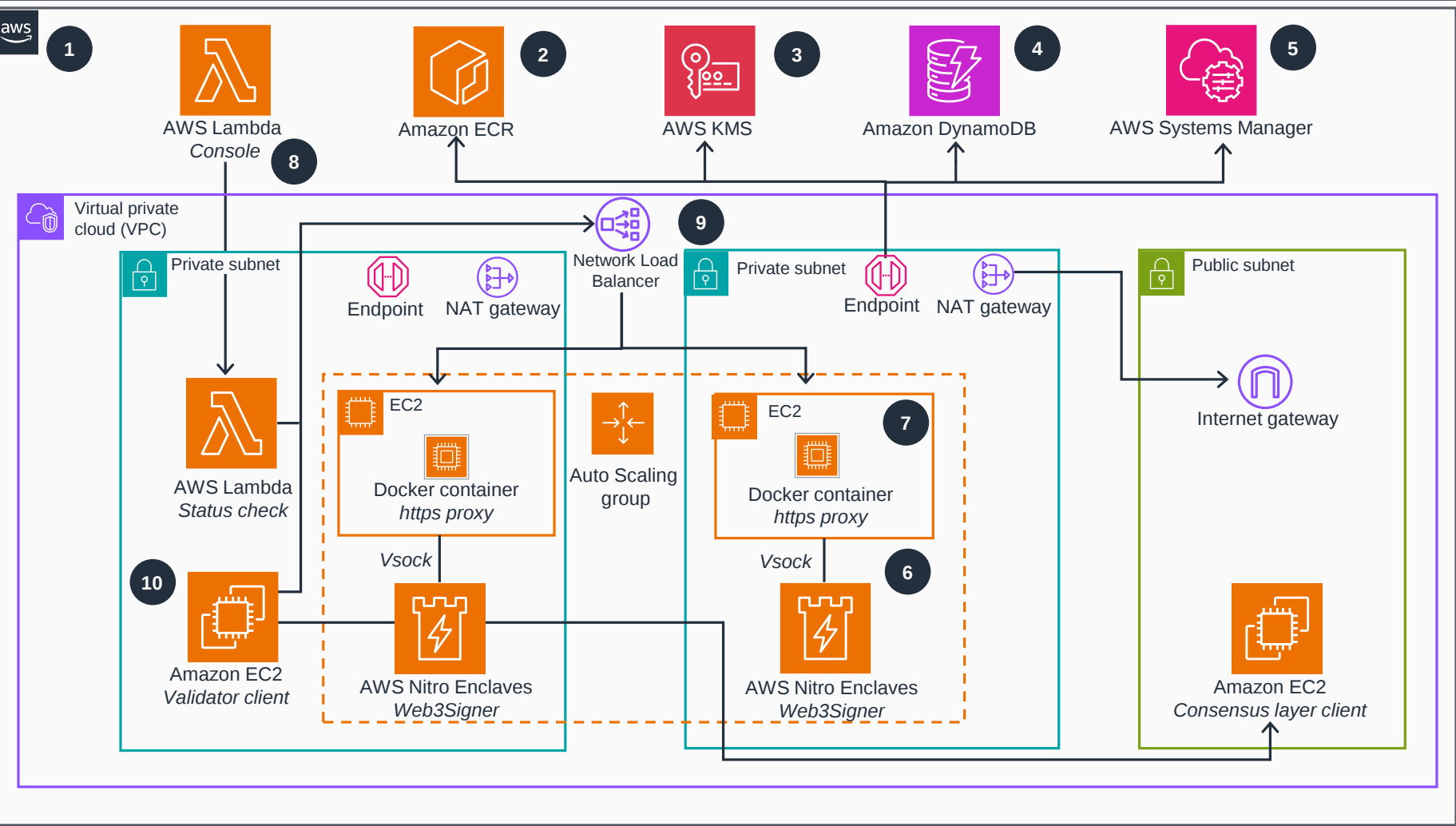


Guidance for Secure Blockchain Validation Using AWS Nitro Enclaves

This architecture diagram shows a secure, scalable, and cost-efficient blockchain key management solution that offers flexibility in signing algorithms and can be used for blockchain validation.



- 1 Run the **AWS Cloud Development Kit (AWS CDK)** stack through your local machine.
- 2 Once you run the **AWS CDK** stack, the required container artifacts are uploaded to the **Amazon Elastic Container Registry (Amazon ECR)**. All Docker containers will be pulled from **Amazon ECR** later.
- 3 Config artifacts are encrypted through a symmetric encryption key using **AWS Key Management Service (AWS KMS)**.
- 4 Encrypted config artifacts are stored in **Amazon DynamoDB**.
- 5 Run the Web3Signer initialization with an **AWS Systems Manager** command.
- 6 AWS Nitro Enclaves automatically decrypt config artifacts through **AWS KMS** using cryptographic attestation.
- 7 The Web3Signer process starts with Nitro Enclaves and exposes the HTTPS API on a parent **Amazon Elastic Compute Cloud (Amazon EC2)** instance.
- 8 Control the Web3Signer status through the **AWS Lambda** console. The `state` command provides information about the current status of the **Lambda** function.
- 9 Requests are routed through a **Network Load Balancer** to the next healthy **Amazon EC2** instance that runs isolated in a private subnet.
- 10 Requests originating from the **Amazon EC2** validator or consensus client can be routed to a **Web3Signer** instance through a **Network Load Balancer**. The validator client is not enclosed in this Guidance.