The need of a feature!

-> Let's say, an election is ongoing between Trump & Kamala.

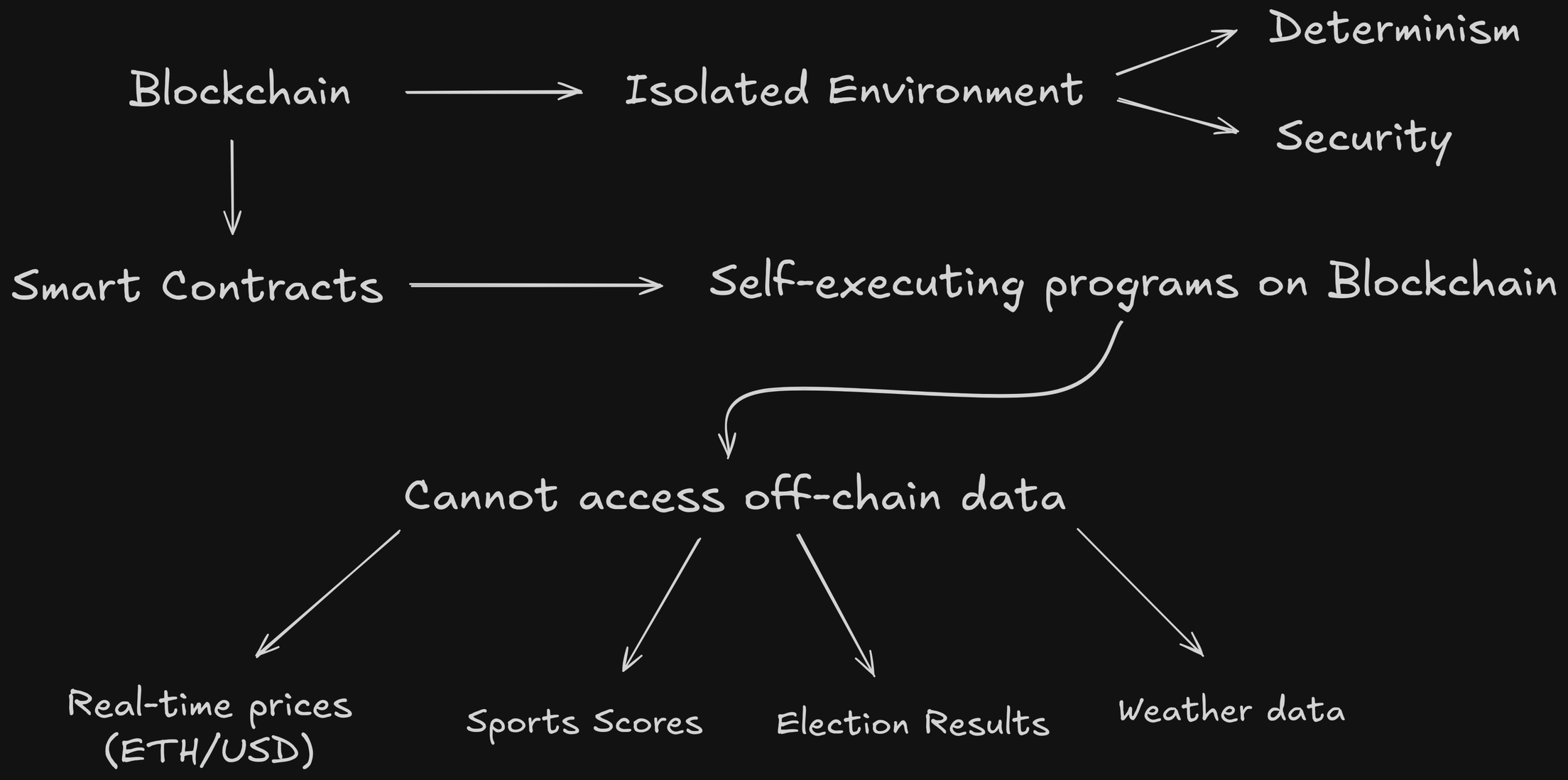
-> Alice comes in and bets 20 USDC in favour of Trump.
Bob comes in and bets 20 USDC in favour of Kamala.

-> Total money in the smart contract pool is 40 USDC.

-> Election Results come out, how will the smart contract decide who won the electon?

-> A feature is needed to fetch the event's result.

A Smart Contract Limitation



Let's Meet Oracles!

Blockchains → Isolated by design

↓

Smart Contracts → Disconnected from real word Info

Q - How do we connect blockchain to real world info?

Oracles → Connect Blockchain to External System

↓

Input + Output access of real world → Smart Contract working on real world Info

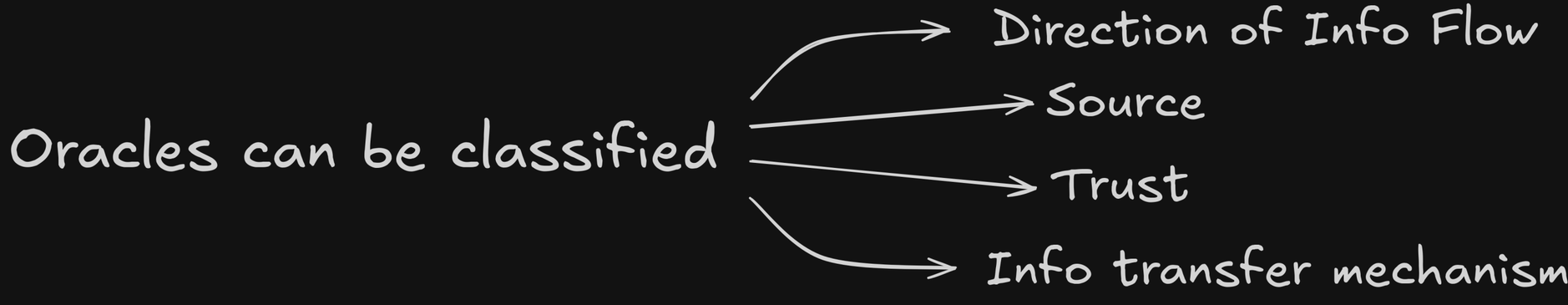
Oracles

-> Provide smart contracts with external information.

