Private and confidential transactions with Hyperledger Fabric

How this open source blockchain framework ensures custom levels of privacy and confidentiality

Elli Androulaki
Sharon Weed Cocco
Chris Ferris

May 11, 2018

Discover the mechanisms provided by Hyperledger Fabric to accommodate different levels of privacy and confidentiality for different network needs.

In industries of every stripe, news of significant data breaches seems to surface on a weekly basis. This vulnerability has elevated awareness of how critical it is to preserve the privacy of user data. *Privacy* is defined as the right of each individual or legal entity to control the degree to which they will share their personal or business information with their environment.

> *" In transaction systems, such as blockchain networks, privacy is frequently achieved by mechanisms that enforce the confidentiality of data and the anonymity of transaction participants. "*

Data confidentiality mechanisms ensure that individuals or organizations are prevented from accessing data that they are not authorized to access, such as classified information of other organizations' transactions. *Anonymity* requires that participants of transactions are concealed.

Blockchain technology has inspired novel techniques to help address privacy concerns in a decentralized setting. However, as different blockchain systems come with different privacy features and models, each use case will dictate the best approach or blockchain technology required.

Privacy in public vs. private blockchain systems

Public (in other words, permissionless) blockchain systems like Bitcoin were the first to face privacy challenges. Participation in these systems is open to anyone and, as such, user behavior is shielded behind virtual pseudonyms (or "addresses") that users generate to represent

themselves in their transactions. On the other hand, transaction details are in the clear, and available on the public ledger of the system.

In certain enterprise use cases, government regulations require understanding who is involved in the transactions, thus preventing the use of public blockchain systems (such as Bitcoin) where identities are pseudonymous. Further, the public availability of the content of transactions in such systems can be problematic for numerous business use cases. Why? Imagine a business obtaining computer parts from a vendor. Given the large volume of computer parts purchased, the supplier provides a discount to the business when trading the asset for currency. For the supplier, the actual discount is sensitive business information, as the supplier may not want to provide the same discount to businesses who purchase lower volumes.

As a response to these challenges, a couple of blockchain systems have been introduced, built on top of Bitcoin. Blockstream's Confidential Transactions and Assets is a prominent example. It allows pseudonymous transfer of coins and assets without leaking the actual value of the coins or type of assets that are being exchanged. ZeroCash is another example. It's an open network that offers stronger privacy where — in addition to concealing the value of the assets exchanged — it conceals the owner of the coins as well as the actual transaction graph. However, as all these systems target open networks, they offer unconditional privacy.

Permissioned blockchains have emerged as an alternative to public ones to address enterprise needs for having known and identifiable participants. They've achieved the scale, confidentiality, and privacy necessary to enable enterprise applications.

3 privacy mechanisms in Hyperledger Fabric

Hyperledger Fabric is a permissioned blockchain, which means it is equipped with a membership infrastructure that enables participants of the network to both strongly authenticate themselves in transactions, and prove authorization to perform a variety of system operations, such as reconfiguration. Starting from its permissioned nature, Hyperledger Fabric offers mechanisms to accommodate multiple flavors of privacy, depending on the use case.

1. Channels in Hyperledger Fabric

Hyperledger Fabric's channel architecture can offer privacy in certain cases.

> *" A channel is like a virtual blockchain network that sits on top of a physical blockchain network with its own access rules. Channels employ their own transaction ordering mechanism and thus provide scalability, ultimately allowing for effective ordering and partition of huge amounts of data. "*

Channels in Hyperledger Fabric are configured with access policies that govern access to the channel's resources (chaincodes, transactions, and ledger state), thus preserving the privacy and confidentiality of information exclusively within the nodes that are in the channel. Channels achieve

better quality of robustness when a node is down given alternate paths to get to the destination, while also providing scalability allowing for effective sharing of huge amounts of data.

From a privacy perspective, channels are useful in cases where a subgroup of the blockchain network's participants have a lot of transactions in common (enough to justify the creation of a new broadcast order channel), and these transactions can be processed with no dependency on state controlled by entities outside this group.

How CLSNet is using channels

CLSNet is a revolutionary FX product that addresses the wider post-trade processing needs of FX market participants. Built on a distributed ledger technology platform, CLSNet covers trades settling outside core CLS Settlement while introducing standardization and automation for the entire FX market.

