Tech Explainers

PERMISSIONED BLOCKCHAINS

INTRODUCTION

Cryptocurrencies—bitcoin, ether, XRP, just to name a few—tend to be conflated with the underlying technology that powers them, blockchain. But blockchain can be highly useful as a database structure even detached from cryptocurrencies or the non-fungible token projects used in gaming or art that are built on top of them.

Generally speaking, blockchains can be categorized as permissioned or permissionless, each of which is characterized by different features. Permissionless blockchains—the Bitcoin blockchain, for example—allow anyone to join and rely on incentives to function, and are by nature global, open and interoperable. In contrast, permissioned blockchains require permission to participate and are thus designed for use cases that require privacy and control. Permissioned blockchains are well-suited for enterprise use, especially in highly regulated industries, because access can be restricted to verified members according to business needs, and confidential information can be limited to specific parties while still providing some of the benefits unique to blockchain technology such as transparency and immutability.[1] However, not many understand how blockchain technology can be deployed in this way: while some enterprises in the United States use blockchains, their use is more established and pervasive in other economies where the technology is not as conflated with cryptocurrency.[2] In this Tech Explainer, we will first explain the problem permissioned blockchains can solve and how permissioned blockchains operate theoretically, and then use real-world examples to demonstrate their key benefits.

PERMISSIONED BLOCKCHAINS

A permissioned blockchain provides an environment for distributed parties to update a database, or *ledger*, pursuant to a *consensus protocol* executed through *smart contracts*—all concepts we will address below.[3] It is important to note that while we are exploring the workings of permissioned blockchains at a fundamental level, they are highly customizable beyond the basic shared features and, indeed, this flexibility is one of their key advantages.

---

1 *See, e.g.*, Kate Vitasek, et al., *How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenge*s, HARV. BUS. REV. (Jan. 5, 2022), https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges.

2 *See, e.g.*, Sasha Rosenthal-Larrea, Daniel Barabander & Leslie Liu, *Understanding China's Crypto-Blockchain Dichotomy*, LAW360 (Sept. 6, 2023, 3:15 PM), https://www.law360.com/articles/1711971/understanding-china-s-crypto-blockchain-dichotomy.

3 The descriptions in this technology explainer are loosely based on the workings of Hyperledger Fabric, an open source platform for permissioned blockchains. While the specific protocol for various permissioned blockchains may differ, the basic concepts we introduce should be generally applicable to the workings of any particular permissioned blockchain.

Permissioned Blockchains as an Alternative Solution to Transaction Friction

In many cases, data is stored where it is created, but other parties also need access to that data to complete transactions. When each party maintains its own siloed database, there is friction in communicating data between the various databases. There are two solutions to deal with this friction. The first is centralization. The various parties can put a trusted party in charge and everyone will integrate their systems with that party. In many scenarios, this is an acceptable outcome, especially when there is an identifiable trusted party. A benefit of this system is efficiency: after all, only one database needs to be maintained. Most of our daily interactions on the internet now are on centralized systems that rely on a single administrator (usually the company operating the particular website), often called Web2.

But what happens in a scenario where it is not possible to identify a trusted party, and the participants don't trust each other enough to give each other control over their databases? This is where blockchain can shine because it provides an interoperable system where data can be transparent and easily accessible to multiple parties without sacrificing security and authenticity.[4]

Blockchain Basics

A blockchain is a decentralized, immutable ledger on which transactions are recorded—however, blockchain can support complex functionality, which is achieved through the use of *smart contracts*. Despite its name, a smart contract is not a legal contract; rather, it is functional code that is stored on the blockchain and that produces a certain result given certain inputs. For example, a simple smart contract can contain series of "if-then" statements that are triggered when pre-defined conditions are met.

A fundamental feature of blockchain is its immutable nature, which provides for a layer of trust among participants. Instead of storing data on a centralized server, blockchain achieves this layer of trust through identical blockchains, each one of which is referred to as a *ledger* on which transactions are recorded, or "written." Each participant in a given blockchain stores and updates their own ledger. To ensure each participant has an identical ledger, the blockchain has a number of participants who validate proposed transactions, include validated transactions in blocks, then broadcast the updated blocks to the entire network. Each ledger, which contains the same transactions in the same order, immutably stores information of all transactions that have occurred. The blockchain is composed of multiple sequential "*blocks*," with each block containing a bundle of transactions, including information about the newest transaction but also information about the prior blocks in the sequence, which means that the blockchain contains a record of every previous version itself that has existed.

