SMART CONTRACTS ON STELLAR

What they are, how they work,
and why they matter

LEIGH MCCULLOCH

VENDING MACHINES

STEP 1 OF 4

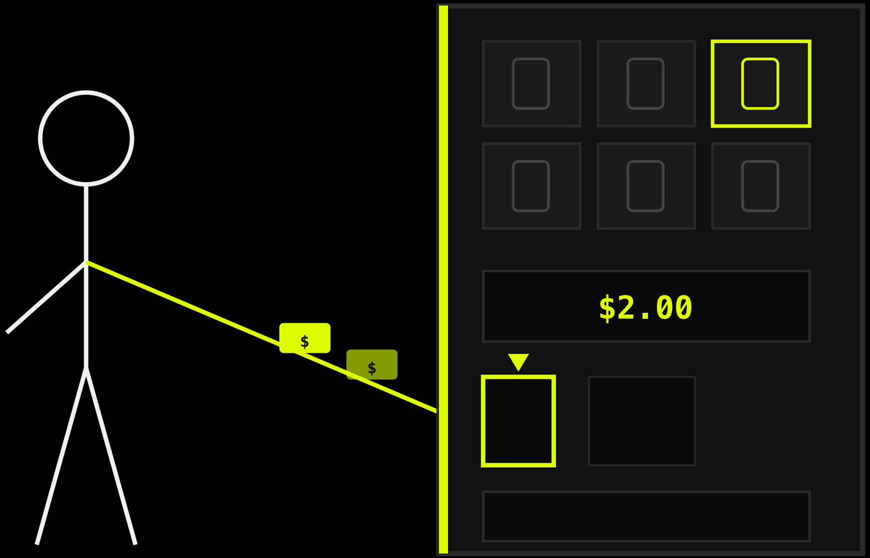
CHOOSE

STEP 2 OF 4

THE PRICE IS SHOWN

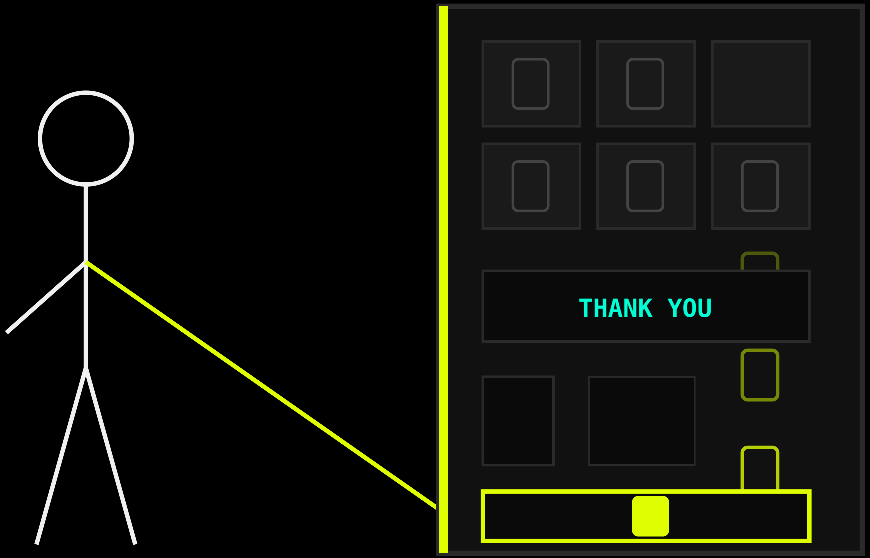
STEP 3 OF 4

YOUPAY



STEP 4 OF 4

SWAP COMPLETE



THE ANCESTOR OF SMART CONTRACTS

- **1880s** — Vending machines appear. Automated agreements, no human in the middle.
- **1994** — Computer scientist **Nick Szabo** sees the connection.
- He calls the vending machine the **"ancestor of smart contracts"** and coins the term.
- **14 years before Bitcoin. Even more before Ethereum.**

WHAT IS A SMART CONTRACT?

