April 2023

Configuring and Auditing VPC Network Traffic Using a Private Hyperledger Blockchain

Kishore Jagannath

Configuring and Auditing VPC Network Traffic Using a Private Hyperledger Blockchain

ABSTRACT

Organizations with cloud computing operations set up connectivity between their networks to facilitate secure, low cost communication. Such inter-organization connectivity opens up network boundaries to applications running in networks that belong to cross-border business units or organizations. Participating organizations require secure, tamper-proof audit trails of communications across network boundaries without relying on the cloud provider. This disclosure describes blockchain-based techniques to provide trust, immutability, and independent verifiability of audit logs of network traffic between organizations. A permission-based blockchain built using hyperledger fabric is provided to enable efficient audit of network communication between networks belonging to different parties or entities. A private blockchain network for a VPC (virtual private cloud) network connection is configured to efficiently store network traffic data as a distributed ledger.

KEYWORDS

- Virtual private cloud (VPC)
- Virtual private network (VPN)
- Blockchain
- Hyperledger fabric
- Cloud interconnect
- Cloud audit
- Network audit
- Smart contract

BACKGROUND

Organizations with cloud computing operations set up connectivity between their networks to facilitate secure, low cost communication. The network can span across networks belonging to different organizational units and/or across organizations. Such inter-organization connectivity provides access to workloads via private IP addresses, thereby opening network boundaries to applications running in networks that belong to cross-border business units or organizations. Organizations that participate in inter-organization networking require secure, tamper-proof audit trails of communications across network boundaries. Also, organizations have a requirement to be able to independently verify the authenticity of network logs without relying on the cloud provider. Proper auditing of the inter-network communication is essential.

Today, network traffic is logged using traditional, log-based methodologies. For example, virtual private cloud (VPC) flow-logs into the cloud provider can be used to log the traffic flow between networks. However, cloud providers completely own these logs. It is not possible for their enterprise customers to verify the authenticity of the logs. Conventional logging techniques do not provide guarantees of trust, reliability, and tamper-evidence. Networks that connect different parties, e.g., organizations or business units, may reside in different data centers or cloud providers, and require a trusted and tamper-proof mechanism to audit the traffic flowing between them. Aside from network communications, organizations may also need to monitor applications that are accessed, source machines initiating communication, protocols used, etc.

Networks can be connected across organizations or business units in various ways, for example:

- **Cloud interconnect:** Connect two networks across data center boundaries either directly or via a third-party provider.

- **Virtual private network (VPN):** An encrypted IPSec connection across networks facilitates secure private communication.
- **Peering:** Networks are made peers to facilitate private connections across them.

Hyperledger fabric is an enterprise blockchain to configure private or permission-based blockchain networks. It facilitates the creation and deployment of smart contract programs that can store immutable data across organizations and peers within the hyperledger fabric network.

DESCRIPTION

This disclosure describes blockchain-based techniques to provide trust, immutability, and independent verifiability of network traffic audit logs. A permission-based blockchain built using hyperledger fabric is used to efficiently audit network communication, e.g., interconnected VPC communication, between networks belonging to different parties or entities. A private blockchain network for a VPC network connection is configured to efficiently store network traffic data as a distributed ledger.

The tasks include setting up a hyperledger and auditing network traffic. The task of setting up and configuring the hyperledger is performed by a blockchain configuration engine (BCE). The task of auditing network traffic is performed by a blockchain audit engine (BAE). These components are explained in greater detail below.

