NERVOS BLOCKCHAIN

A Beginner Starter Guide

V1:23

NERVOS BLOCKCHAIN

HOW TO USE

Each section starts with:

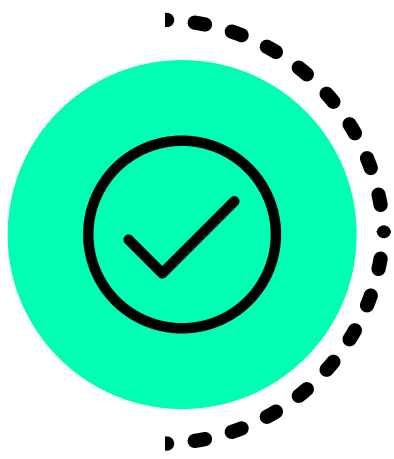
- What you will learn.
- A list of questions to answer.
- Terms to know.
- Useful links for further information.

Each section ends with:

- A list of questions to answer.
- Links to further information.

NERVOS BLOCKCHAIN

Contents



BUILD SOMETHING

GLOSSARY

Useful terms reviewed.

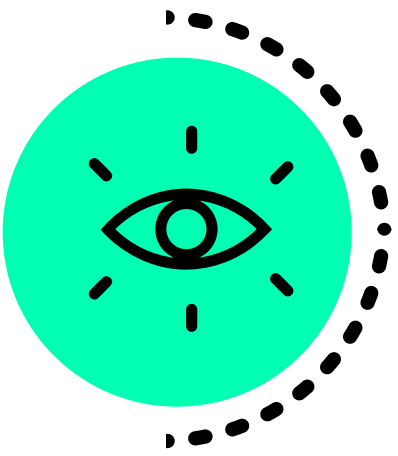
EXTRA RESOURCES

More links to get started.

NERVOS BLOCKCHAIN

Contents

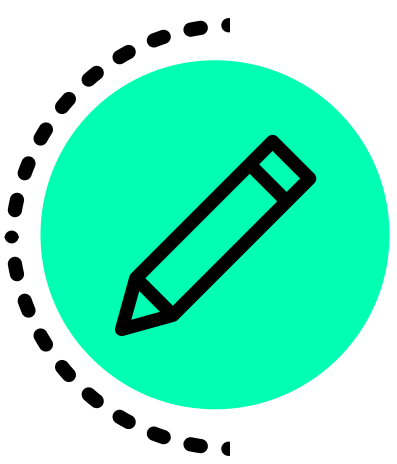
1 **UNDERSTAND**
A brief introduction to the Nervos Blockchain.



DEFINE

- What is it?
- How does the blockchain work?

USEFUL TERMS:



BLOCKCHAIN **CKB**

CONSENSUS

CELL **CKBYTE** **NATIVE TOKEN**

LEARN MORE:

NERVOS BASICS

WHAT IS NERVOS

NERVOS BLOCKCHAIN

Introduction

WHAT IS THE NERVOS BLOCKCHAIN/NETWORK ?

It is a multi-layer public blockchain network. Designed to enable multi-chain interoperability.

NERVOS BLOCKCHAIN

Foundation Layer

ALSO KNOWN AS:

CKB

COMMON
KNOWLEDGE
BASE

MEANING:

CKB stores information everyone is aware of. Therefore all stored data is common knowledge.

COMMON KNOWLEDGE:

is the state of this information agreed via global consensus.

State is the history and current available information of the blockchain.

Global consensus is the shared understanding of the history and current state of the blockchain.

NERVOS BLOCKCHAIN
CONSENSUS

WHAT IS CONSENSUS?

Consensus is the agreement on the state of the CKB between participants on the network.

Meaning:

All participants agree on data states such as

- **which digital assets users hold.**

Who are the participants?

The participants are nodes or computers holding a copy of the CKB.

Meaning:

- This creates a network.
- Data (transactions) flow through the network between computers.
- This data is recorded.

An agreement must be achieved on:

- which transactions are valid.
- What order did the transactions occur.

NERVOS BLOCKCHAIN

CONSENSUS

The Majority of nodes (computers) agree on valid transactions and the order. Therefore, share information about the history and current state of the blockchain.

HOW IS THIS ACHIEVED?

CKB uses a Proof of WorK (PoW) based consensus algorithm.

NC-MAX

Meaning:

The algorithm demands the nodes follow the rules in order to participate.

How?

Using:

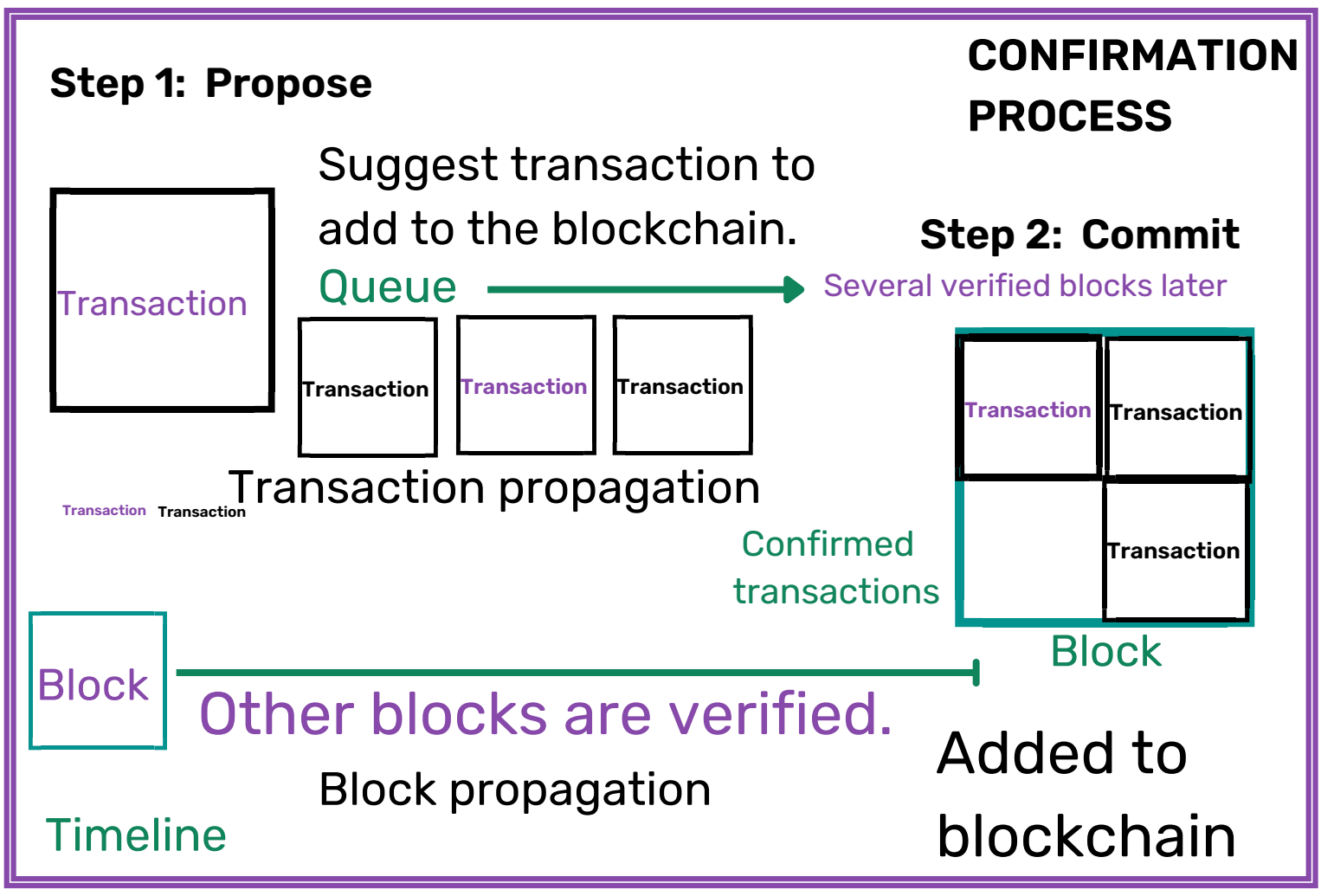
- Two-step transaction confirmation.
- Dynamic block interval and block reward.
- Considering all blocks in difficulty adjustment.