CLSNet utilizes key privacy and confidential capabilities in Hyperledger Fabric to achieve their business objective. Learn more in this video.

Bilateral business relationships with a heavy volume of transactions can meet their privacy requirements via channels. Take the example of the computer parts supplier. The supplier could establish a different channel with each business partner to serve their bilateral business relationship. Of course, the rate of transactions should be high enough and the number of business partners (and resulting channels) should be low enough for this use case to also preserve the scalability advantages of the network's channel architecture. The channel access configurability allows for preserving both the privacy of the supplier and each of its partners through shielding the entire transactions of theirs from parties outside this channel.

Channels can be further used in combination with private transactions and zero-knowledge proof technologies as described below to strengthen privacy and confidentiality.

2. Private transactions in Hyperledger Fabric

Private transactions offer transaction privacy at a more fine-grained level than channels.

> *" Verified.Me by SecureKey Technologies relies on strong privacy and confidentiality requirements. The solution depends on minimizing data disclosure and retention to appropriate parties, while still retaining the evidence of actions taken in the network. This balance is fundamental, and the foundation is provided in Hyperledger Fabric with the combination of Channels and Private Transactions. Watch the video to understand the real business value at work utilizing Hyperledger Fabric technology. "*
>
> Greg Wolfond, CEO, SecureKey Technologies

To view this video, , please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

The database storing the private data is updated alongside the public ledger as transactions containing references to private data are committed. In fact, the hashes on the public ledger serve as verifiable proof of the data. Private transactions can be combined with anonymous client authentication (see next section) to avoid leaking the connection between the identity of the transaction's creator and the ledger stored (hashed) data.

This feature is especially useful in cases where, for regulatory or legal reasons, private data is not allowed to reside off the premise of the parties involved in the transaction. Consider an example in the healthcare sector where a patient's health information should be released only for a specified amount of time. For example, a patient's prescription history may be made available to a specialist for a period of time before a specific surgery occurs. Private transactions would ensure data confidentiality in only allowing the patient and the specialist to see the information for a specified amount of time while also recording the hash of the data as evidence that the transaction occurred. Privacy is achieved in that there is control over who can access the actual sensitive data. If anonymous client authentication is used in addition to this (see the next section), stronger privacy would be offered as the identity of the entity that introduced or updated the (hashed) record will also be concealed.

Private transactions should be used with care in cases where the pattern of private data updates is also sensitive information and could be used to derive the actual private data. Although Hyperledger Fabric architecture prevents unauthorized access to the actual private data, shared ledger participants can still see when a private data (hashed) entry is modified. In the previous example, if a private data entry represents the number of visits by a specific patient to a hospital (assuming the patient has regular weekly meetings with his or her doctor), then patterns of updates to this entry could provide information about the reason for that patient’s visit to the doctor (for example, that the patient suffers from chronic disease).

While private transactions protect the actual private data from being directly accessed by unauthorized parties, they do not prevent public ledger participants from detecting when this private data is being modified. Private data hashes occupy key-value entries in the ledger state, whose changes are publicly available.

Also, private transactions do not conceal the parties who are allowed access to the private data. This information is available on the ledger for private data dissemination to take place properly.

Finally, private transactions would need to be accompanied with anonymous client authentication mechanisms (described in the next section) to avoid leaking the connection between the identity of the transaction's creator and the ledger stored (hashed) data.

3. Zero-knowledge proof (ZKP) technologies in Hyperledger Fabric

Zero-knowledge proof primitives enable a party who possesses a secret (the prover) to prove to another party (the verifier) that its secret satisfies a certain set of properties (knowledge) without revealing the actual secret (zero-knowledge).

> *“ A zero-knowledge proof (ZKP) allows a “prover” to assure a “verifier” that they have knowledge of a secret without revealing the secret itself. It's a way to show you know something that satisfies a statement without showing what you know. ”*

Here's a basic example to demonstrate the power of ZKP. If you show your ID to the bouncer at a bar, you end up revealing your name, address, and age. If you used ZKP, you would be able to transform your ID into another form that would preserve the fact that it is a valid ID and the fact that you meet the bar’s age requirements, while concealing your name, address, and exact age.