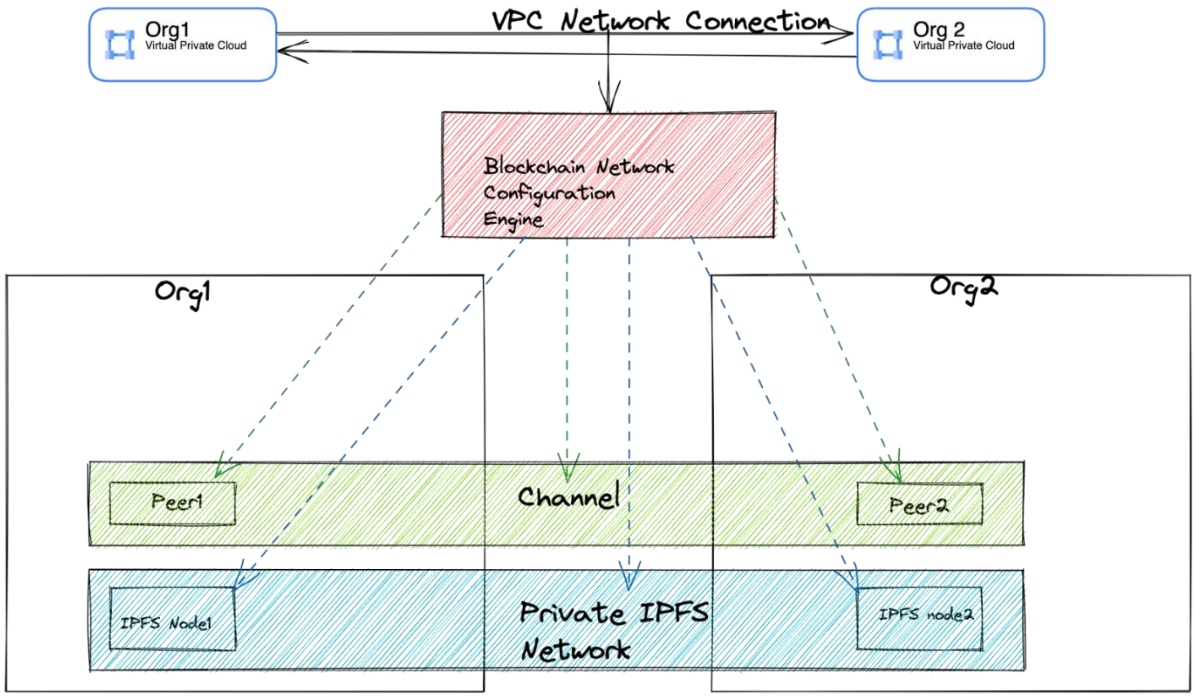

Fig. 1: Role of the BCE in inter-network communication. The two networks can belong to different organizations and are connected using one of the connectivity modes (VPN, peering, cloud interconnect)

Blockchain Configuration Engine (BCE)

As illustrated in Fig. 1, the BCE configures the hyperledger fabric blockchain network for a specific VPC connectivity model. A network administrator can choose if the network communication is to be audited via blockchain. If the administrator chooses this option, then in the event of a connection across two networks, the BCE performs a set of tasks to set up and configure a hyperledger fabric network between the entities involved in network communication.

1. Create a fabric node and an Interplanetary File System (IPFS) node per organization if such nodes have not already been created. The nodes host the fabric peers and store the audit ledger across different channels.
2. Create a peer-to-peer network entity. Since the networks can belong to different organizations, this effectively entails the setting up of a trusted private blockchain network between two different organizations or organizational units.

3. For each VPC network connection in the cloud, create a fabric channel. Add as members to the channel peers across fabric organizations. Thus, a fabric channel is created for a network connection, and the channel comprises peers belonging to the different entities owning the networks.
4. Deploy a smart contract into the peers. The smart contract includes logic for storing network traffic data in the form of distributed ledgers.

Note that there is a fabric channel and a private IPFS network per network connection. The IPFS is useful for storing large amounts of network-traffic data, e.g., for storing the entire payload of transmitted network data.