The specific bundle of transactions in a particular block is collectively represented as a *hash* that distinguishes each block as unique. A hash is a one-way function that takes data and converts it to a unique string of characters that corresponds only to that specific set of data, and that cannot be used to identify the underlying data—in very simplistic terms, the function is an encoder and the hash is the resulting codified representation of the underlying data. Unlike other types of code, though, which can be decoded, the hash flows only in one direction: once data is "hashed," the resulting output, the "hash," cannot be decrypted or altered.

4 While blockchain is the most widely known form of decentralized ledger technology, it is not the only one. Others, such as Directed Acyclic Graphs, also function without the need for a central administrator. *See, e.g.*, IOTA FOUND., IOTA FOR BUSINESS: PERMISSIONLESS INNOVATION, https://files.iota.org/comms/IOTA _ for _ Business.pdf.

A particular block, in its hash form, includes information about the newest transaction. That is, each block includes information about all of the prior blocks in the blockchain and therefore information about every prior transaction. If someone in the present moment tried to sneak in a record of a falsified prior transaction—for example, changing the data for a transaction that took place ten transactions ago—the data for the "bundle of transactions" in each of the prior nine blocks on the blockchains would be altered, *and thus the hash for each of those prior blocks would be different than what appears on each participant's ledger.* It would immediately be apparent to all involved that a modification had been attempted and the blockchain would reject the new false ledger entry. This ensures that once a transaction has been added to the ledger, it cannot be modified. Because information cannot be changed after the fact and the entire history is available on a blockchain, participants can easily determine the provenance of information. The parties do not need to rely on a central authority for transactions to occur: instead they have a trusted immutable record to refer to.

Another fundamental feature of decentralized transactions is the removal of centralized intermediaries, which relies upon the use of *digital signatures*. To produce a signature, each participant is assigned a private key, which is kept confidential, and a public key, which is publicly available. A digital signature is a mathematical function that uses the *private key-public key* pairing to verify the authenticity of a specific transaction. Thus, a unique signature is generated depending on the private key and the specific transaction. Using cryptographic methods, others can verify the validity of the transaction using a participant's public key without knowing the private key. Digital signatures underlie every blockchain, providing for a cryptographic verification system. Just like in a permissioned blockchain, there are digital signatures on the permissionless blockchain, with the only difference being who is allowed to write and verify the signature.

Fundamental Features of Permissioned Blockchains

While both permissioned and permissionless blockchains can solve the problems of trust, immutability and transparency, permissioned blockchains have several properties that are especially desirable for use by private companies in connection with the operation of their businesses. One of the biggest differences between permissionless blockchains such as the Bitcoin or Ethereum blockchain and the permissioned ones we will describe here is how parties validate a transaction, or how a new block is added to the blockchain. In other words, each decentralized system contains a requirement that *consensus* between participants be reached on which transactions are valid before changing the state of the blockchain. There are a variety of mechanisms for achieving this, such as, in many permissionless systems, proof of work and proof of stake. Permissioned blockchains involve other consensus mechanisms that can be more tailored towards the specific business scenario.[5]

In a permissionless blockchain that uses the proof of work consensus mechanism, after a participant engages in a transaction using their private key, they broadcast this transaction to the entire network as a request for inclusion in the next block. Rather than trusting any particular party to write a new transaction to the blockchain, a system is put in place that rewards participants—or *nodes*—on the blockchain, who have no direct knowledge of the new transaction or the parties to that transactions, for performing calculations in order to guess a pre-defined random number. The node that guesses that random number first, once such guess is validated by other network participants, can add the transaction to the blockchain as part of a new block and can receive a reward for doing so (or be punished in the form of wasted resources for acting dishonestly).

---

5 *See, e.g.*, *Consensus in Hyperledger Fabric*, GEEKSFORGEEKS, https://www.geeksforgeeks.org/consensus-in-hyperledger-fabric.

With permissioned blockchains, however, the organizations involved in validating a transaction are frequently parties to the transaction. In a permissioned blockchain, each participant has a defined *role*, and each role has certain *permissions* associated with it. Importantly, *permissions* define what parties can do on the network (including who can access what data, who can record which transactions and who can validate the transactions) and the rules can be tailored for any type of business scenario. The identity of participants in a permissioned blockchain are also generally not anonymized, which enhances security. Thus, the roles participants have on permissioned blockchains often mirror relationships between parties in the real world.