NERVOS BLOCKCHAIN

CONSENSUS

WHAT IS TWO-STEP TRANSACTION CONFIRMATION ?

It is a Propose and Commit confirmation process.



Meaning:

NC-MAX splits the confirmation into two steps.

First a transaction is proposed. Several blocks are verified while a transactions waits to be added. Second a transaction is committed to the block.

Benefit:

Allows time for transactions to move up the queue. Without slowing down block propagation.

NERVOS BLOCKCHAIN
CONSENSUS

WHAT IS
DYNAMIC BLOCK INTERVAL AND BLOCK REWARD ?

NC-MAX automatically adjusts block intervals based on network performance.

How?

The concensus tracks the time of the number of orphan blocks created and adapts block interval time.

Benefits:

- Shorter block times.
- Security not compromised.

Orphan block is a block that has been solved but not accepted by the network.

Block Interval is the time between block creation.

NERVOS BLOCKCHAIN
CONSENSUS

WHAT IS

CONSIDERING ALL BLOCKS IN DIFFICULTY ADJUSTMENT?

NC-MAX difficulty adjustment mechanism counts all blocks when estimating mining power.

Meaning:

The Algorithm measures the networks collective computing power and maintains the networks target difficulty necessary to obtain a valid proof.

Why?

- To defend against selfish mining.

Selfish mining, when miners gain a larger share of mining rewards, while contributing less hash power.

Target difficulty, a math computation level set by the network.

Valid proof, a computation of the hashed block data. Lower than the target difficulty.

NERVOS BLOCKCHAIN
CONSENSUS

Overall NC-MAX algorithm Benefits:

Improving

- block propagation.
- block throughput.
- resistance to selfish mining.
- adds security

NERVOS BLOCKCHAIN
REVIEW

QUESTIONS ?

Q1. What is the name of the Nervos foundation layer?

Q2. What does CKB mean?

Q3. What is Consensus?

Q4. Who are the participants?

Q5. How is consensus achieved?

Q6. Why is consensus important?

Further information:

NC-Max algorithm

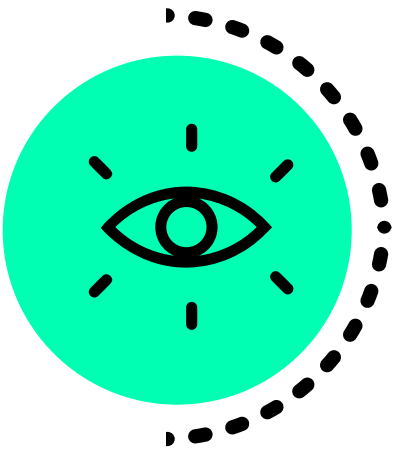
Consensus

POW (Proof Of Work)

NERVOS BLOCKCHAIN

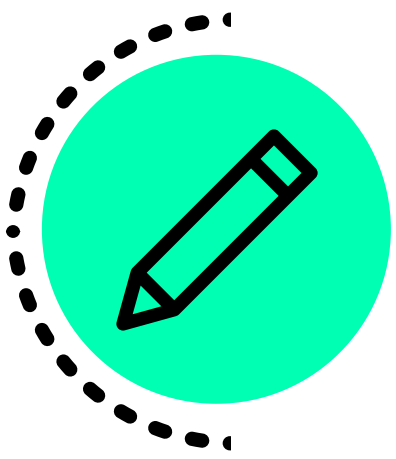
2 UNDERSTAND

This section talks about the CKB's role as the foundation layer.



DEFINE

- What is the foundation layer?
- How is the foundation layer built?
- How does it work/ How is data stored?



USEFUL TERMS:

THE FOUNDATION LAYER

CKB

CELL

CKBYTE

NATIVE TOKEN

CELL MODEL

CONSUMPTION

UNCONSUMED

LIVE CELL

CONSUMED

DEAD CELL

LOCK SCRIPT

TYPE SCRIPT

LEARN MORE:

NERVOS CELL BASICS

NERVOS BLOCKCHAIN

COMMON KNOWLEDGE BASE

CKB **THE FOUNDATION LAYER**

DESIGNED TO:

- Maximise decentralisation

At the same time as being:

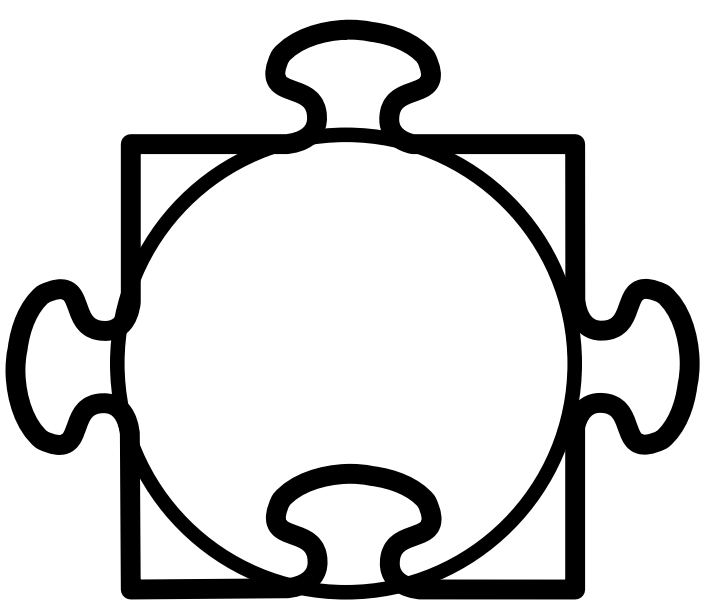
- Minimal
- Flexible
- Secure

Primary Objective:

Reliably preserve any data and stored assets.

HOW?