Take the vending machine pattern — an agreement that enforces itself.

Remove the physical machine. Just the logic.

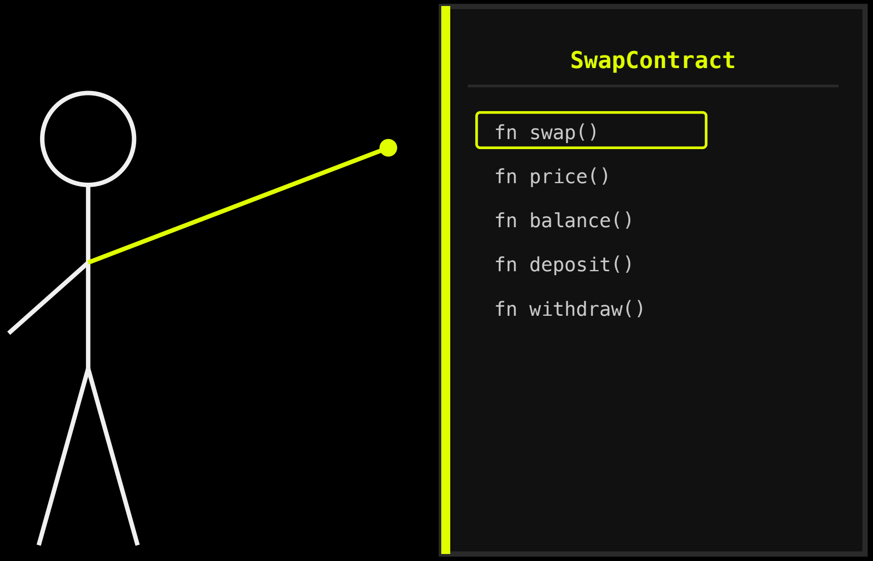
Put it on a network of computers that **nobody owns**.

Now anyone, anywhere, can use it.

AN AGREEMENT THAT ENFORCES ITSELF, RUNNING ON A COMPUTER NOBODY CONTROLS.

STEP 1 OF 4

IDENTIFY

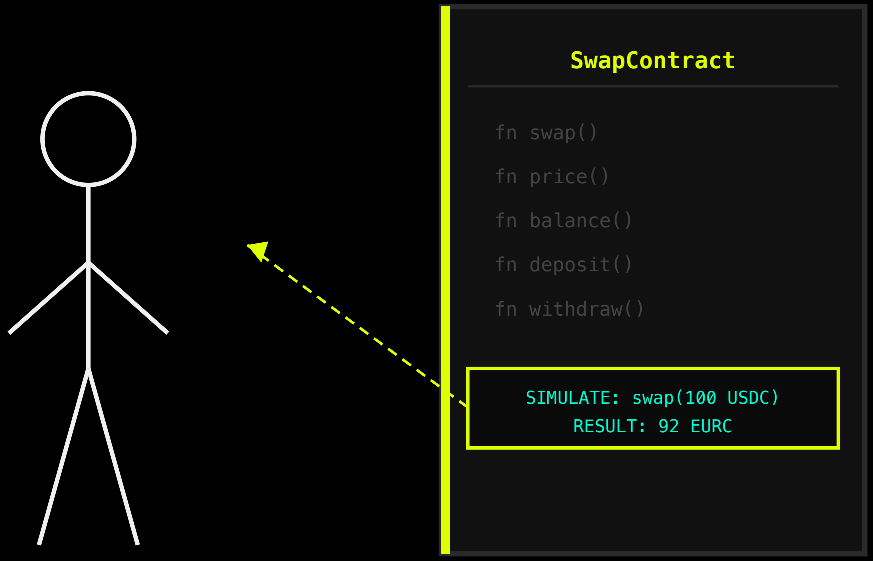


SwapContract

```
fn swap()
fn price()
fn balance()
fn deposit()
fn withdraw()
```

