

Deloitte.



Securing Blockchain Workloads on AWS

Security considerations when planning to deploy Amazon Managed Blockchain workloads

Contents

What is blockchain?	1
How does blockchain function?	1
Blockchain core concepts	1
AWS managed blockchain	2
Security considerations for blockchain	3

What is blockchain?

Blockchain's (or distributed ledger technology) evolution has been compared to the early rising of the internet with comments and arguments of the technology's potential to disrupt multiple industries, including Healthcare, Public Sector, Energy, Manufacturing, and particularly Financial Services, where it is predicted to be the beating heart of finance and the ultimate provider of a new industry fabric. A Blockchain, or distributed ledger, is a technological protocol that enables data to be exchanged directly between different contracting parties within a network without the need for intermediaries. Each transaction is communicated to all network nodes, and once verified and confirmed, is added to an immutable transaction chain.

How does blockchain function?

Typically, a user or node will initiate a transaction, which signs it with its private key. Essentially, the private key will generate a unique digital signature that will validate the identity and prevent the transaction from being altered. If anyone were to attempt to modify the transaction information, the digital signature would change, no one would be able to verify it, and it would be discarded. The transaction would then be broadcast to the verifying nodes. The blockchain platform can use different methods to verify whether the transaction is valid or not, which are referred to as consensus algorithms. Once enough of the nodes verify that the transaction is authentic, it will be placed on the ledger and will incorporate a hash of the previous block to protect it from alteration. For most ledgers, aside from those that fall into the distributed ledger technology (DLT) category, information on these transactions is then incorporated into a "block" that cryptographically linked to the previous block to form a chain, thus the name blockchain.

Blockchain core concepts

Cryptography: Blockchain's transactions achieve validity, trust, and finality based on cryptographic proofs and underlying mathematical computations between various trading partners

Immutability: Blockchain transactions cannot be deleted or altered. These characteristics of data object ownership, data revision, and data governance, are typically structured and defined as part of a data architecture

Members: This term is applicable to permissioned blockchains such as Hyperledger fabric and is used to describe a unique identity in the network. For example, a member might be an organization in a consortium of banks. A single AWS account might have multiple members. Each member can run one or more peer nodes.

Nodes: A distributed network of computers running software that can verify blocks and transaction data, endorse transactions, and store a local copy of ledger.

Smart Contracts: Provide automated actions based on triggers. They typically are used to automate the execution of an agreement without any intermediary's involvement. Smart contracts in Hyperledger Fabric are known as "Chaincode".

Decentralized database: Each participating partner always has access to a distributed database in its entirety. No single party controls the database, which every party can verify or regenerate if required without having a central intermediary. Data structures and data hashing also influence architecture modelling.

Distributed transaction-processing platform: Ledgers handle a range of transactions, including exchanging value, assets, or other entities. Transaction processing is moving from a monolithic approach towards an integrative, digital platform

Permissions: Permissions are determined by the nodes participating in a blockchain network: any user can add nodes to a permissionless blockchain network, whereas on a permissioned blockchain, only pre-authorized users can add nodes to the network.

AWS managed blockchain

Amazon Managed Blockchain is a managed service that makes it easier to join public networks or create and manage scalable private networks using the popular open-source frameworks Hyperledger Fabric and Ethereum. You can use Managed Blockchain to create scalable blockchain resources and networks quickly and efficiently using the AWS Management Console, the AWS command line interface (CLI,) or the Managed Blockchain SDK.

Frameworks of AWS managed blockchain

Ethereum

Ethereum is a decentralized blockchain framework that establishes a peer-to-peer network to securely execute and verify application code. This code is called “smart contracts” and allows participants to conduct verified transactions without a trusted central authority.

Transactions are sent and received by Ethereum accounts that are created by users, and Ethereum’s native cryptocurrency, Ether, is used as a cost for processing transactions on the network. A sender must sign transactions and spend Ether. These transaction records are immutable, verifiable, and securely distributed across the network, which gives participants full ownership and visibility into this data.

Hyperledger Fabric

Hyperledger Fabric is an open source blockchain framework from the Linux Foundation that enables participants to write blockchain applications. It offers access control and permissions for data on the blockchain. Hyperledger fabric allows creation of a private blockchain network and limits the transactions that each party can view.