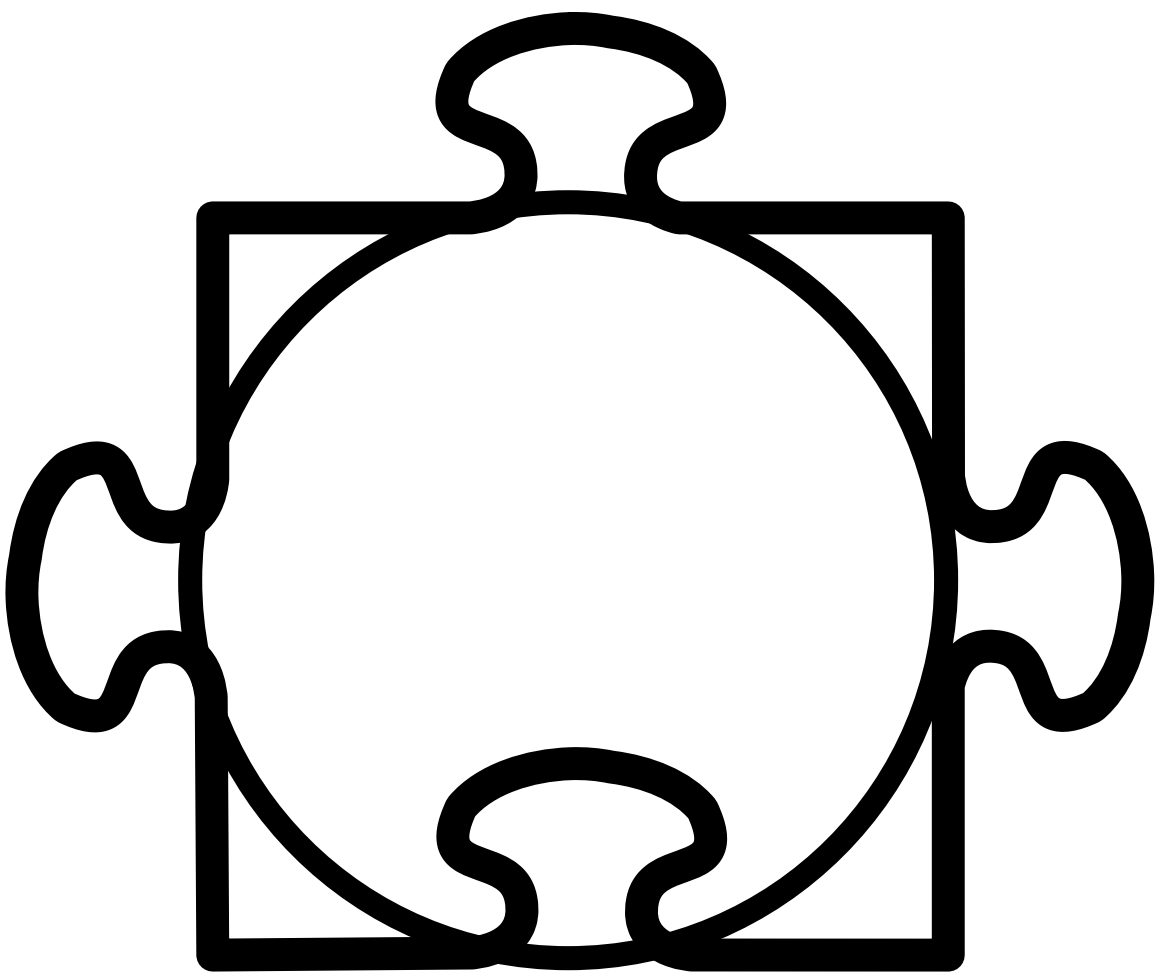
USING CELLS.



Cells are the primary state units.

NERVOS BLOCKCHAIN
CELL

WHAT IS A CELL?



EACH CELL CONTAINS:

- A Lock Script
- A Type Script
- Data

Lock Script defines who has permission to use it.

Type Script (optional) if present, enforces the rules on the usage of the cell.

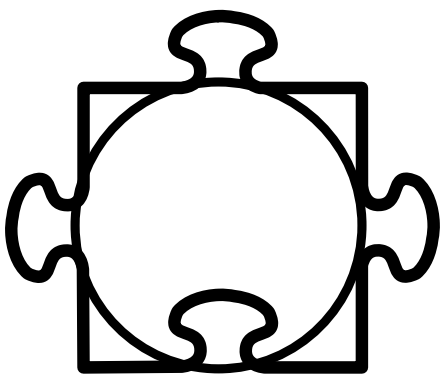
Data there is no restriction on the data type contained in the cell.

For example:

- CKbytes
- Tokens
- Code

NERVOS BLOCKCHAIN

CELL MODEL



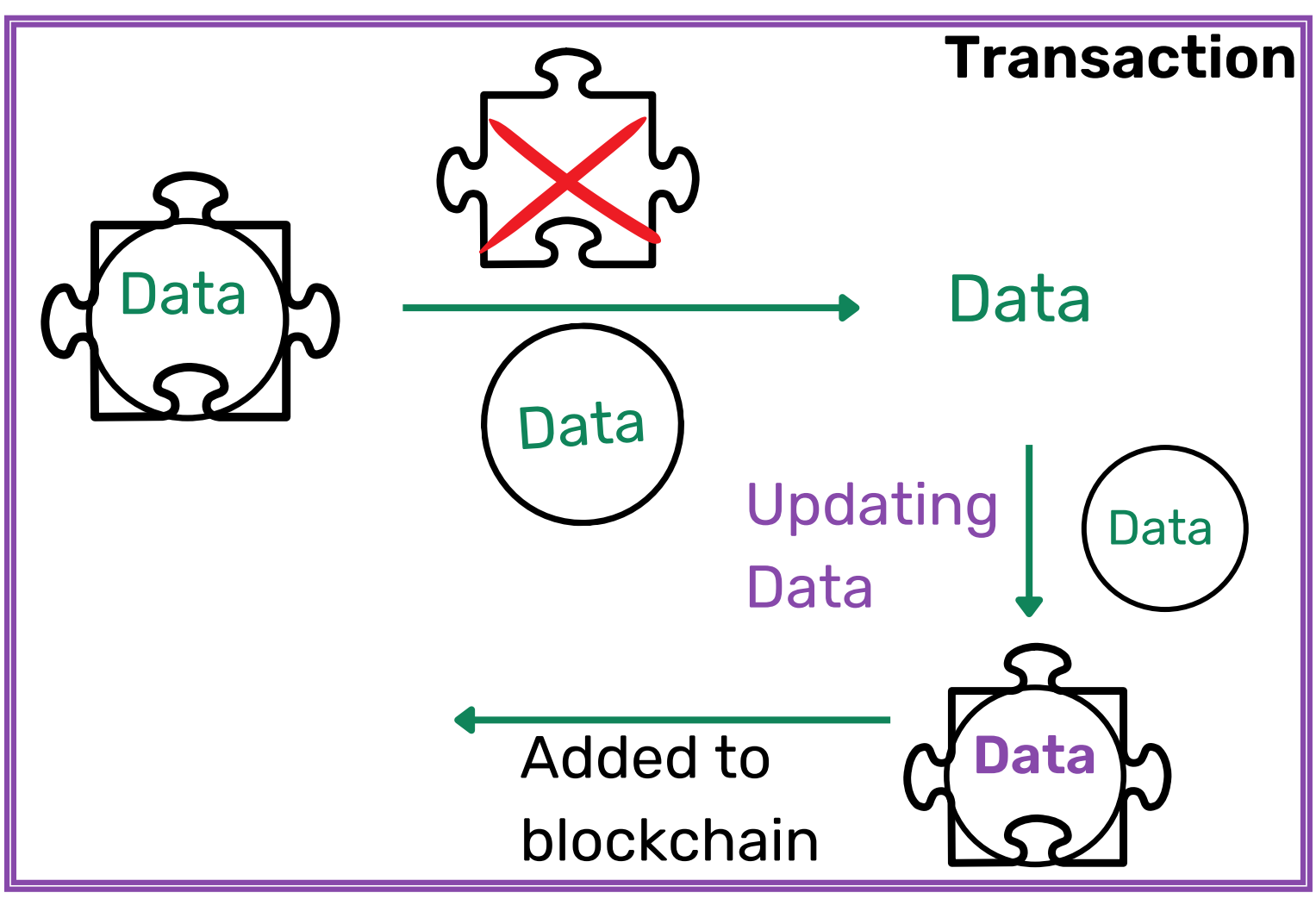
A cell is immutable.