STEP 2 OF 4

SIMULATE



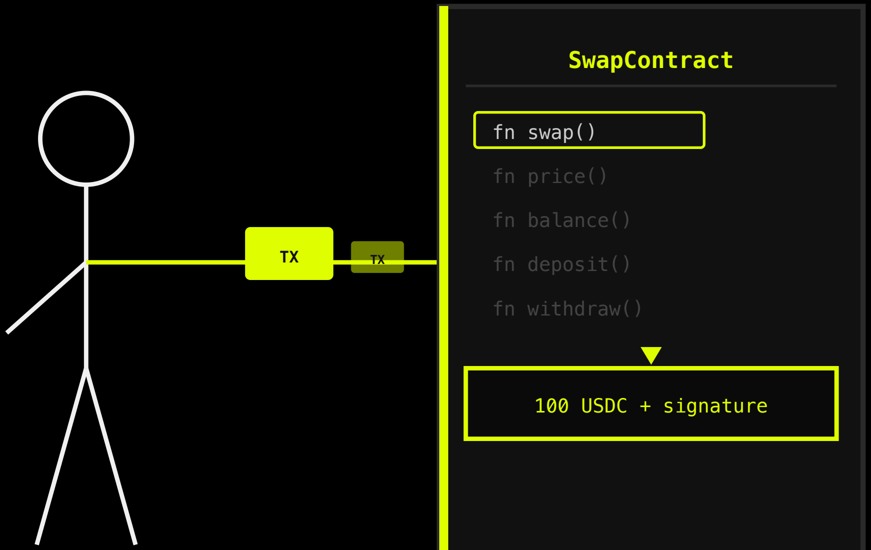
SwapContract

```
fn swap()
fn price()
fn balance()
fn deposit()
fn withdraw()
```

SIMULATE: swap(100 USDC)
RESULT: 92 EURC

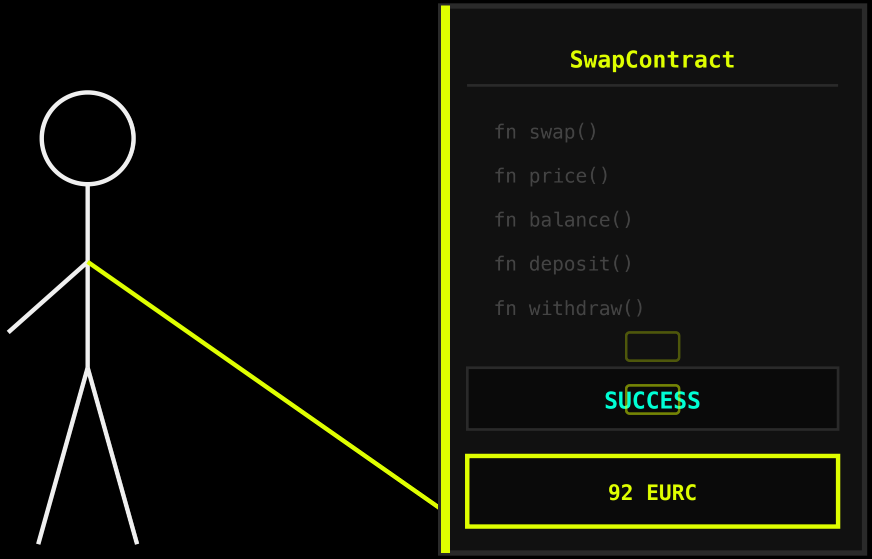
STEP 3 OF 4

SUBMIT



STEP 4 OF 4

EXECUTE



SwapContract

fn swap()

fn price()

fn balance()

fn deposit()

fn withdraw()

SUCCESS

92 EURC

THE STELLAR NETWORK

A blockchain founded in 2014, focused on **payments** and **financial access**. Think of it as a plaza where vending machines can be deployed.