USE CASES

Even with a description of their basic functioning, it can be difficult to envision exactly how businesses might use permissioned blockchains in real-world scenarios. Through the examples below, we highlight some key benefits of blockchain, including interoperability, traceability, efficiency and privacy.

Supply Chain

Supply chain operations typically involve multiple parties and multiple, simultaneously occurring transactions, in situations where the integrity and provenance of data is crucial. Upon delivery of an item, certificates are often transmitted that purport to identify the authenticity of the item, for instance, by certifying a food product as organic. Fake certificates would endanger the entire product chain, leading to issues of safety and trust. Traditionally, each party in a supply chain maintains a siloed database of key information containing data relevant to its specific role. This fragmentation creates a problem: with no standardization, integrating with each system to obtain information is highly cumbersome. It would also be very complicated when inconsistencies arise between databases: which database should control?

Examples of supply chain enterprises using blockchain solutions abound, from Walmart tracing food and freight to Honeywell facilitating trade of used aerospace parts. Walmart has used blockchain in a variety of fields, to great success.[6] Walmart's supply chain tracing allows for food safety, food system efficiency and market transparency. In the United States, tracing the provenance of sliced mangoes sold in a Walmart store went from almost a week to 2.2 seconds.[7] In China, Walmart engaged in a larger scale project of tracing pork. In 2016, Walmart collaborated with local providers and regulators to develop a safer food ecosystem. After each participant uploaded certificates of authenticity to the blockchain, the blockchain connected and verified all parties along the supply chain, from suppliers to shippers to consumers.[8] By 2020, consumers were able to scan unique QR codes for more than a hundred products to obtain information on how the good was sourced and shipped.[9]

---

6 Zifa Mae, *Walmart & Blockchain: New Era of Supply Chain Management*, CHANGELLY BLOG (Apr. 7, 2023), https://changelly.com/blog/walmart-blockchain.

7 Hyperledger Found., *How Walmart Brought Unprecedented Transparency to the Food Supply Chain With Hyperledger Fabric*, https://www.hyperledger.org/case-studies/walmart-case-study.

8 Archana Sristy, *Blockchain in the Food Supply Chain—What Does the Future Look Like?*, WALMART GLOB. TECH (Nov. 30, 2021), https://tech.walmart.com/content/walmart-global-tech/en _ us/news/articles/blockchain-in-the-food-supply-chain.html.

9 EUROPEAN UNION CHAMBER COMM. CHINA, *Walmart China Blockchain Traceability Platform* (Dec. 14, 2020), https://www.europeanchamber.com.cn/en/members-news/3303/walmart _ china _ blockchain _ traceability _ platform.

In 2021, Walmart Canada began using DL Freight, a permissioned blockchain, to manage invoices from and payments to 70 freight carriers. Transporting massive amounts of goods across borders was a highly complicated project: over 200 data points needed to be factored into each invoice. Each shipload required tracking data points such as "stop locations, gallons of fuel, and temperature updates that need to be independently calculated and incorporated into each invoice."[10] Prior to adopting blockchain, more than 70% of the invoices required reconciliation. The crux of the problem was that Walmart and its carriers all used independent information systems that were not interoperable. Thus, reconciliation needed to be performed manually, leading to a labor-intensive and time-consuming process that was riddled with inconsistencies.[11]

Using DL Freight has reduced the percentage of disputed invoices from more than 70% to less than 1%, and the disputes with discrepancies are easily flagged and resolved.[12] The privacy of permissioned blockchains allowed Walmart to meet industry-grade security requirements.[13] Further, the transparency provided by the blockchain has also allowed for immense operational improvements. With detailed information for each stage visible on-chain, blockchain allowed Walmart to determine the most efficient routes, even at the most granular level. It can now optimize efficiency down to the smallest details, from choosing the best vehicle, route and load weight to the optimal time to travel.[14]

Likewise, since 2018, Honeywell's use of permissioned blockchain in the aerospace industry has exemplified the technology's advantages of transparency and interoperability in a heavily regulated industry. Once plagued by bulky documentation from various facilities that were not interoperable, blockchain has allowed aircraft records to be generated and saved on a digital and searchable ledger.[15]