Meaning:

No changes can be made once added to the blockchain.

HOW IS DATA UPDATED?

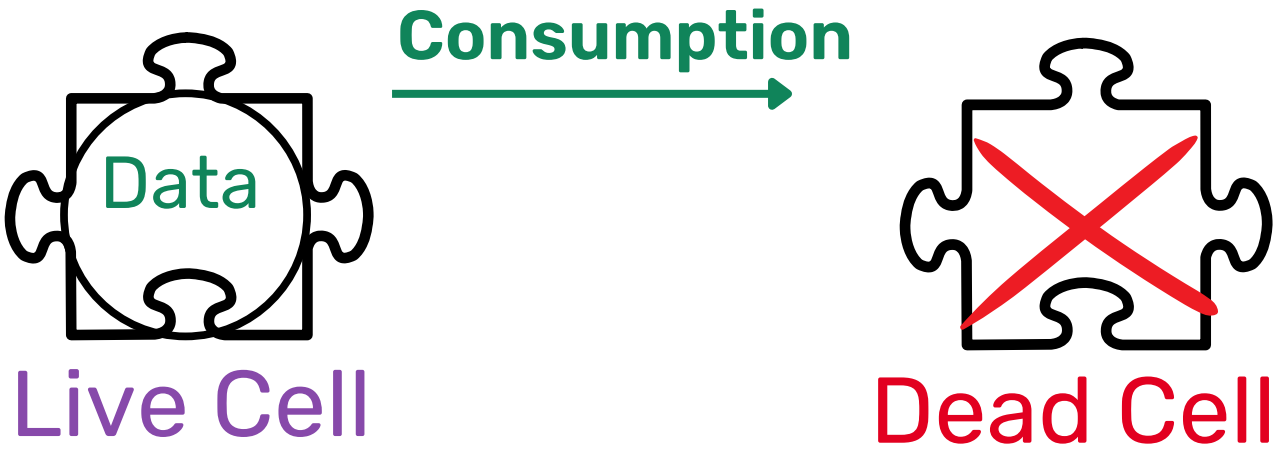
Via a process called Consumption.



- Each cell is consumed once.

CELL IS EITHER :

Unconsumed **Consumed**



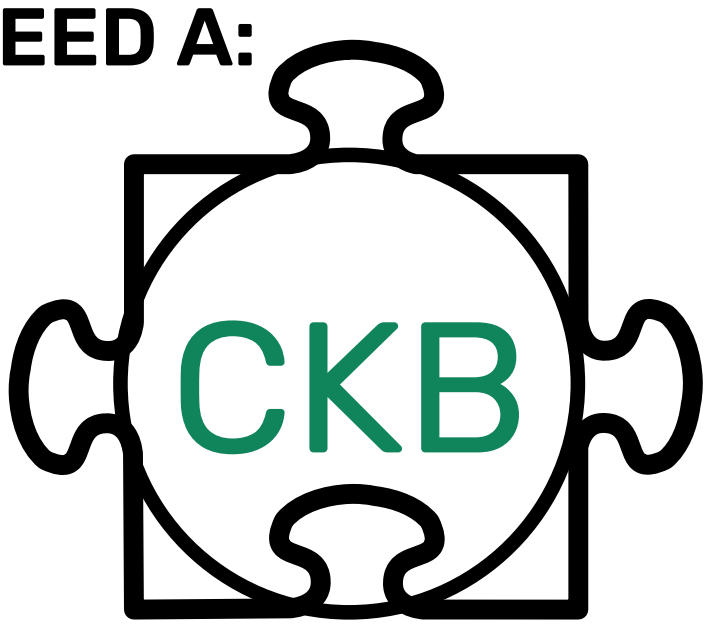
Once dead/destroyed it can no longer be used.

NERVOS BLOCKCHAIN

STORING DATA

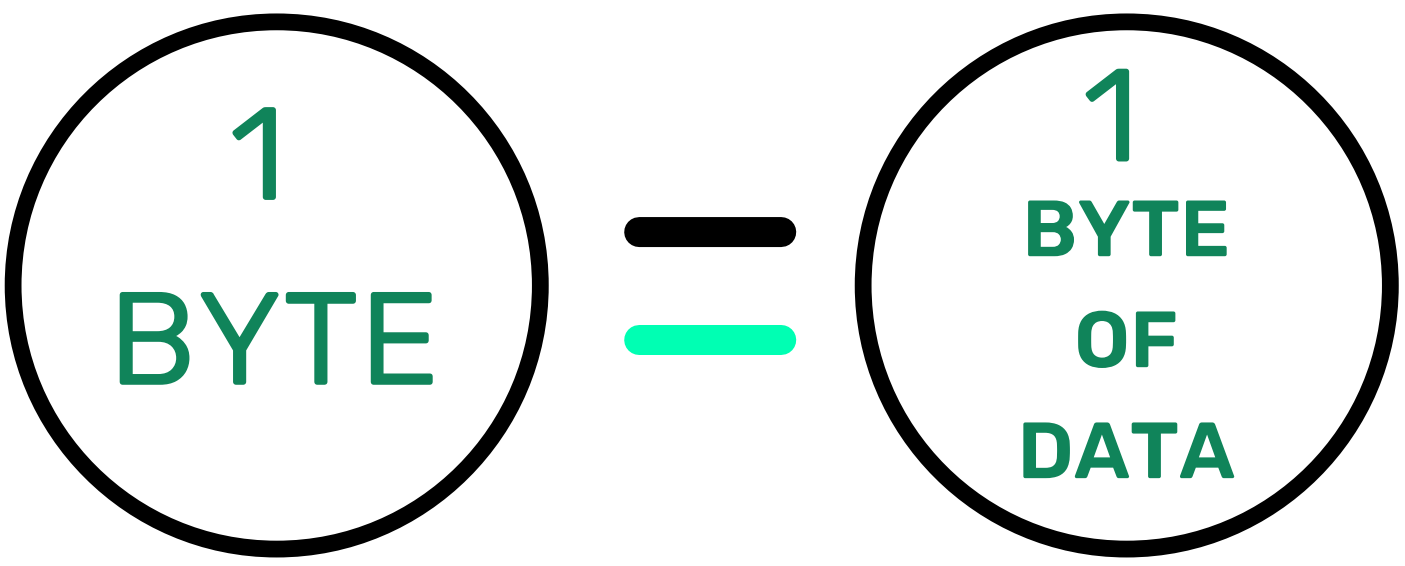
HOW TO STORE DATA?

