there may not be enough to have a single party manage the books and records required to manage the trade effectively.

The advantages have inherent trade-offs, however. The consensus mechanism used in distributed infrastructures relies on a majority of parties to perform according to the rules. In permissioned ledgers for which the number of parties may be small, there is a greater chance for a small group of malicious parties to adversely impact the ledger by validating activity that should not have been validated. While this tampering would be observable by the other participants and could hence be addressed in the real world through legal action, it adds risk and associated costs that should be considered.

Decentralized

In a fully decentralized setup, access to the ledger is public. Anyone is allowed to access the entire history of data transactions, create new transactions and validate transactions into new blocks. Bitcoin is an example of a decentralized ledger. Given sufficient participants, it is unlikely in a well-designed infrastructure that any one party could gain enough control over the network to tamper with transactions.

While a fully decentralized infrastructure may be the ideal end state for establishing decentralized markets that can run independently of trusted parties, certain considerations are impacting their full implementation at present. Some of these issues require an understanding of how public ledgers operate.

While activity recorded in a permissioned ledger is validated by participants on an equal basis, public ledgers require arbitrary parties to validate activity. Consequently, an incentive to validate transactions is required. This incentive is based on most public ledgers' designs, which require tokens to perform functions on the network. Consequently, these tokens' value is based on market demand. When tokens are provided as an economic incentive to participants who assist in the validation process, public ledgers can operate in a fully decentralized manner.

This leads to three considerations.

- Firstly, to engage with the ledger, participants will need to purchase tokens at the market price. As many of these ledgers are very new and the market is still being developed, this price can fluctuate extensively. Consequently, basing a company's operations on a public infrastructure has monetary exchange risk implications that are not present in centralized infrastructures or permissioned ledgers.
- Secondly, the validation process itself for most public

- ledgers can be very inefficient. To prevent activity from being arbitrarily validated and to secure the ledger against attack, validating activity requires the solving of complex calculations. Because the token rewards are available for validating this activity, massive industrial mining operations in the bitcoin world are dedicated to computing the calculations. This has led to a centralization of parties validating the activity and substantial amounts of energy expenditure. More efficient and decentralized validation mechanisms that are being developed have not yet been broadly adopted and can be difficult to adopt, particularly as the large-scale miners have their entire businesses to lose.
- Thirdly, when changes are required for the code that allows the ledger to run, public ledgers, if open to community development, cannot move as quickly or efficiently to upgrade or improve as development that is closely managed.
- While these are not fundamental flaws, they do impact the business case for which infrastructure to use in its current state.

4. Potential applications for harnessing the power of distributed infrastructure technology

Distributed infrastructure technology has many potential applications, through its abilities to disintermediate, reconcile and scale. The following potential applications could harness the power of the technology.