After a plane retires, there is enormous demand for valuable parts that can be reused, such as engines. Resale requires requisite certification from multiple agencies, including the U.S. Federal Aviation Administration, as well as detailed repair records. Airlines typically use dozens of repair facilities with siloed databases. In the process, they deal with physical paperwork that is critical to determining a part's value.[16] When done on paper, this process is highly intensive and prone to error. With blockchain, customers are privy to important data describing the entire lifecycle of each part, such as the number of hours it was in service, all repairs made and all previous owners of the part.[17] Each authenticated user on the blockchain, such as customers and suppliers, possesses a copy of the immutable database and is able to access its contents in real time. When a physical document is missing, parties can retrieve the data from the ledger using unique serial numbers.[18] Regulatory agencies can also easily verify the records for each part, streamlining the regulatory oversight process.

---

10 Vitasek, et al., *supra* note 1.

11 *Id.*

12 *Id.*

13 *Id.*

14 *Id.*

15 HONEYWELL, *Honeywell Uses Blockchain To Digitize Aircraft Records, Parts Pedigree Data* (Aug. 4, 2020), https://www.honeywell.com/us/en/press/2020/08/honeywell-uses-blockchain-to-digitize-aircraft-records-parts-pedigree-data.

16 MILITARY AEROSPACE, *Honeywell Uses Blockchain to Digitize Aircraft Records, Parts Pedigree Data* (Aug. 6, 2020), https://www.militaryaerospace.com/commercial-aerospace/article/14231597/aircraft-digital-records-parts-pedigree-blockchain.

17 HYPERLEDGER FOUND., *Honeywell Aerospace Creates Multimillion Dollar Online Parts Marketplace With Hyperledger Fabric* (Nov. 13, 2019), https://www.hyperledger.org/blog/2019/11/13/honeywell-aerospace-creates-multi-million-dollar-online-parts-marketplace-with-hyperledger-fabric.

18 *Id.*

Finance

Currently, financial institutions mainly operate siloed databases. With each party operating a different database in a sector that requires accurate transfers of funds and ownership, blockchain allows for interoperability, transparency and efficiency. In 2017, China CITIC Bank spearheaded a blockchain network among domestic banks that allowed letters of credit—guarantees that sellers will be paid for a large transaction—to be standardized and traced more effectively in the banking system.[19] In January 2023, the European Investment Bank issued a £50 million three-year floating bond using a combination of permissioned and permissionless blockchains.[20] The permissioned blockchain provides a record of digital ownership and allows verified participants to manage the floating rate bond and its lifecycle events.[21] At the same time, the permissionless blockchain, used for information purposes, provides increased transparency to the market regarding holdings of the digital bonds on an anonymized basis.[22] Use of blockchain for the bonds allowed for significantly lower issuance cost than traditional methods and simultaneous delivery-vs-payment settlement.[23]

Healthcare

In healthcare, a major problem is siloed databases leading to incomplete views of medical histories. Because a typical patient sees multiple providers during her lifetime, pieces of her medical records could be in the hands of her primary care physician, her specialists, her hospital system or her health plan.[24] Medical errors can result from uncompleted actions or errors of omission in patient records across poorly coordinated disparate health systems.[25] Without interoperable IT systems, different organizations receive medical records transferred on paper, which could result in the loss of vital information or life-threatening inaccuracies. At the same time, the security and privacy of medical records is highly important.

Blockchain produces a single and accurate view of a patient's record while allowing patients transparent access to and control over their own data. In March 2023, Avaneer Health launched a permissioned blockchain with a number of major health providers to allow real-time access to holistic medical records.[26] To operate this blockchain, patients, providers and third-party vendors first commit data to

---

19 Joshua Althauser, *Chinese Banks Launch First Blockchain-Enabled Credit Applications*, COIN TELEGRAPH (July 29, 2017), https://cointelegraph.com/news/chinese-banks-launch-first-blockchain-enabled-credit-applications.

20 EURO. INVESTMENT BANK, *EIB Issues Its First Ever Digital Bond in Pound Sterling* (Jan. 31, 2023), https://www.eib.org/en/press/all/2023-030-eib-issues-its-first-ever-digital-bond-in-british-pounds.