2014
FOUNDED

~5s
SETTLEMENT

<$0.01
PER TXN

Global
ACCESS

STELLAR'S OG VENDING MACHINE

- **26 built-in operations** — send payments, create offers, manage trust
- A built-in decentralized exchange
- Like a machine with **26 preset buttons**
- Useful — but you couldn't add new buttons
- Want something not on the menu? **Convince the whole network to add a 27th button**

SOROBAN: THE PROGRAMMABLE MACHINE

FEBRUARY 2024 — LIVE ON STELLAR

Soroban — Stellar's smart contract platform

Written in **Rust**, compiled to **WebAssembly**

Anyone can build a **new machine** with custom rules

Not just 26 buttons — **unlimited possibilities**

The old preset buttons still work too

WAS STELLAR THE FIRST SMART CONTRACT BLOCKCHAIN?

No.

> **Ethereum** (2015) — the first general-purpose smart contract platform
>
> Vitalik Buterin saw Bitcoin's limitations and built a blockchain **designed for programmable contracts**
>
> Solidity, the EVM, gas — Ethereum defined the vocabulary
>
> Since then: Solana, Avalanche, Polkadot, and many more
>
> Stellar chose to **wait and learn** — then build Soroban

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE

Code + Tests

2. AUDIT

Review +
Verify

3. COMPILE

.wasm file

4. UPLOAD

To the network

5. DEPLOY

Create an instance

6. USE

Call, interact, compose

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE

Code + Tests

2. AUDIT

Review + Verify

3. COMPILE

.wasm file

4. UPLOAD

To the network

5. DEPLOY

Create an instance

6. USE

Call, interact, compose

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE

Code + Tests

2. AUDIT

Review +
Verify

3. COMPILE

.wasm file

4. UPLOAD

To the network

5. DEPLOY

Create an instance

6. USE

Call, interact, compose

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE

Code + Tests

2. AUDIT

Review + Verify

3. COMPILE

.wasm file

4. UPLOAD

To the network

5. DEPLOY

Create an instance

6. USE

Call, interact, compose

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE

Code + Tests

2. AUDIT

Review + Verify

3. COMPILE

.wasm file

4. UPLOAD

To the network

5. DEPLOY

Create an instance

6. USE

Call, interact, compose

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE
Code + Tests

2. AUDIT
Review + Verify

3. COMPILE
.wasm file

4. UPLOAD
To the network

5. DEPLOY
Create an instance

6. USE
Call, interact, compose

CDLZFC3SYJYDZT7K67VZ75HPJVIEUVNIXF47ZG2FB2RMQQVU2HHGCYSC

LIFECYCLE OF SMART CONTRACT DEVELOPMENT

1. WRITE

Code + Tests

2. AUDIT

Review + Verify

3. COMPILE

.wasm file

4. UPLOAD

To the network

5. DEPLOY

Create an instance

6. USE

Call, interact, compose

CDLZFC3SYJYDZT7K67VZ75HPJVIEUVNIXF47ZG2FB2RMQQVU2HHGCYSC

THE BUILDING BLOCKS

Every contract has some common components.

Logic

THE RULES. WHAT HAPPENS WHEN YOU PUSH A BUTTON.

Storage

THE MACHINE'S MEMORY. INSTANCE, PERSISTENT, OR TEMPORARY.

Auth

REQUIRE_AUTH() — VERIFY WHO'S PUSHING THE BUTTON.

Events

RECEIPTS. A LOG OF EVERYTHING THAT HAPPENED.

Cross-Call

MACHINES CAN CALL OTHER MACHINES.

THE BUILDING BLOCKS

Every contract has some common components.

Logic

THE RULES. WHAT HAPPENS WHEN YOU PUSH A BUTTON.

Storage

THE MACHINE'S MEMORY. INSTANCE, PERSISTENT, OR TEMPORARY.