YOU NEED A:



COMMON KNOWLEDGE BYTE

To store data on the CKB you need to hold:



What type of data?

- Smart contracts
- Tokens
- NFTs
- And more....

ALL REQUIRE CKBYTES TO BE STORED/REPRESENTED ON THE BLOCKCHAIN.

NERVOS BLOCKCHAIN
CKBYTE

A COMMON KNOWLEDGE BYTE

CKBYTE

IS

A way to store data.

&

- The Native token of the CKB.

You need:

100 CKBYTES to store 100 BYTES OF DATA

If your data occupies space on the CKB, your CKBytes remain locked.

If your data is no longer needed and is removed, your CKBytes become available to use.

CKBYTES ARE USED TO PAY FEES FROM ANY TRANSACTIONS OR COMPUTATIONS.

NERVOS BLOCKCHAIN
REVIEW

QUESTIONS ?

Q1. What is the main objective of the Nervos foundation layer?

Q2. What three benefits does the Nervos CKB offer?

Q3. What do you need to store data?

Q4. How are cells updated?

Q5. What is the native token of Nervos?

Q6. What type of data can be stored?

Further information:

CKB layer 1

Cell Model (Video)

Cell Model (Article)

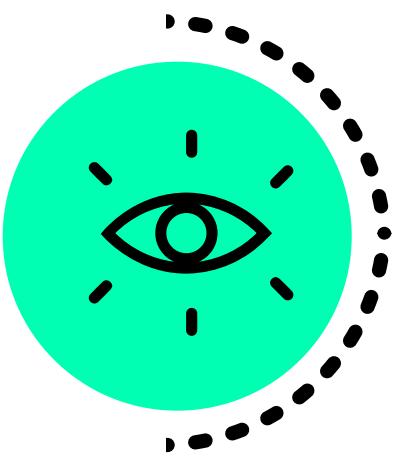
NERVOS BLOCKCHAIN

Contents

3

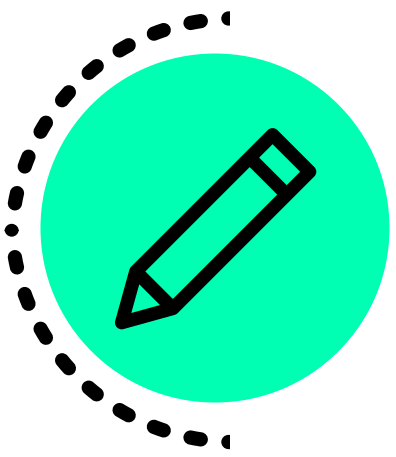
UNDERSTAND

Deeper dive into the layers and the architecture of Nervos.



DEFINE

- Why is a layered architecture important for the Nervos blockchain?
- What is the focus of each layer?



USEFUL TERMS:

DECENTRALISATION

SECURITY

SCALABILITY

INSTANTANEOUS TRANSACTIONS

INTEROPERABLE

OPTIMISTIC RROLLUP

TRILEMMA

LEARN MORE:

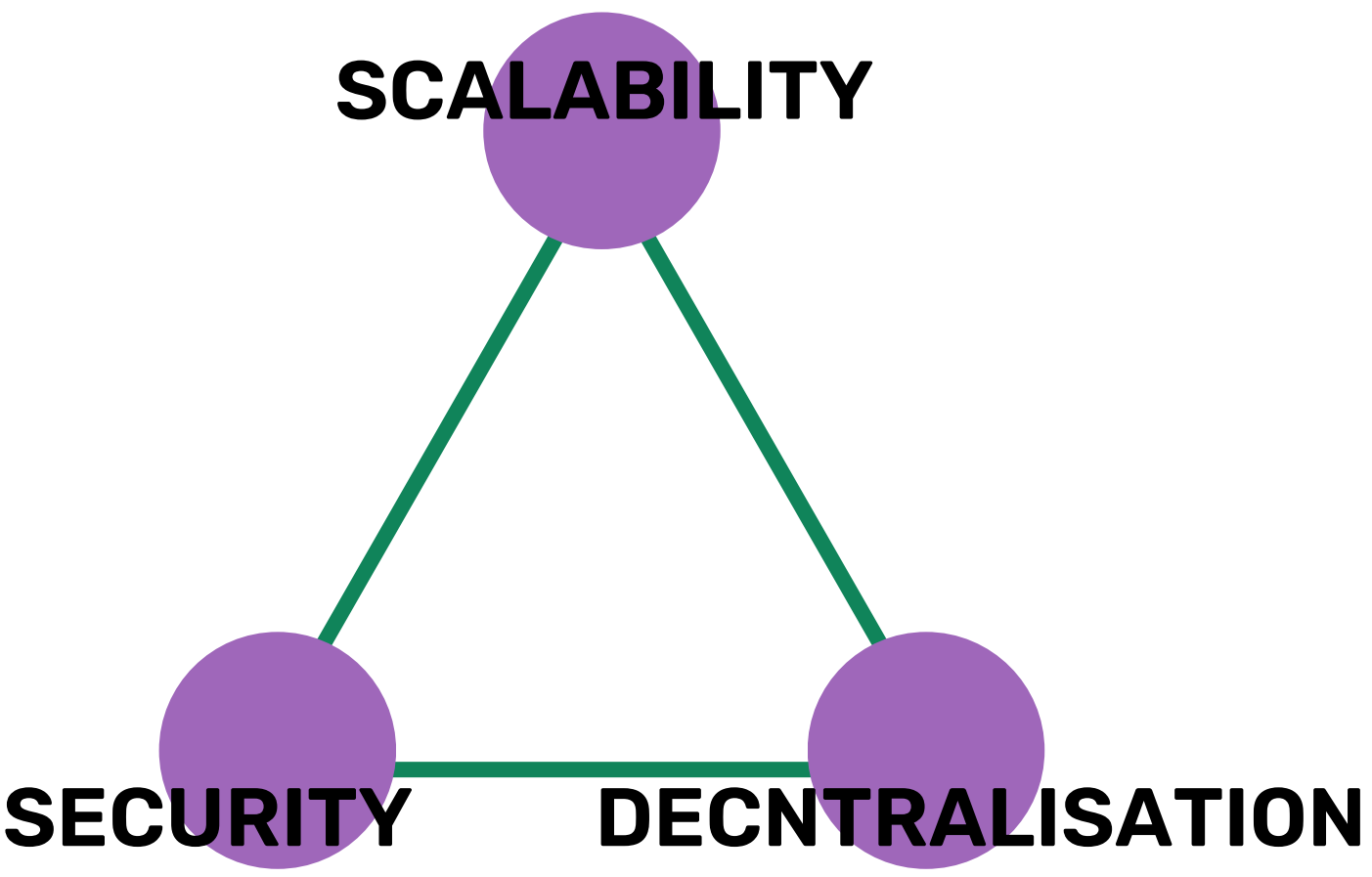
LAYER 1

The Importance of Nervos Network layers.

