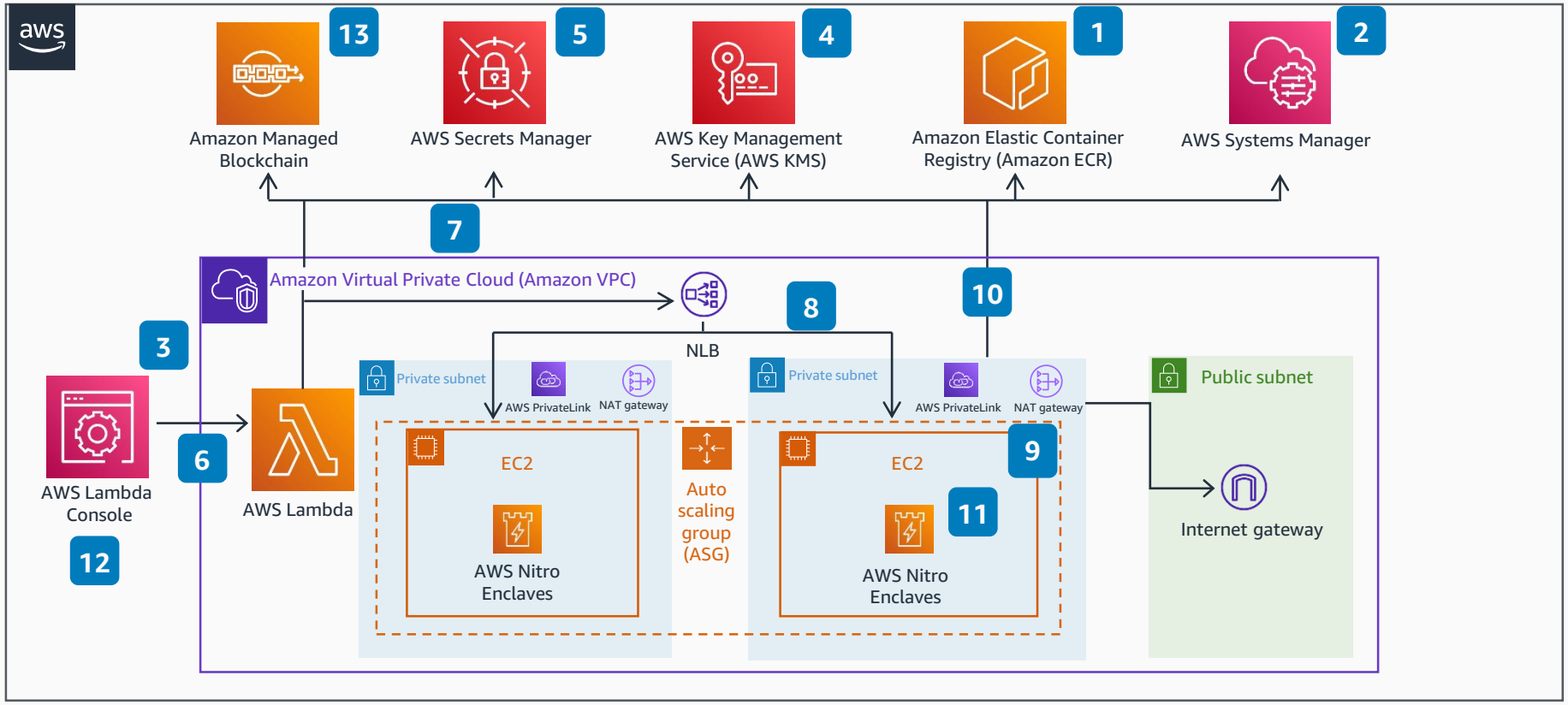
Guidance for Secure Blockchain Key Management with AWS Nitro Enclaves

A secure, scalable, and cost efficient blockchain key management solution that offers flexibility for signing algorithms.

This architecture shows how you can use AWS Nitro Enclaves and AWS Secrets Manager for secure blockchain transaction signing. This flexible and highly available Guidance has a software-defined nature that supports cryptographic algorithms.



1. Deployment is based on **AWS Cloud Development Kit** (AWS CDK). Required Docker containers are stored on **Amazon Elastic Container Registry** (Amazon ECR).
2. Secure access to AWS Nitro Enclave parent instances is realized through **AWS Systems Manager** without using secure shell (SSH).
3. Customer can interact with system through **AWS Lambda** console or add an individual point of integration.
4. Private key must be encrypted through a **symmetrical** key in **AWS Key Management Service** (AWS KMS).
5. Encrypted private key is stored in **AWS Secrets Manager**.
6. Customer triggers transaction signing request through **Lambda** console.
7. Encrypted private key is downloaded and passed to **Amazon Elastic Compute Cloud** (Amazon EC2) instance along with transaction parameters.
8. Request is routed through Network Load Balancers (NLB) to the next healthy **Amazon EC2** instance running isolated in a private subnet.
9. **Amazon EC2** instance is the parent instance for the signing process running inside an AWS Nitro Enclave.
10. Request (from step 5) is passed into AWS Nitro Enclave. Cryptographic attestation is used to securely communicate with **AWS KMS** from inside the enclave through **AWS PrivateLink** to get the key decrypted.
11. Transaction is signed inside AWS Nitro Enclave. Signed transaction is returned to user, private key is deleted from inside the enclave.
12. Signed transaction is returned to the **Lambda console.**
13. The transaction can now be released to the public Ethereum network through **Amazon Managed Blockchain**.

Reviewed for technical accuracy March 1, 2023

AWS Reference Architecture