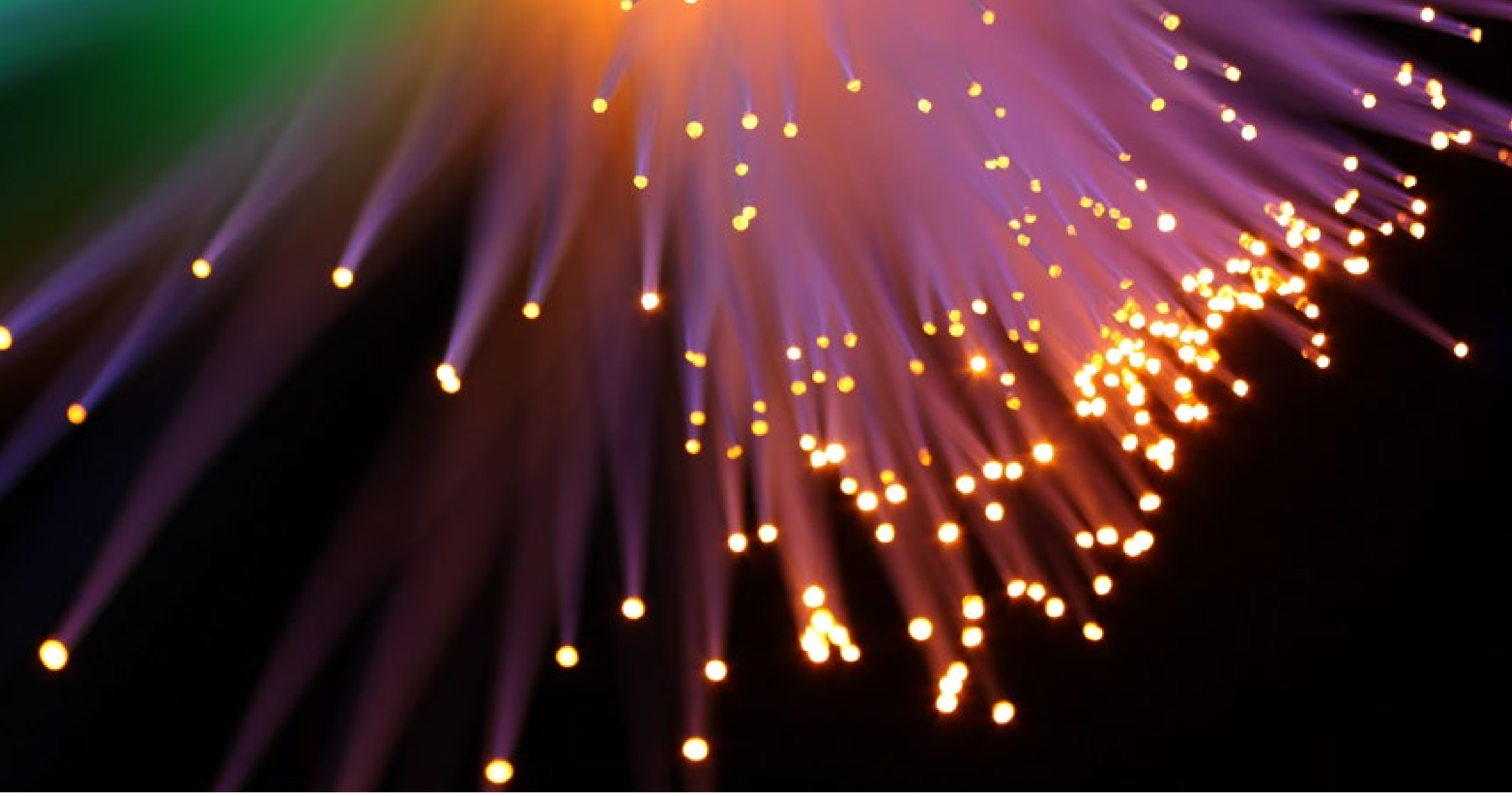
Clearing and settlement

Clearing and settlement has been touted as a promising use case of the technology. While such activities currently require a trusted intermediary to perform the tasks, a distributed infrastructure solution could potentially replace a clearing house or exchange's infrastructure by allowing the activities to be performed directly peer-to-peer. Such an infrastructure in clearing and settlement allows for disintermediation, and, as a result, potential reductions to time and costs. In addition to these benefits, the technology can potentially make audit and tax operations easier, and simplify regulatory reporting by standardizing the recording of historical data; this could ultimately lead to far greater cost savings.

Trade finance and supply chain management

With multiple parties in multiple jurisdictions exchanging multiple physical goods and multiple documents, trade finance – and with it, supply chain management – can be a very complex process. When dealing in cross-border transactions and relationships, the burden on a trusted centralized party can be significant. Consequently, a number of vendors and financial institutions are considering distributed infrastructure as a solution to manage the tracking of products and their associated financing, payment and documentation. With the ability for any party in the chain to record its activity and for any other party to verify the activity, the technology may allow for more efficient, less burdensome trade finance and supply chain management for buyers, suppliers, transporters and financiers.

Closed economies and loyalty points



Other use cases may benefit from the immutable ledger's ability to automatically reconcile multiple sources. Companies that offer credit card rewards programs, through which customers earn redeemable points or miles when purchasing goods, often find it difficult to reconcile the points earned to the points redeemed. Without adequate knowledge of the number of outstanding points and their origins, financial institutions lose considerably not only through poor records of distributed points, but also in the amount of capital required to hold in reserve as well as potential customer intelligence.

Insurance claims management

Distributed infrastructure technology could significantly improve the claims management process. Currently, claims management is a cumbersome process for insurers, involving different parties who exchange lots of paper-based information in handling a claim. This is often centrally coordinated by the insurer itself, resulting in a highly administrative back-office process. A distributed ledger could enable the insurer and various third parties involved in the process to easily and instantly access and update relevant information regarding a claim (e.g., claim forms, evidence, police reports, third-party expertise reports).