Auth

REQUIRE_AUTH() — VERIFY WHO'S PUSHING THE BUTTON.

Events

RECEIPTS. A LOG OF EVERYTHING THAT HAPPENED.

Cross-Call

MACHINES CAN CALL OTHER MACHINES.

THE BUILDING BLOCKS

Every contract has some common components.

Logic

THE RULES. WHAT HAPPENS WHEN YOU PUSH A BUTTON.

Storage

THE MACHINE'S MEMORY. INSTANCE, PERSISTENT, OR TEMPORARY.

Auth

REQUIRE_AUTH() — VERIFY WHO'S PUSHING THE BUTTON.

Events

RECEIPTS. A LOG OF EVERYTHING THAT HAPPENED.

Cross-Call

MACHINES CAN CALL OTHER MACHINES.

THE BUILDING BLOCKS

Every contract has some common components.

Logic

THE RULES. WHAT HAPPENS WHEN YOU PUSH A BUTTON.

Storage

THE MACHINE'S MEMORY. INSTANCE, PERSISTENT, OR TEMPORARY.

Auth

REQUIRE_AUTH() — VERIFY WHO'S PUSHING THE BUTTON.

Events

RECEIPTS. A LOG OF EVERYTHING THAT HAPPENED.

Cross-Call

MACHINES CAN CALL OTHER MACHINES.

THE BUILDING BLOCKS

Every contract has some common components.

Logic

THE RULES. WHAT HAPPENS WHEN YOU PUSH A BUTTON.

Storage

THE MACHINE'S MEMORY. INSTANCE, PERSISTENT, OR TEMPORARY.

Auth

REQUIRE_AUTH() — VERIFY WHO'S PUSHING THE BUTTON.

Events

RECEIPTS. A LOG OF EVERYTHING THAT HAPPENED.

Cross-Call

MACHINES CAN CALL OTHER MACHINES.

THE BUILDING BLOCKS

Every contract has some common components.

Logic

THE RULES. WHAT HAPPENS WHEN YOU PUSH A BUTTON.

Storage

THE MACHINE'S MEMORY. INSTANCE, PERSISTENT, OR TEMPORARY.

Auth

REQUIRE_AUTH() — VERIFY WHO'S PUSHING THE BUTTON.