The table below shows the key differences between Ethereum and Hyperledger Fabric Frameworks:

Feature	Ethereum	Hyperledger Fabric
Confidentiality	Public blockchain	Private blockchain
Governance	Ethereum Developers	Linux Foundation
Participation	Public blockchain	Organizations having Certificate of Authorization
Programming Language	Solidity, Vyper	Golang, JavaScript, or Java
Mechanism	Proof of Stake	Pluggable consensus mechanism
Ledger Type	Permissionless	Permissioned
Cryptocurrency/Tokens	Ether or Ethereum	None



Security considerations for blockchain

Many of the same security considerations that apply to traditional application workloads also need to be considered for blockchain workloads. With that said, there are a few specific areas that are unique and/or may require additional focus due to the nature of these types of workloads: Identity and Access Management, Cryptographic Key Management, Data Protection, and Smart Contract development. Some of the specific decisions that need to be made when deploying these types of workloads on AWS are outlined below:

Identity and access management

There are several elements to this, and they differ slightly depending on whether you are using Hyperledger Fabric or Ethereum but there are essentially three levels of access you need to manage.

1. Manage access to deploy and manage Amazon Managed blockchain infrastructure

This is handled the same way as with other AWS resources: authentication is handled by AWS, and permissions are determined by the IAM permissions associated with the IAM principal. As with other permissions in AWS, it is recommended that a least privilege strategy be employed and only those that should have access to perform these activities are permitted to do so. One potential approach here is to create a dedicated IAM role that will be used for creating new Hyperledger Fabric Peer Node or Invitation Proposals and allow only designated personnel, or better yet if embracing a “shift-left” approach, deployment pipeline identities, the ability to assume that role only when performing these operations. The use of guardrails in the form of Service Control Policies (SCPs) can also be helpful for enforcement. Additionally monitoring and alerting can be setup to identify anomalous, suspicious, or unauthorized activities.

2. Managing access to interact with the Hyperledger Fabric or Ethereum API

Hyperledger Fabric - When the first member is created on a Hyperledger Fabric network on Amazon Managed Blockchain, the member's first user must be specified. Managed Blockchain registers the identity of this user automatically with the Hyperledger Fabric CA. This is called a “bootstrap identity”. Even though the identity is registered, additional steps must be taken to enroll this user as an admin and update certificates. These steps

can be performed from a Hyperledger Fabric framework client machine as outlined by AWS [here](#). After the prior steps have been completed, the identity can install and instantiate chaincode, which can be used to enroll additional identities as admins. An important callout here is that **Amazon Managed Blockchain does not support revoking user certificates. After an admin is created, the admin persists for the life of the member. This is an important consideration when developing an IAM Lifecycle strategy.**

Ethereum - The process is similar on Amazon Managed Blockchain,; however, there is no concept of additional admin users, and only the authorized IAM principal in the AWS account that created the node can interact with it using the [Ethereum APIs](#).

As mentioned previously regarding the deployment of the nodes themselves, it is a good idea to implement restriction on these actions and use a dedicated IAM role ideally assumed by a deployment pipeline when performing these activities.

An important note here is that Ethereum running on Amazon Managed Blockchain currently does not support the use of IAM policies for authorization out of the box. However, with ERC725 being the identity standard in Ethereum, theoretically it could be possible to manage access via smart contracts and this is an emerging area of development. Hyperledger Fabric currently does not support resource based policies but attribute-based policies are supported through a combination of tagging and using IAM. Both utilize an AWS sigv4 signature for authentication.

3. Manage access for external users interacting with the blockchain

The interaction of a user with an application that is running on a Hyperledger Fabric blockchain network must be explicitly allowed. To do this, user accounts, in the form of certificates and with the appropriate permissions, will need to be created in the [Hyperledger Fabric CA](#), a mechanism that allows the users to authenticate and gain access to the certificate to perform the desired activities. One such solution that has been developed for this and uses Amazon Cognito, Amazon API gateway and AWS Lambda, which can be employed to allow users to interact with the Blockchain, is illustrated [here](#). As with administrative users, it is a good idea to develop a strategy early on for how user identities and the associated certificates will be managed to identify lifecycle perspective.