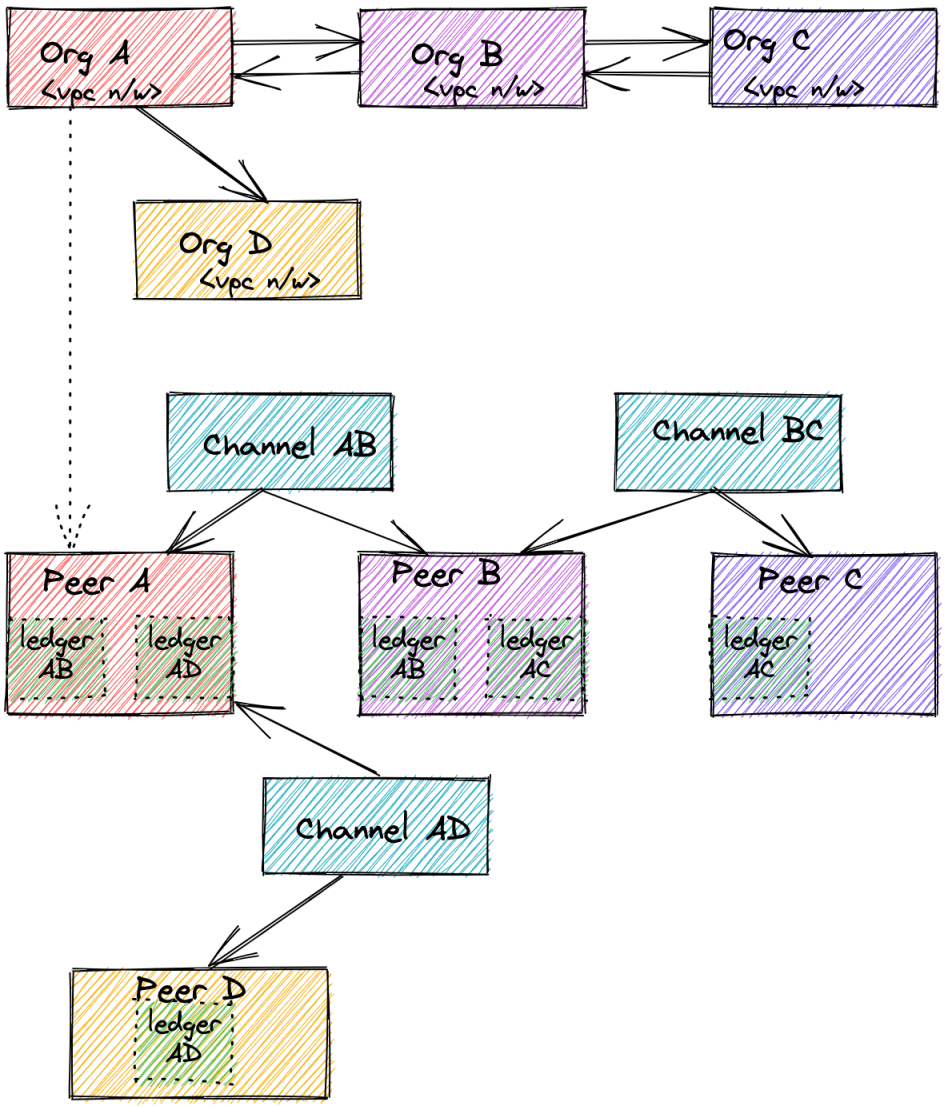

Fig. 2: Relationship between fabric-network entities and VPC networks

Fig. 2 illustrates the relationship between hyperledger fabric network entities and VPC cloud network connections. In the example of Fig. 2, Organization A is connected to networks in Organizations B and D. Further, the network in Organization B is connected to a network in Organization C. For a specific VPC network entity (e.g., Organization A), there exists a peer in the fabric network. For every network connection across two different entities (organizations or business units) a fabric channel is created. Effectively, a channel comprises two peers corresponding to the two entities on either side of the network connection. Since the audit logs

for different network connections are stored in different channels, these audit logs are isolated across VPC network connections.

The BCE deploys the smart contract into the peers. The smart contract includes the implementation to store, update, view, and delete the network audit attributes in the blockchain database. Network attributes (audit information) stored in the blockchain database or the fabric network include the source IP address of the incoming payload; the source port; the destination IP address; the destination port; the destination protocol; a unique hash of source IP, port, destination IP, port, and protocol; an array containing request date and time; an optional identifier (IPFS-cin) to locate the content in the IPFS private network; etc. These attributes, captured as part of the audit, are stored as distributed ledgers in fabric peer nodes belonging to different entities. Hence both the entities (on either side of VPC network connection) independently store the immutable audit data within their nodes in the hyperledger fabric platform.