Two privacy aspects of Hyperledger Fabric will be achieved using ZKPs: Anonymous client authentication with Identity Mixer, and privacy-preserving exchange of assets with Zero-Knowledge Asset Transfer (ZKAT). We'll cover both in the next sections.

Anonymous client authentication with Identity Mixer

Identity Mixer is available in the Hyperledger Fabric 1.1 tech preview (and coming as a release feature in Hyperledger Fabric 1.2). It leverages ZKP to offer anonymous authentication for clients in their transactions. ZKP protocols take place between the Fabric client whose secret is its actual identity — and any attributes associated with it — and the rest of network entities, such as its peers. These entities wish to verify that the creator of a transaction is a member of a particular organization (known as a "membership proof"), or that it is in possession of a specific set of attributes (known as "selective disclosure of attributes").

In both cases, the protocols guarantee that nothing is revealed about the client’s identity beyond whether the corresponding statement is true.

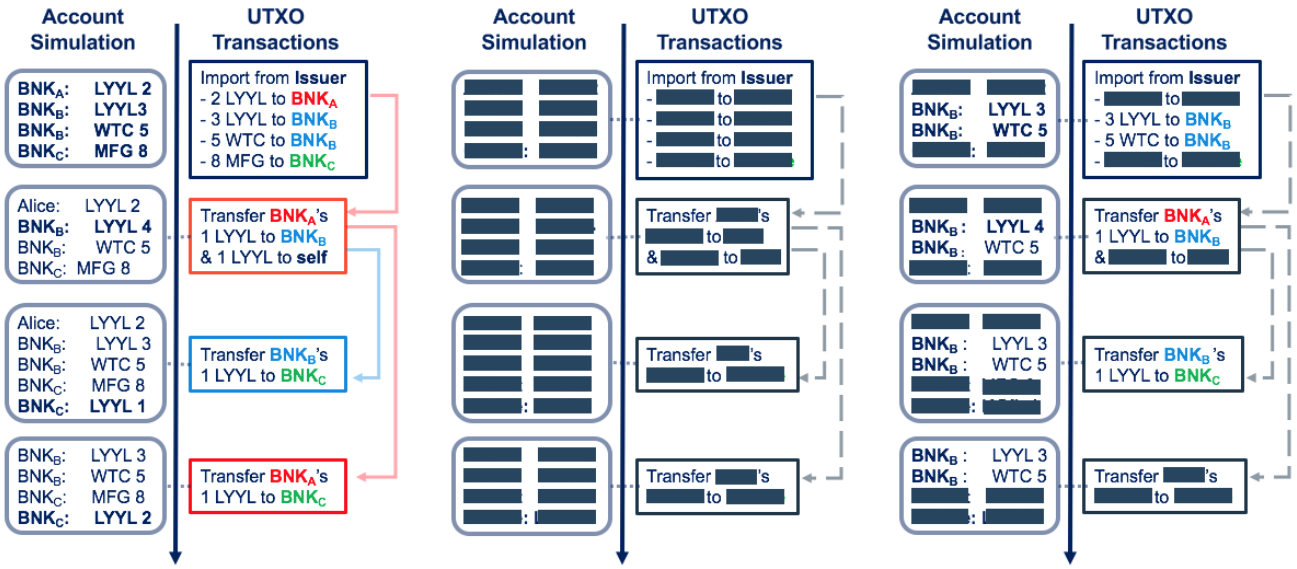
Privacy-preserving exchange of assets with Zero-Knowledge Asset Transfer (ZKAT)

In an upcoming release, Hyperledger Fabric will integrate ZKP into a wider range of applications targeting asset management. Demonstrated at Consensus 2018, the Hyperledger Fabric community showed the next evolution and use of ZKP to accommodate privacy-preserving asset management with audit support (also known as Zero-Knowledge Asset Transfer, or ZKAT). It allows transactors to issue assets and request transfer of their assets without revealing anything to the public ledger for the assets being exchanged beyond the fact that the transfer complies with the asset management rules (that each asset is transferred at its owner's request, and there is no new value created through the transfer). ZKAT is built on top of anonymous authentication mechanisms offered by Identity Mixer.