Data Protection

AWS offers a variety of tools and services which can help to strengthen aspects of data protection if incorporated effectively in the blockchain design. AWS provides out-of-the-box options to handle encrypting data in transit and at rest for Amazon Managed Blockchain. By default, Managed Blockchain uses an HTTPS/TLS connection to encrypt all data that is transmitted from the AWS CLI on a client computer to AWS service endpoints as well as to communicate with other AWS resources. Amazon Managed Blockchain also offers fully managed encryption at rest. Managed Blockchain encryption at rest provides enhanced security by encrypting all data at rest on Ethereum nodes that use Managed Blockchain-owned encryption keys in AWS Key Management Service (AWS KMS). By default, the member key is owned by AWS but can also be managed by the customer for an additional charge. Something important to be aware of is the supported encryption key options are slightly different depending on the framework being used for the Amazon Managed Blockchain service. For Hyperledger Fabric, an AWS owned key, or a Customer Managed Key (CMK) can

be configured. A CMK gives the customer control over the keying material that is used, the interval at which the key is rotated, and allows them to manually rotate the key if necessary and is the recommended option when available. Using a Customer Managed Key (CMK) or AWS Managed Key is not supported for Amazon Managed Blockchain using Ethereum, only an [AWS Owned Key](#) which is managed by Amazon Managed Blockchain service is currently supported.

Encrypting data in transit and at rest is an important part of protecting data but what about restricting access to information so that only those that are authorized have access? In some ways the very idea of this goes against one of the core concepts of blockchain, which is transparency, but this is often a requirement for certain data in real world applications of this technology.

One option for restricting access to data on Hyperledger fabric, is to use [private data collections](#). These collections allow one to store the data so that it can only be accessed by a certain portion of authorized organizations, and those authorized organizations can access that data

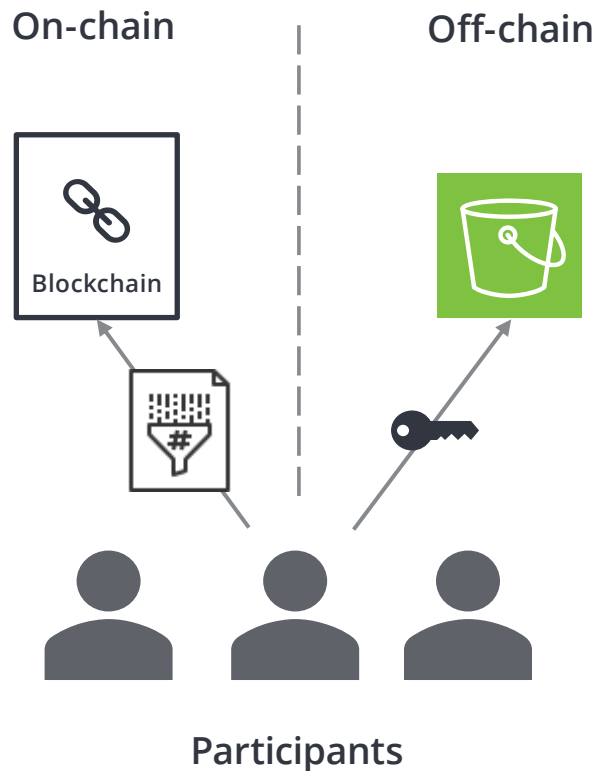


Figure 2 – Storing Data Off-Chain

without needing to create a separate channel. The private data collection consists of the sensitive data, which is sent peer-to-peer over the authorized organizations, and a hash of the private data. The hash is written to the ledgers of every authorized peer on the channel and retains evidence of each transaction.

Access to data can also be restricted by using a “channel”, a channel is a private communication pathway between two or more members of a Hyperledger Fabric network on Amazon Managed Blockchain. Channel is built by members (organizations), shared ledger, anchor peers per member, ordering service nodes and chaincode applications. Each transaction on Hyperledger fabric network occurs on a channel and everyone should be authenticated, authorized to transact on a channel. Members shares their admin certificates and root CA with the channel creator when they join the channel which is used to authenticate and authorize members of the channel.

Another approach is the use of hashing. As mentioned previously, this process is at the core of how blockchain functions and involves the use of an encryption key to create a one-way encryption which is not decryptable. There is no way to decipher this information with the hash alone; however, the hash can be used to validate the information by re-hashing it and comparing the results. Unlike encryption, hashing does not provide

as a mechanism to securely distribute information but it can be used by two separate parties to validate the information, which is still a common requirement for use cases involving smart contracts. You can combine this with a mechanism to store the data off-chain to address the need to securely store and distribute this information. One example of a solution built to do just that can be found [here](#). It utilizes Amazon API Gateway, Step Function, and Lambda to store the off-chain data in S3. You can then create bucket policies and/or leverage IAM to allow only designated external parties to access the data.