NERVOS BLOCKCHAIN

Multilayer Architecture

WHY IS A LAYERED ARCHITECTURE USED?



To provide a better balance to the blockchain Trilemma.

MEANING:

The Nervos Network's design enables a truly interoperable blockchain platform, by using different layers for important blockchain components.

THIS STARTS WITH LAYER 1

NERVOS BLOCKCHAIN

LAYER FOCUS

LAYER 1

FOCUS:

- Provide trust to higher layers
- Security
- Decentralisation

MEANING:

The CKB foundation layer supports the entire blockchain structure.

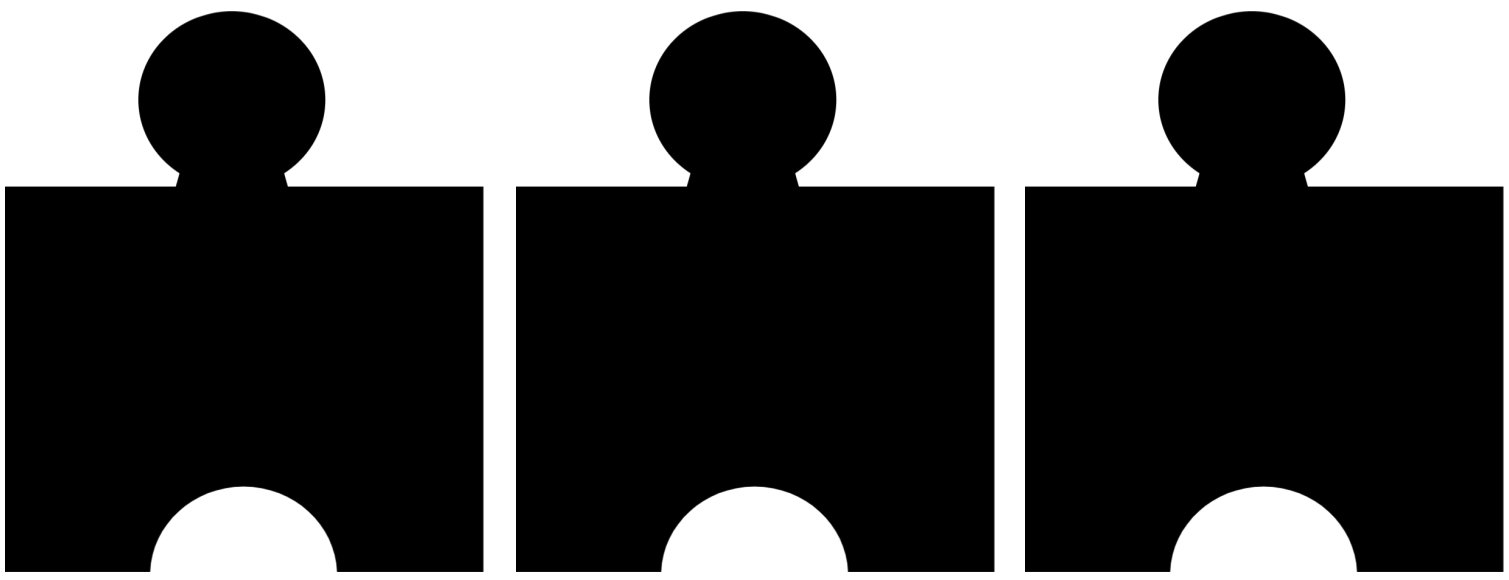
Every layer built on top, relies on this security and decentralisation.

Layers 2+ inherits this trust and can have a different focus.

NERVOS BLOCKCHAIN

LAYER FOCUS

LAYER 2 +



FOCUS:

- Scalability
- Providing almost instantaneous transactions

MEANING:

- Layer 2 and above are optimised for high throughput.

SCALABILITY:

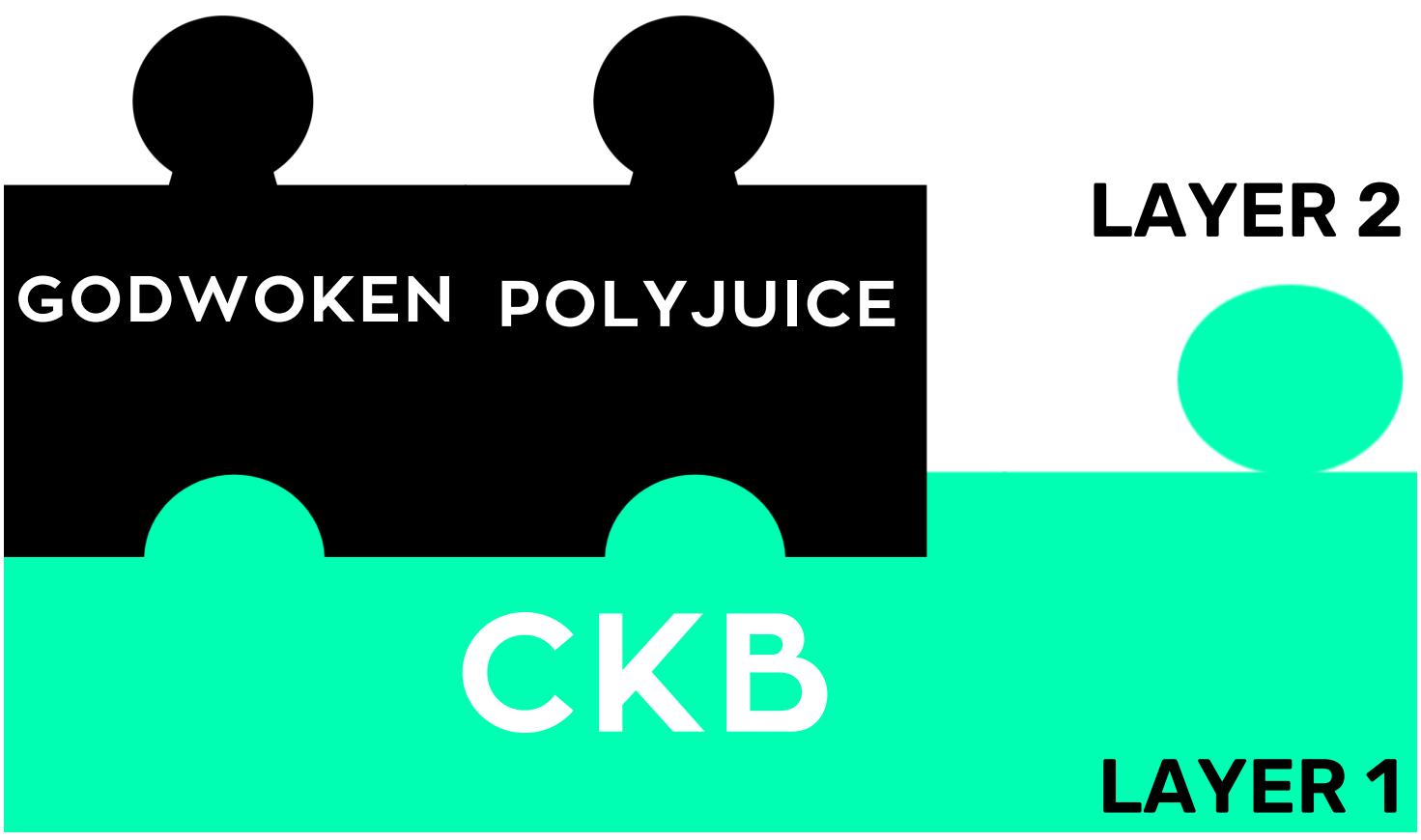
- The Nervos blockchain allows for unlimited levels of scalability.
- Any number of layers can be added to increase total network capacity.