Internet of Things applications

When combined with distributed infrastructure technology, the Internet of Things (IoT), can significantly expand the ROI of an asset — its utilization. In manufacturing, for example, a distributed infrastructure-based IoT could power efficient product data-keeping. All information pertaining to a product from the point of manufacture through the time it reaches the end user can be stored on the ledger. This would include product history, revisions, warranty information and expiration date (if applicable), thus making the ledger a trusted source of product data. Via access to the maintenance schedules on the ledger, service requests can be triggered when a product requires maintenance.

Home appliances can be designed to interact with each other to reduce energy consumption based on utilization. As an example, a washer can determine when the detergent supply decreases and automatically refill itself. The machine could also trigger a service request if it detects a component malfunction or a maintenance request based on usage and/or maintenance schedule. Blockchain can be the technology to store all of this information.

Within financial services, IoT can link the performance of a manufacturer to its lending potential. Sensors attached to goods produced at the manufacturing plant would monitor the products' retail sales, a good measure of how the business is doing. Banks can use this information to assist in a lending decision.

Honduras recently implemented blockchain technology to develop incorruptible land registries. Blockchain and distributed infrastructure technology also has potential applications in insurance (the tracking of high-value goods to protect against insurance fraud), trade finance, supply chain management (the effective management and tracing of documents and entities participating in the process) and distributed identity, independent of countries or states.

5. Other factors to consider before applying the technology

As promising as distributed infrastructure seems, like all technology, it is only an enabler. In addition to the question of how to configure the technology, other factors determine whether distributed infrastructure can truly meet a business need.

Regulatory approval can strongly impact the success of any distributed infrastructure implementation. For example, developing a distributed ledger to assist in the clearing and settlement of financial assets may involve custodial considerations, especially if assets are considered to be held on the network at any point. These custodial considerations may require a party to submit to regulatory requirements, which in turn could increase the compliance costs of such a system. On the other hand, a well-designed, standardized, automatically reconciled ledger could provide immediate real-time access to the relevant regulator for all partner institutions on the network. This could prove to save considerable costs and therefore outweigh the additional compliance costs involved in establishing the system.

Any solution will ultimately need to fit into an organization's existing financial ecosystem. Considering this fit beforehand will improve the integration process later, should the concept prove successful. Additionally, many technological partners offer different applications of distributed infrastructure technology. Choosing the partner that fits a business need and desired configuration is vital to the technology's individual success. Data privacy is another technological consideration. For example, while trading assets on an open blockchain may significantly cut costs, it is not a practical solution if all transactions are observable by all parties in the system. Consequently, the design of the technology itself will need to be reviewed depending on the application of choice.

Furthermore, moving any product or service from a centralized to a decentralized mode of operation will have vast impacts on an entire organization. A business' front office, operations, compliance, tax, accounting, legal and technology offices are likely to be involved. Any strategic identification of opportunities to improve a business using this technology will therefore need to consider the end-to-end operational impact of each solution.

6. In conclusion

The blockchain and distributed infrastructure technology are exciting developments that show promise for the financial services industry. While there are significant potential benefits to applying the technology, doing so successfully is a challenge. By thoroughly considering how the technology could meet business needs, and the role of other external and internal factors, firms can significantly improve the likelihood that their initiatives for distributed infrastructure will succeed.

Contacts

Angus Champion de Crespigny
Ernst & Young LLP
+1 212 773 6717
angus.championdecrespigny@ey.com

Imran Gulamhuseinwala
Ernst & Young LLP
+44 20 7980 9563
igulamhuseinwala@uk.ey.com

Matt Hatch
Ernst & Young LLP
+1 415 894 8219
matthew.hatch@ey.com

Nikhil Lele
Ernst & Young LLP
+1 212 773 1996
nikhil.lele@ey.com

Marieke van Eenennaam
Ernst & Young Advisory
+31 6 2125 2736
marieke.van.eenennaam@nl.ey.com

Freek van Dam
Ernst & Young Advisory
+31 6 2908 4142
freek.van.dam@nl.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace
Nearly 46,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 9,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

SCORE no. CK1045

1601-1812228 NE
ED None

ey.com