One last thing related to data protection that is important to consider whenever evaluating blockchain as a potential solution are regulatory requirements. Data protection related regulatory requirements such as regulatory requirements related to GDPR ([General Data Protection Regulation](#)) must be considered when developing blockchain based solutions. Blockchain's decentralized nature makes it nearly impossible to designate responsibility for controlling data and enforcing GDPR standards and at the time of this writing, there is currently no definite conclusion on whether blockchain technologies can comply with GDPR's data modification and erasure requirements. This can be a non-starter for some organizations in highly regulated environments.



Cryptographic Key Management

So far, we have discussed how Blockchain leverages cryptographic algorithms and keys to link transactions, guarantee immutability in a distributed ledger, authenticate users, and protect data. It is hard to overstate just how important it is that these keys are securely stored and managed. Developing and implementing an effective encryption key management strategy early on is critical. Some important things to consider when developing this are outlined below:

1. Cryptographic key management using industry standards and leading practices, which advocates storing encryption keys away from the blockchain ledger in a secure way.
2. Users should be authenticated and authorized to use keys.
3. Cryptographic keys need to be available for smart contracts and users. This is a challenge in a distributed blockchain environment.
4. Blockchain uses atypical cryptographic algorithms that are incompatible with some existing key management solutions
5. Access to cryptographic keys needs to be restricted and process in place for granting and revoking access to keys.

Encryption (with key management) is one of the strongest data protection methods available—often serving as the last line of defense against threats when other controls have failed. Customer-managed keys can be allocated by account, service, region, application, and/or by environment. It is critical to standardize the key hierarchy for native services before rolling out to cloud accounts. Organizations should also determine how keys should be generated, stored, rotated, and deactivated—and build a process around the lifecycle.

A centralized key management system:

- Allows organizations to manage large numbers of keys throughout their lifecycle
- Makes auditing and policy enforcement easier to implement
- Allows for key distribution to a single or multi-cloud environments

AWS Key Management Service can be a valuable tool to help with the process. It provides a mechanism to securely generate, store, rotate and restrict access to keys. With this said, there are some important things to keep in mind beyond just leveraging this service.

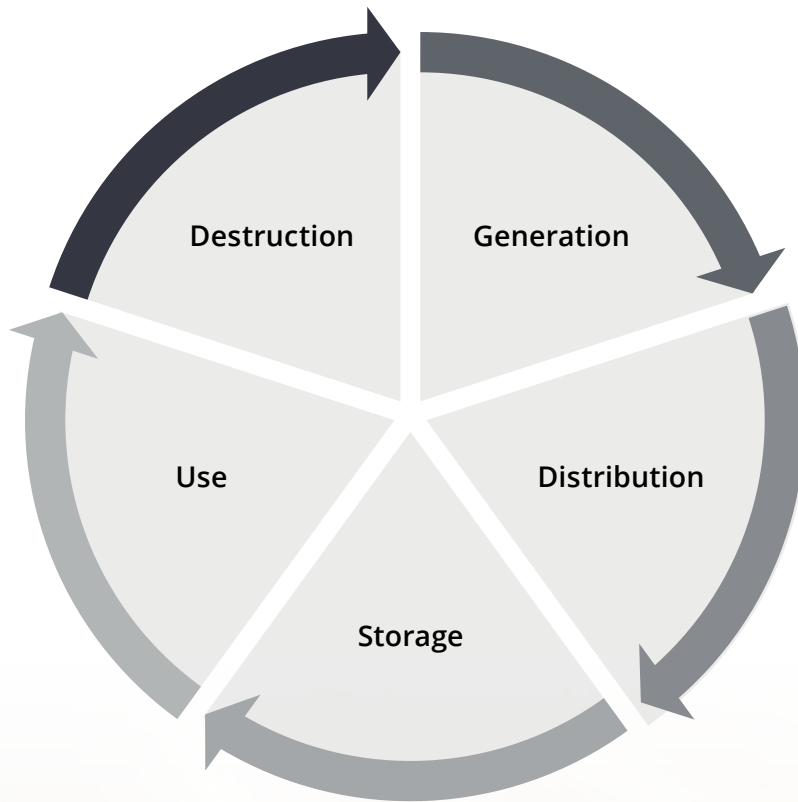
For one, Hyperledger Fabric has its own certificate authority that is used to manage user identities and issues enrollment certificates for securely communicating within the blockchain network. When an admin is created, a certificate is generated and stored on the Hyperledger Fabric Client Machine. Additional admin users can also be created if required. Each admin user will get their own set of keys created. For an organization a root certificate is stored in the Fabric certificate authority (CA). For the different users in an organization the Fabric CA also issues certificates. An enterprise-grade Fabric CA uses various components and can be deployed in different ways using a Hardware Security Module (HSM) such as AWS Cloud HSM for added protection.