Blockchain Audit Engine (BAE)

The blockchain audit engine (BAE) stores traffic data within the hyperledger fabric across participating entities. As traffic flows across the networks, the BAE is invoked to store the audit data in the hyperledger fabric distributed ledger. The BAE also stores network traffic in the blockchain ledger as necessary. It acts as the hyperledger fabric client, interacting with the fabric gateway to store network audit information as distributed ledgers.

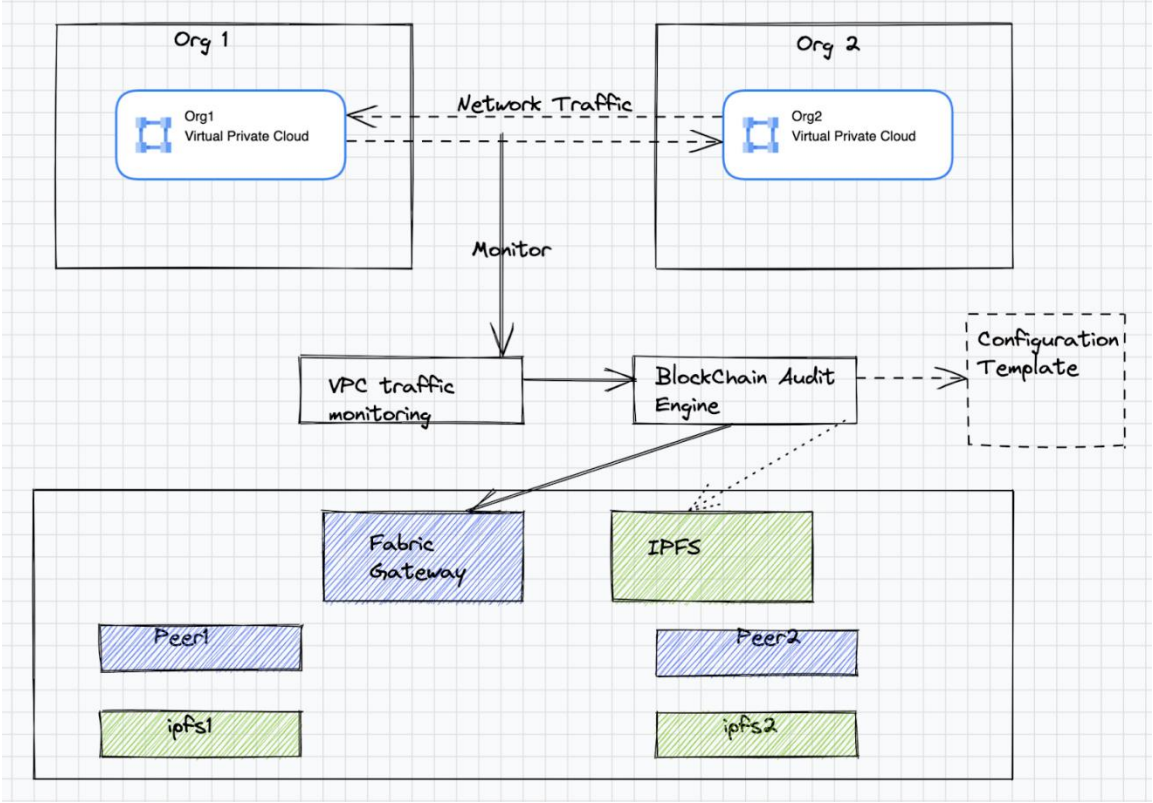

Fig. 3: The role of the BAE in inter-network communication

Fig. 3 illustrates the role of the BAE in inter-network communication. As illustrated in Fig. 3, the BAE can optionally store the complete payload of the network communication in a private IPFS network. In this case, private IPFS clusters with separate nodes for each entity or organization are created to store the payload (the actual data that is transmitted across networks).