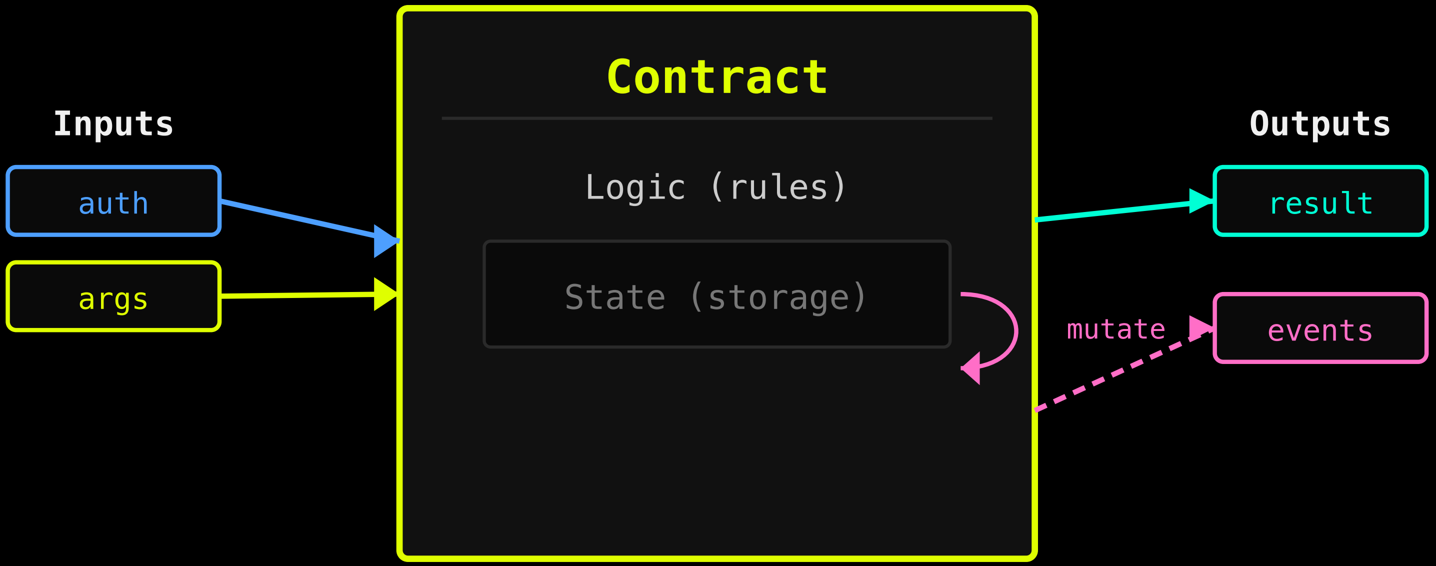
Events

RECEIPTS. A LOG OF EVERYTHING THAT HAPPENED.

Cross-Call

MACHINES CAN CALL OTHER MACHINES.

HOW A CONTRACT WORKS



WHY DO SMART CONTRACTS MATTER?

SDF MISSION

CREATE EQUITABLE ACCESS TO THE GLOBAL FINANCIAL SYSTEM.

Smart contracts let anyone build the financial services that make this possible.

EXAMPLES

Tokens

CREATE AND MANAGE ANY DIGITAL ASSET

Swaps

EXCHANGE ONE ASSET FOR ANOTHER

Lending

BORROW AND LEND WITH PROGRAMMABLE TERMS

Liquidity

POOL ASSETS SO ANYONE CAN TRADE

Insurance

AUTOMATED PAYOUTS WHEN CONDITIONS ARE MET

Payments

PROGRAMMABLE MONEY FLOWS AND SPLITS

Savings

EARN YIELD ON DEPOSITED ASSETS

Escrow

HOLD FUNDS UNTIL CONDITIONS ARE MET

Payroll

AUTOMATED RECURRING DISTRIBUTIONS

Crowdfund

RAISE CAPITAL WITH TRANSPARENT RULES

Invoicing

PROGRAMMABLE BILLING AND SETTLEMENT

Custody

MULTI-SIG AND PROGRAMMABLE ACCESS CONTROL

TOKENS CAN REPRESENT ANYTHING

Same interface. Same transfer, balance, approve. Different meaning.

USDC

US DOLLARS, ON-CHAIN. REDEEMABLE 1:1.

LOYALTY

REWARD POINTS. EARN, TRANSFER, REDEEM.

TICKET

EVENT ACCESS. VERIFIABLE, TRADEABLE.

SHARE

OWNERSHIP. DIVIDENDS, VOTING RIGHTS.

ONE MACHINE PATTERN.

INFINITE USE CASES.

EXAMPLES ON STELLAR

Blend
Lending

Soroswap
Swaps

Sushi
Swaps

Reflector
Price Oracle

Axelar
Bridge

FxDAO
Stablecoin

Soroban Domains
Naming Service

Kale
Mining Game

DeFindex
Index Vaults

Soroswap Aggregator
DEX Aggregator

Batch Executor
Batch Operations

...