Additionally, in Ethereum, an account is essentially a cryptographic key pair (public and private). By default, these are created outside of AWS and it is common for users to manage their own keys which they then use to sign transactions, but this can pose challenges when it comes to security and manageability. Additionally, for certain use cases such as those involving automated external processes it is necessary to have a mechanism to centrally store and access these keys. This is where a service like AWS KMS can be leveraged. An excellent example how this has been done can be found in this [series of blog posts](#).



Finally, there are some challenges associated with utilizing AWS KMS for certain low-level tasks. Some of the blockchain clients don't natively support AWS KMS and there are some incompatibilities with the cryptographic algorithms used. One approach that is gaining traction to address these challenges is the use of AWS Nitro Enclaves to perform tasks on the blockchain. AWS Nitro Enclaves securely protects highly sensitive data by allowing

customers to create isolated compute environments that reduce attack surface area. An excellent set of AWS blog posts that detail these challenges and how one can go about using AWS Nitro Enclaves for this can be found [here](#). A table of possible options for generating, storing, and managing cryptographic keys used for encryption at rest, authentication, hashing, and transactions is shown below.



Cryptographic Key Generation

Cryptographic Key Storage

Cryptographic Key Usage



AWS Key Management Service



AWS CloudHSM



AWS Secrets Manager



AWS CloudHSM



AWS Nitro Enclaves



AWS CloudHSM

Smart contract development

As mentioned previously, smart contracts are really just tiny programs distributed to all nodes in a blockchain network that automatically execute a predetermined set of actions when certain conditions are met. As such, just like any other code, they are subject to flaws that can allow them to operate in unintended ways. There have been several instances recently where a vulnerability in a smart contract was exploited, resulting in tens of millions of dollars in losses; thus, it is imperative that security checks be incorporated into the smart contract development process to identify any potential security issues as early as possible and well before these are deployed to the blockchain.

Before diving into recommendations to identify and address vulnerabilities in smart contracts, one important distinction to point out is, unlike typical application code, smart contracts on Ethereum are immutable, which means that once they are deployed to the blockchain they cannot be changed. That's not to say there are not methods to upgrade these to fix a vulnerability, change the logic, or add a new feature, but a strategy for this needs to be established early in the process. Since this can have a big

impact on the way in which contracts are initially written, this should ideally be decided before initial development starts. Some information on updating smart contracts in Ethereum can be found [here](#) which talks about the common methods that can be used to as well as the pros and cons of each. Once that is sorted out, the next focus should be on how to incorporate security into the overall smart contract development process. Generally, this includes taking all the steps usually performed as part of the secure code development process, but the key differences being the types of vulnerabilities and the tooling available to detect these. A good place to start is to review some useful information is this [page from Ethereum.org](#). Due to the relatively young age of blockchain, many of the tools to support this process are still in early stages of development, but they have come a long way in recent years. Some of the popular open-source tools that are available to help with this are [Slither](#), [Mythril](#) or [Manticore](#), but this is an evolving landscape. The figure below illustrates a possible workflow utilizing AWS CodeCommit and an open-source tool, such as one listed above, running inside an AWS CodeBuild job to scan the chaincode for vulnerabilities before deploying it to the blockchain.