While maintaining security and decentralisation.

NERVOS BLOCKCHAIN

LAYER FOCUS

WHAT ARE THE CURRENT LAYERS?



WHAT IS GODWOKEN?

Godwoken consists of two components.

GODWOKEN + POLYJUICE.

Godwoken the optimistic rollup framework.

Polyjuice the EVM compatibility framework.

MEANING:

These frameworks work together to create a scalable EVM compatible solution for Nervos.

NERVOS BLOCKCHAIN

LAYER FOCUS

WHAT IS AN OPTIMISTIC ROLLUP?

Optimistic rollup processes transactions outside of the Ethereum Mainnet.

MEANING:

Computation and data storage is moved off-chain.

Minimal information is published about transactions on-chain.

Automatically assumes all transactions are valid.

HOW?

Thousands of transactions are collected (**rollups)** in batches before being submitted to the Mainnet.

WHY?

- Reduces congestion on the base layer.
- Improves scalability

NERVOS BLOCKCHAIN
REVIEW

QUESTIONS ?

Q1. What does Layer 2 inherit from Layer 1?

Q2. What is the focus of layer 2?

Q3. Name the current layer 2?

Q4. What is the focus of layer 2?

Q5. What is the blockchain Trilema?

Q6. What is the Nervos blockchain's solution to the Trilemma?

Further information:

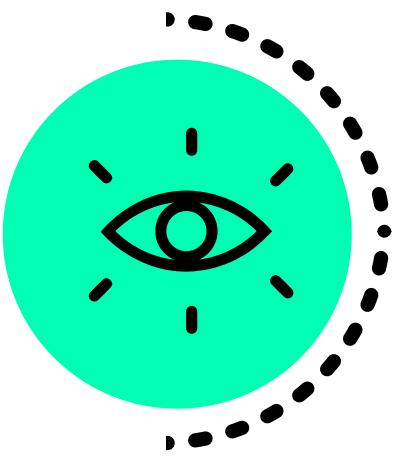
The Importance of Nervos Network layers.

NERVOS BLOCKCHAIN

4

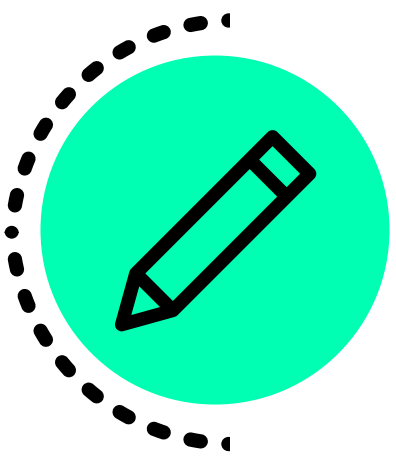
UNDERSTAND

How to build on Nervos.



DEFINE

- What do I need to know to build for each layer?
- Which Layer to get started with?



USEFUL TERMS:

SOLIDITY

RUST

LEARN MORE:

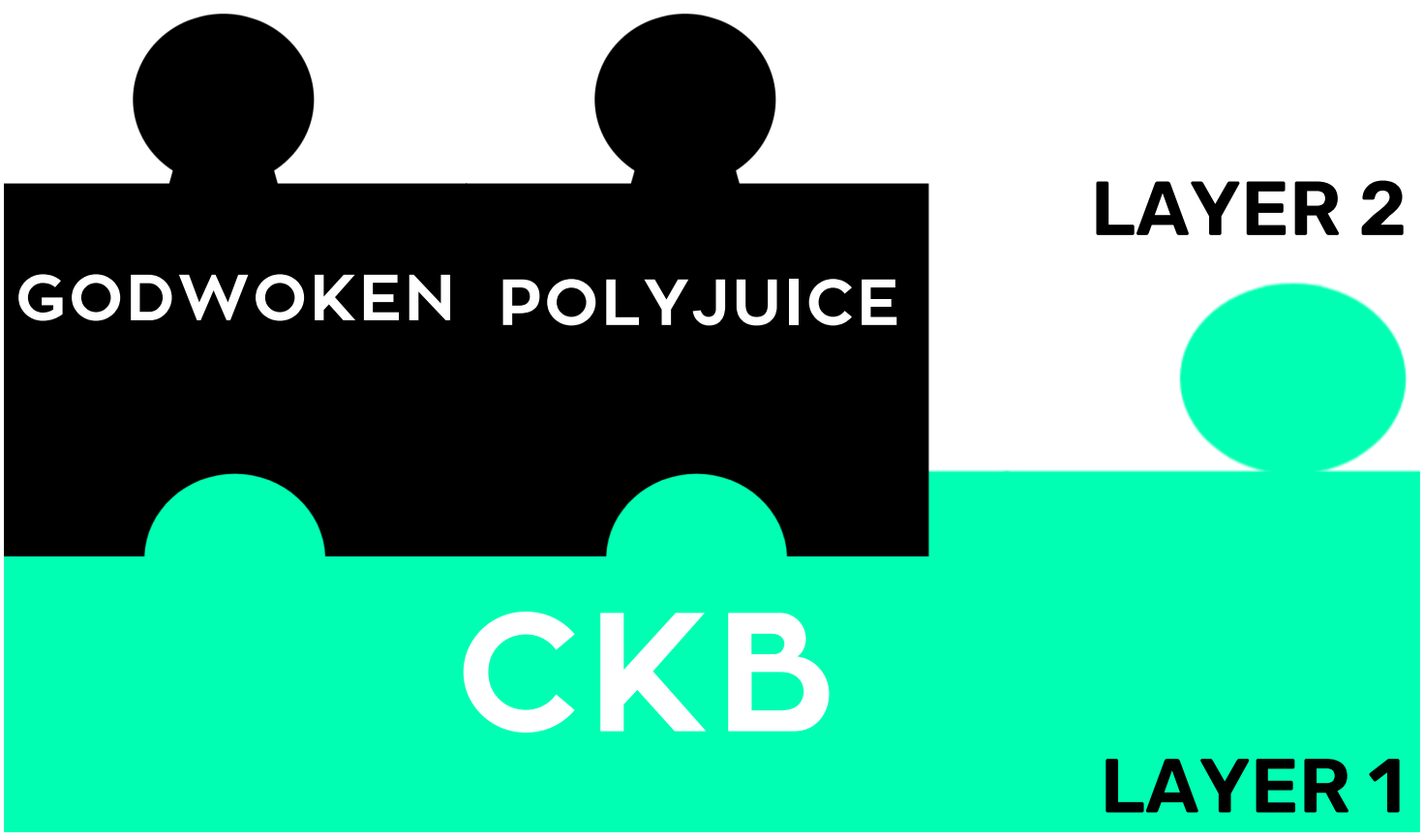
L1 DEVELOPER COURSE

L2 DEVELOPER COURSE

NERVOS BLOCKCHAIN

LAYER LANGUAGES

WHAT LANGUAGES CAN I CODE WITH?