A SMALL SAMPLE — MANY MORE ARE LIVE AND BEING BUILT

Tokens

CREATE AND MANAGE ANY DIGITAL ASSET

Swaps

EXCHANGE ONE ASSET FOR ANOTHER

Lending

BORROW AND LEND WITH PROGRAMMABLE TERMS

Liquidity

POOL ASSETS SO ANYONE CAN TRADE

Insurance

AUTOMATED PAYOUTS WHEN CONDITIONS ARE MET

Payments

PROGRAMMABLE MONEY FLOWS AND SPLITS

Savings

EARN YIELD ON DEPOSITED ASSETS

Escrow

HOLD FUNDS UNTIL CONDITIONS ARE MET

Payroll

AUTOMATED RECURRING DISTRIBUTIONS

Crowdfund

RAISE CAPITAL WITH TRANSPARENT RULES

Invoicing

PROGRAMMABLE BILLING AND SETTLEMENT

Custody

MULTI-SIG AND PROGRAMMABLE ACCESS CONTROL

Voting

TRANSPARENT, AUDITABLE GOVERNANCE

Supply Chain

TRACK PROVENANCE, EACH STEP IMMUTABLE

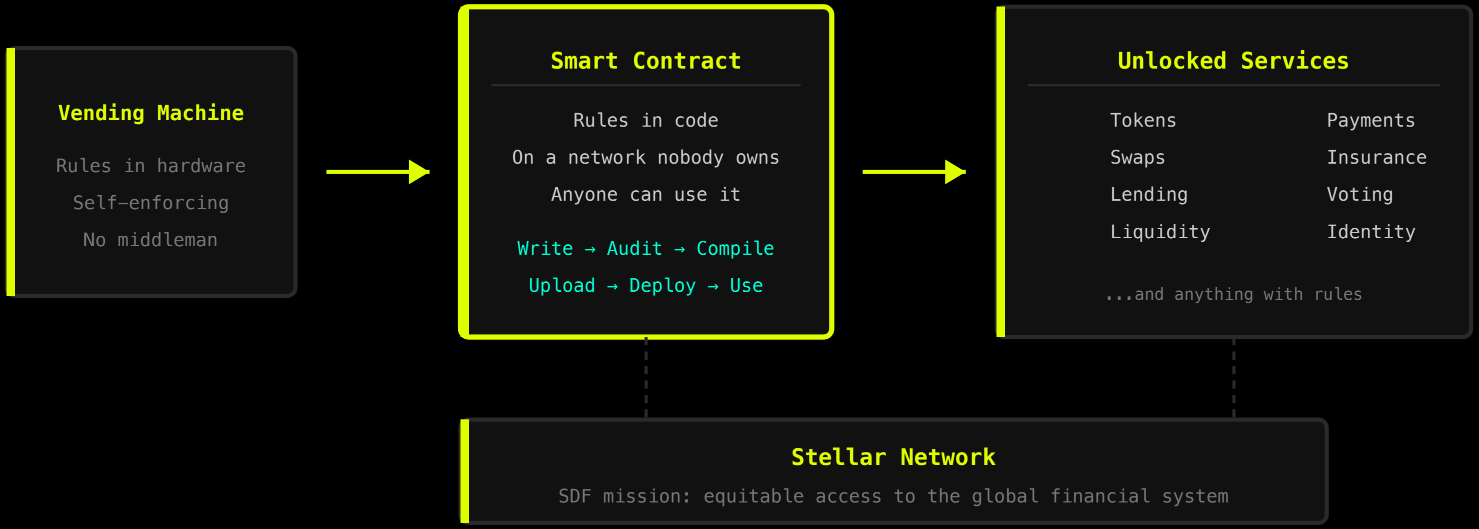
Gaming

IN-GAME ITEMS AS REAL TRADEABLE TOKENS

Identity

PROVE THINGS WITHOUT REVEALING EVERYTHING

RECAP



Vending Machine

Rules in hardware

Self-enforcing

No middleman

Smart Contract

Rules in code

On a network nobody owns

Anyone can use it

Write → Audit → Compile

Upload → Deploy → Use

Unlocked Services

- Tokens
- Swaps
- Lending
- Liquidity
- Payments
- Insurance
- Voting
- Identity

...and anything with rules

Stellar Network

SDF mission: equitable access to the global financial system

QUESTIONS?

DEVELOPERS.STELLAR.ORG