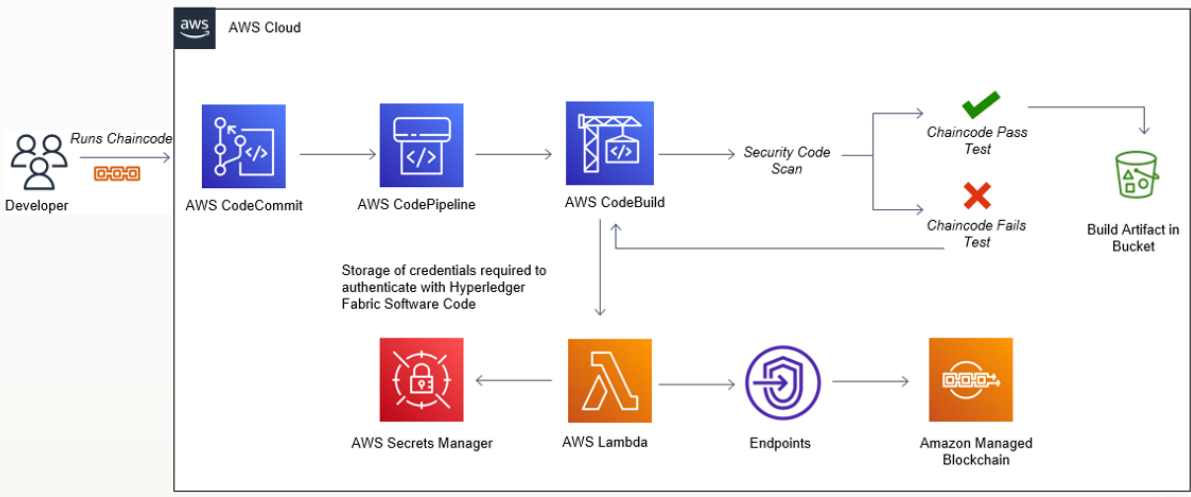


Figure 4 – Chaincode Deployment Flow

Contact

Aaron Brown

Advisory Partner, Cyber Risk Services AWS Alliance Leader

Deloitte & Touche LLP

aaronbrown@deloitte.com

Ravi Dhaval

Advisory Senior Manager, Cyber Risk Services

Practice and Innovation Lead

Deloitte & Touche LLP

rdhaval@deloitte.com

Tim Davis

Advisory Principal, Blockchain & Digital Assets leader

Risk & Financial Advisory

Deloitte & Touche LLP

timdavis@deloitte.com

Authors

Deloitte & Touche LLP

Aaron Lennon

Advisory Specialist Leader, Cyber Risk Services

Deloitte & Touche LLP

alennon@deloitte.com

Barathi Krishnamurthy

Advisory Senior Consultant, Cyber Risk Services

Deloitte & Touche LLP

bkrishnamurthy@deloitte.com

Hannah Dutler

Advisory Consultant, Cyber Risk Services

Deloitte & Touche LLP

hdutler@deloitte.com

Nishit Shetty

Advisory Consultant, Cyber Risk Services

Deloitte & Touche LLP

nishitshetty@deloitte.com

Jay Brown

Advisory Consultant, Cyber Risk Services

Deloitte & Touche LLP

jaybrown@deloitte.com

Special Thanks

Steve Bollers

AWS Sr. Partner Solutions Architect

Amazon Web Services

sbollers@amazon.com

Jeff Kaiserman

AWS Principal GSI Security Partner Solutions Architect

Amazon Web Services

jkaiserm@amazon.com

Sources:

1. Work with Hyperledger Fabric Components and Chaincode— Amazon Managed Blockchain
2. Using the Ethereum APIs with Amazon Managed Blockchain — Amazon Managed Blockchain
3. Welcome to Hyperledger Fabric CA (Certificate Authority) — hyperledger-fabric-cadocs master documentation
4. Integrate Amazon Managed Blockchain identities with Amazon Cognito | AWS Database Blog
5. Private data — hyperledger-fabricdocs main documentation
6. Create Additional Isolation to further Protect Highly Sensitive Data within EC2 Instances | AWS Nitro Enclaves
7. Store off-chain data using Amazon Managed Blockchain and Amazon S3: Part 1 | AWS Database Blog
8. EPRS_STU(2019)634445_EN.pdf (europa.eu)
9. Develop Hyperledger Fabric Chaincode - Amazon Managed Blockchain
10. Smart contract security | ethereum.org
11. Hedera – How it Works: Hashgraph ConsensusHedera – How it Works: Hashgraph Consensus
12. Freeman Law: Permissioned and Permissionless BlockchainsFreeman Law: Permissioned and Permissionless Blockchains
13. GitHub - ConsenSys/mythril: Security analysis tool for EVM bytecode. Supports smart contracts built for Ethereum, Hedera, Quorum, VeChain, Roostock, Tron and other EVM-compatible blockchains.
14. GitHub - trailofbits/manticore: Symbolic execution toolGitHub - trailofbits/manticore: Symbolic execution tool





About this publication

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.