Unlike other privacy-preserving asset management systems for blockchain, ZKAT is tailored to the needs of enterprise networks. In particular, auditability of the privacy-preserving transactions is a crucial differentiator from other schemes available. Each user is assigned a specific auditor who is entitled unlimited access to all the transactions of that user. The auditors are passive; they

may come in afterwards and extract the confidential information of all transactions the audited user is involved in, but they cannot access the data for any other party.

Three privacy asset management models (based on unspent transaction output model exclusively) are currently adopted by existing blockchain systems. You can see them illustrated in the next figure, where three banks (Bank A, Bank B, and Bank C) trade three types of assets on the blockchain (Loyyal points, Water Canary, and MUFG ones).



In the figure, the model on the left has no privacy mechanism. The model in the middle supports full privacy, concealing the identities of transaction participants and traded assets details. The model on the right demonstrates the secure auditing capability of ZKAT the auditor assigned to a specific Bank is allowed unrestricted access to all transactions involving this bank.

Audit-enabled privacy is useful particularly in financial use cases. Banks make money by lending at rates higher than the cost of money they acquired. As a result, if a bank were to use a blockchain network with this advanced ZKP capability applied, they would want to be able to exchange assets (money) and record the corresponding transactions in the shared ledger without revealing the fact that they are transacting, with whom they transact, or the amount of the assets they are exchanging in their transactions. Failure to do so would clearly compromise their confidentiality regulations, and expose their business models.

With zero-knowledge proof, transactions containing verifiable proof that the asset (money) is exchanged are available on the ledger, without revealing the lending rates or the quantity and parties a bank trades, allowing the bank at any particular time to understand the liquidity of what they have in cash. The additional advantage with Hyperledger Fabric is they can now be audited based on ZKAT.

Differences from other blockchain technologies

Zero-knowledge proof protocols for asset management implemented on Hyperledger Fabric permissioned blockchains are state of the art. Strong privacy is supported where not only the anonymity of transaction participants is preserved but also complete unlinkability of the assets transferred from one party to the other (that is, UTXO graph concealment).

In addition, these protocols are tailored to the needs of permissioned systems. The long-term identities of individual users are considered, providing strong accountability and non-repudiation of user participation in transactions, and offering strong and secure auditing features on the privacy-preserving transactions that are announced in the blockchain. Hyperledger Fabric protocols support an audit model where auditors are assigned to one or more users in the system but are not involved in transactions. These protocols guarantee that auditors will later be able to audit transactions of the users assigned to them, given only the transactions logs stored in the blockchain.

On a more technical level, protocols in Hyperledger Fabric rely on standard cryptographic assumptions and exhibit a lightweight setup that can be easily decentralized. Last but not least, these demonstrate constant transaction creation and validation times that do not depend on the number of transactions already submitted to the ledger.

Conclusion

Over the past several years, blockchain has become recognized as a game-changer for many industries. The year 2018 will continue to bring state-of-the-art privacy and confidentiality enhancements, as more permissioned DLTs move into production. In this article, we've discussed privacy features in existing blockchain systems and the use cases they're best suited to, as well as new enhancements soon to be available in Hyperledger Fabric.

Depending on your network's needs for privacy and confidentiality, application developers may chose to implement Hyperledger Fabric channels, private transactions, and/or different levels of zero-knowledge proof, including anonymous client authentication with Identity Mixer and privacy-preserving asset management with audit support (Zero-Knowledge Asset Transfer, ZKAT). Hyperledger Fabric is bringing a new level playing field to permissioned enterprise blockchains.

Next steps

- IBM Blockchain runs on Hyperledger Fabric. Let the new IBM Blockchain Platform Starter Plan (free while in beta) help you **kick-start your blockchain network**.
- Once you launch your Starter Plan instance, then **deploy a sample network and run your first blockchain application**.
- Learn how to create business networks from scratch using Hyperledger Composer in our popular series, **Hyperledger Composer basics**, by Steve Perry.

- Stay in the know with the monthly Blockchain Newsletter for developers. Check out the **current issue** and **subscribe**.

- Check out the many **code patterns**, which provide roadmaps for solving complex problems with blockchain technology, and include architecture diagrams, code repos, and additional reading.

- Stop by the **Blockchain Developer Center**. It's your source for free tools and tutorials, along with code and community support, for developing and deploying blockchain solutions for business.