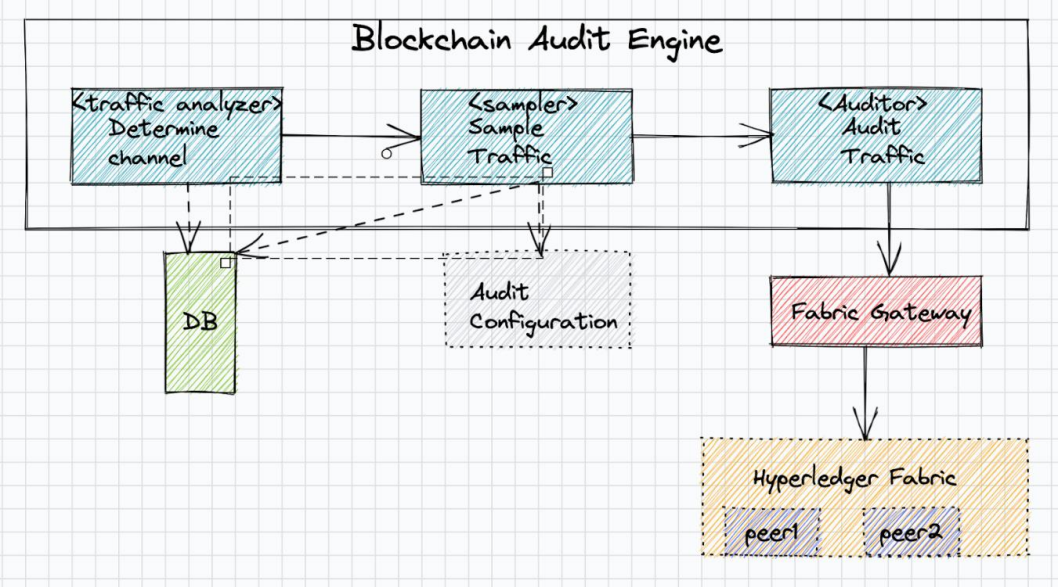

Fig. 4: Components of the BAE

Fig. 4 illustrates that the components of the BAE include a traffic analyzer, a sampler, an auditor, etc., explained in greater detail below.

- The traffic analyzer analyzes the source and the destination network and determines the channel in which the audit information will be stored.
- The sampler is used to sample and optimize the amount of data stored in the distributed ledger. Typically, network communications involve repetitive traffic flows from source to destination. Hence the ID in actual audit information, e.g., the hash comprising source IP and port, destination IP, port and protocol, can be used to detect duplicate data. The audit configuration can contain the number of samples to be logged within a specific time interval, e.g., one hundred samples per hour. The sampler reduces the audit data that is logged, optimizing storage and the amount of transactions sent to the hyperledger fabric.
- The auditor**,** typically a fabric client, invokes the fabric gateway by specifying the channel and by passing the audit data to be stored in hyperledger fabric.

A cloud service provider can provide the above-described capabilities to customers via a user-interface option for securely auditing network connections. This enables trusted auditing of parties or entities involved in a network connection and improves trust in the cloud service provider. The described techniques can be used for traffic inspection, legal compliance, dispute resolution, etc.

The techniques leverage the general concept of blockchain-for-auditing to address the problem of auditing network traffic in a trustworthy and reliable way. Such auditing can be performed by cloud customers without having to rely on the cloud service provider. In particular, the techniques can configure private blockchain networks for a VPC network connection; associate a VPC network to a private blockchain network; audit network traffic efficiently by using a private hyperledger blockchain model; optimize storage to minimize the volume of data logged and to improve logging efficiency; etc.

CONCLUSION

This disclosure describes blockchain-based techniques to provide trust, immutability, and independent verifiability of audit logs of network traffic between organizations. A permission-based blockchain built using hyperledger fabric is provided to enable efficient audit of network communication between networks belonging to different parties or entities. A private blockchain network for a VPC (virtual private cloud) network connection is configured to efficiently store network traffic data as a distributed ledger.