21 *Id.*

22 *Id.*

23 ROY CHOUDHURY, ET AL., IMPACT OF DISTRIBUTED LEDGER TECHNOLOGY IN CAPITAL MARKETS 12, 185 (2023).

24 Shania Kennedy, *Exploring Decentralized Architecture Networks in Healthcare*, TECH TARGET (Jan. 9, 2023), https://healthitanalytics.com/features/exploring-decentralized-architecture-networks-in-healthcare.

25 JOHNS HOPKINS MED., *Study Suggests Medical Errors Now Third Leading Cause of Death in the U.S.* (May 3, 2016), https://www.hopkinsmedicine.org/news/media/releases/study _ suggests _ medical _ errors _ now _ third _ leading _ cause _ of _ death _ in _ the _ us; STL PARTNERS, *5 Blockchain Healthcare Use Cases in Digital Health*, https://stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases.

26 AVANEER HEALTH, *Avaneer Health Launches Its Decentralized Network and Platform to Transform Healthcare Administration* (Mar. 13, 2023), https://avaneerhealth.com/press/avaneer-health-launches-its-decentralized-network-and-platform-to-transform-healthcare-administration; Avaneer Health, *What Is Blockchain?* (Aug. 2, 2022), https://avaneerhealth.com/blog/what-is-blockchain.

the chain and, using private keys, allow it to be discoverable based on permissions set by each party.[27] The parties connected to the network do not have to build direct connections to other members. When a party requires data, it sends a request to the blockchain, which verifies the party's permissions. In this way, data stays with the originator and does not need to be aggregated by outside parties.[28] Critically, data also remains private and decentralized, as it is only shared with approved parties based on permissions set by each party.[29]

The blockchain connects patients and providers on a single, seamless network. Reduced touchpoints means there are fewer chances of security failure, as well as reduced IT and administrative costs.[30] With an immutable ledger, the blockchain also allows for transparency in each step of the healthcare process. Moreover, taking advantage of the security features of decentralized data, Avaneer is exploring the possibility of combining permissioned blockchain with generative AI.[31]

CONCLUSION

Despite the many potentials of blockchain, the technology is still in nascent stages for business use. Many challenges lie ahead as blockchain develops, key among them inertia and unfamiliarity with how the technology operates.[32] Buy-in is hard to come by, and successful examples of blockchain use tend to begin as consortiums of large stakeholders. However, as this Tech Explainer lays out, blockchain provides key advantages such as interoperability and transparency to transactions in multiple sectors. As leading industry players experience the advantages of blockchain, others could be more inclined to explore the technology. Importantly, blockchain is not a panacea. Transactions that are already highly efficient might not need the overhaul, while those that are too complicated might be better resolved with a centralized entity.

---

27 ORBOGRAPH, *Blockchain Solves Interoperability Challenges According to Avaneer Health CEO*, https://orbograph.com/blockchain-solves-interoperability-challenges-according-to-avaneer-health-ceo.

28 Stuart Hanson, *Interoperability: Past, Present, and Future*, MEDCITY NEWS (June 1, 2023, 6:14 PM), https://medcitynews.com/2023/06/healthcare-interoperability-tefca-fhir.

29 AVANEER HEALTH, *The Missing Link in Generative AI for Healthcare* (Sept. 15, 2023), https://avaneerhealth.com/blog/the-missing-link-in-generative-ai-for-healthcare.

30 ORBOGRAPH, *supra* note 27.

31 AVANEER HEALTH, *supra* note 29.

32 *See, e.g.*, Irving Wladawsky-Berger, *Why Are Enterprises Struggling With Blockchain?* (Jan. 5, 2023), https://blog.irvingwb.com/blog/2023/01/why-are-enterprises-struggling-with-blockchain.html.

David J. Kappos
+1-212-474-1168
dkappos@cravath.com

Sasha Rosenthal-Larrea
+1-212-474-1967
srosenthal-larrea@cravath.com

Leslie Liu
+1-212-474-1297
lliu@cravath.com

Cravath, Swaine & Moore LLP

NEW YORK

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
T+1-212-474-1000
F+1-212-474-3700

LONDON

CityPoint
One Ropemaker Street
London EC2Y 9HR
T+44-20-7453-1000
F+44-20-7860-1150

WASHINGTON, D.C.

1601 K Street NW
Washington, D.C. 20006-1682
T+1-202-869-7700
F+1-202-869-7600