LAYER 1 LANGUAGES:

Currently smart contracts can be coded in Rust, Javascript and C.

Design patterns are different from those used in Ethereum.

CKB-Virtual Machine executes smart contracts on Nervos.

LAYER 2 LANGUAGES:

Smart contract development is in Solidity.

NERVOS BLOCKCHAIN

DEVELOPMENT LAYER

WHICH LAYER IS BEST TO DEVELOP ON?

Layer 1's cell model design is more flexible, but development is more challenging.

BENEFITS:

- higher scalability
- flexibility
- re-usability

Layer 2 is a solution for developers familiar with Ethereum.

Or a beginner wanting to get started developing Dapps.

Developers receive the benefits of Ethereum's documentation, tooling and foundation.

START WITH EITHER LAYER. EACH LAYER REQUIRES A DIFFERENT APPROACH.

NERVOS BLOCKCHAIN

TOOLS

WHAT TOOLS DO I NEED FOR LAYER 1?

- Build Tools
- Curl
- Git
- Node.js 16.13.x (LTS)

SMART CONTRACT DEVELOPMENT

- Capsule (Rust).

WALLET

- PW-SDK + MetaMask

BACKEND:

- Express.Js + Lumos or PW-SDK

WHAT TOOLS DO I NEED FOR LAYER 2?

SMART CONTRACT DEVELOPMENT

- Remix, Hardhat or Truffle (Solidity).

WALLET

- PW-SDK + MetaMask

BACKEND:

- Express.js + Web3.js or Ethers.js

NERVOS BLOCKCHAIN

FRONTEND TOOLS

WHAT TOOLS DO I NEED FOR LAYER 1 OR LAYER 2?

FRONTEND:

Use whichever frontend is within your expertise.
There are many ways to display the design.

- React.js, Flutter, Unity e.t.c.

Build Something on Nervos Blockchain

LAYER 1

01

PLAN YOUR IDEA

Focus on building the features. How will the Dapp frontend connect to the smart contract code.

02

LEARN SCRIPTING

Do you know C, Rust or Javascript, you can get started scripting/ writing your smart contract Here.
Get Testnet tokens. Here.

03

LEARN DEVELOPMENT FRAMEWORK

Use Capsule to develop on-chain scripts in C and Rust. With Capsule, you build, compile, test and debug and deploy a new project. Here

04

LEARN TO SEND A TRANSACTION

Learn how to send a transaction from the CKB-command line tool. Here.
Learn how to use the command line Here.

05

CREATE A TOKEN

An example implementation of a token in Rust. Here

NERVOS BLOCKCHAIN

EXAMPLE L1 DAPPS

SIMPLE WALLET IMPLEMENTATION

A DAPP QUERYING BLOCKCHAIN, INTERACTING WITH CKB WALLETS BUILD SIGN SEND TRACK TRANSACTIONS.

Build Something on Nervos Blockchain

LAYER 2

01

PLAN YOUR IDEA

Focus on building the features. How will the Dapp frontend connect to the smart contract code.

02

LEARN SCRIPTING

Do you know Solidity you can get started scripting/ writing your smart contract Here. Get Testnet tokens. Here. Then transfer to Godwoken. Here.

03

LEARN DEVELOPMENT FRAMEWORK

Use Foundry, Remix, Hardhat or Truffle to develop on-chain scripts in Solidty. With these frameworks, you build, compile, test and debug and deploy a new project. Here

04

SETUP

Learn how to setup a Metamask wallet Here. Learn how to deploy a smart contract Here.

05

CREATE A TOKEN

An example implementation of a token in Solidity. Using Remix. Here

NERVOS BLOCKCHAIN

EXAMPLE L2 DAPPS

BUILT ON GODWOKEN

NERVOS BLOCKCHAIN

GLOSSARY

BLOCK

A GROUP OF TRANSACTIONS ENTERED INTO A BLOCKCHAIN; A RECORD THAT STORES DATA.

BLOCKCHAIN (CHAIN)

A SERIES OF BLOCKS THAT ARE BOUND TOGETHER USING CRYPTOGRAPHIC SIGNATURES.

BLOCK PROPAGATION

THE AMOUNT OF CRYPTOCURRENCY CREDITED TO A MINER'S ACCOUNT AFTER THE MINER SUCCESSFULLY ADDS A BLOCK OF TRANSACTIONS TO THE BLOCKCHAIN.

BLOCK INTERVAL

THE LENGTH OF TIME IT TAKES TO CREATE A NEW BLOCK IN A CRYPTOCURRENCY BLOCKCHAIN.

BLOCK REWARD

THE AMOUNT OF CRYPTOCURRENCY CREDITED TO A MINER'S ACCOUNT AFTER THE MINER SUCCESSFULLY ADDS A BLOCK OF TRANSACTIONS TO THE BLOCKCHAIN.

CELL

CELLS ARE THE PRIMARY STATE UNITS IN CKB. THEY HOLD THE AVAILABLE INFORMATION OF THE BLOCKCHAIN.

NERVOS BLOCKCHAIN

GLOSSARY

DAPP DECNTRALISED APPLICATION

DECENTRALIZED APPLICATION. BASICALLY, ANY APP THAT IS BUILT USING BLOCKCHAIN INFRASTRUCTURE. AT A MINIMUM, IT IS A SMART CONTRACT AND A WEB USER INTERFACE.

DEFI

DECENTRALISED FINANCE (DEFI) USES BLOCKCHAIN SMART CONTRACTS TO REMOVE THIRD PARTIES AND CENTRALISED INSTITUTIONS (BANKS) FROM FINANCIAL TRANSACTIONS.

HASH

A SERIES OF BLOCKS THAT ARE BOUND TOGETHER USING CRYPTOGRAPHIC SIGNATURES.

NATIVE TOKEN

THE USE OF BLOCKCHAIN TO REPRESENT THE VALUE OF A DIGITAL ASSET THAT IS NATIVE TO THE BLOCKCHAIN NETWORK. (A CKBYTE)

OFF-CHAIN

TRANSACTIONS RECORDED OUTSIDE THE UNDERLYING BLOCKCHAIN (E.G., TRANSFERS BY THIRD-PARTY WALLET SERVICE PROVIDERS BETWEEN THEIR USERS THAT ARE NOT RECORDED ON A PUBLIC BLOCKCHAIN).

ON-CHAIN

TRANSACTIONS RECORDED ON THE UNDERLYING BLOCKCHAIN.

NERVOS BLOCKCHAIN

GLOSSARY

WALLET

USER-FACING SOFTWARE USED TO INTERACT WITH ON-CHAIN ENTITIES SUCH AS ASSETS, SMART CONTRACTS AND DAPPS.

TBC...

NERVOS BLOCKCHAIN

EXTRA RESOURCES

BEGINNER RESOURCES

NERVOS BLOCKCHAIN