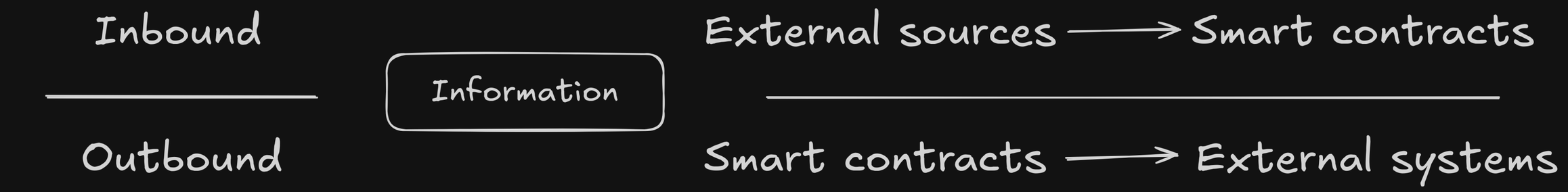
-> Third-party services.

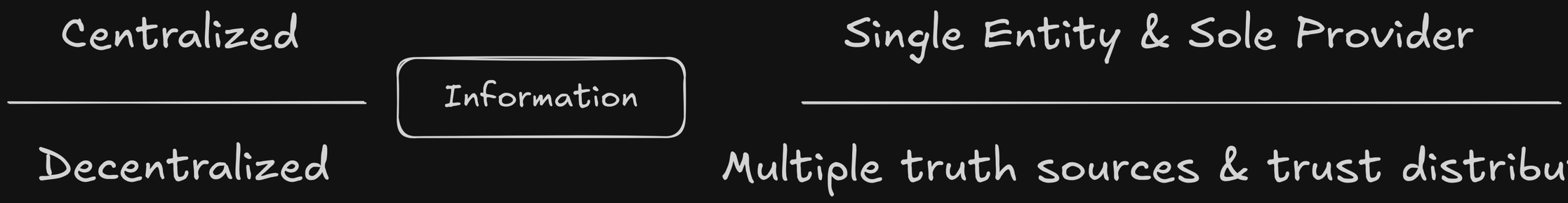
-> Act as a bridge between blockchains and the outside world.

-> Expands functionality by enabling smart contracts to access data beyond their native networks.



Variety of Real World Information!
Types of Oracles!





Variety of Real World Information!
Types of Oracles!

Push

Information

Pull

Without request ⟶ Smart contract

Oracle ⟵ Query ⟵ Smart contract

Data ⟶ Smart contract

Software

Information

Hardware

Online Sources ⟶ Smart contracts

Physical World ⟶ Smart contracts

Check these Oracles

Chainlink Oracle

The most popular

UMA Oracle

UMA' s optimistic oracle
used by Polymarket

Band Protocol

Flare Time Series Oracle

We have a problem!

-> An Indian freelancer does some work for a client in Europe.

-> Gets paid in Bitcoin by the client.

-> By the time the freelancer converts it to rupees, Bitcoin's value drops by 10%.

-> Hence, income was cut by 10%

-> Need to receive crypto payments without worrying about price swings.

-> Something stable and reliable is needed.

Stablecoins in the game!

ETH/Bitcoin → Price Volatility

Stablecoins → Price Stability

Stablecoins →
- Designed in such a way to prevent massive fluctuation like US Dollar & EURO.
- Main goal is to maintain stability.
- Simply put, crypto equivalent of the US dollar (most cases)

Use Cases

-> Price Stability ⟶ Stablecoins pegged to stable assets like the USD.
1 stablecoin ≈ 1 USD.

-> Efficient Trading & Settlement ⟶ Safety during market dips.
Transfer volatile assets.

-> Stable DeFi Ecosystem ⟶ Providing liquidity to AMMs.
Yield farming and staking.

-> Cross-border Transfers ⟶ Fast, low-cost international money transfer.

-> Smart contract interactions ⟶ Using stablecoins removes
uncertainty from token prices.

What "stable" really means

-> Stablecoins maintain a consistent value wrt reference asset (usually $1 USD).

-> Goal ⟶ Preserve Value, Not Grow in Value

Increase or Decrease in Value

Minor Fluctuations →
- Stablecoins fluctuate slightly due to supply-demand imbalances or market liquidity.
  - → Usually corrected via arbitrage.
- Against other currencies ⟶ Changes are similar as wrt USD

Types of Stablecoins

Fiat-collateralized stablecoins ⟶ Most common

Crypto-collateralized stablecoins ⟶ Less dependent on centralized institutions

Commodity-collateralized stablecoins ⟶ Real Asset Backing

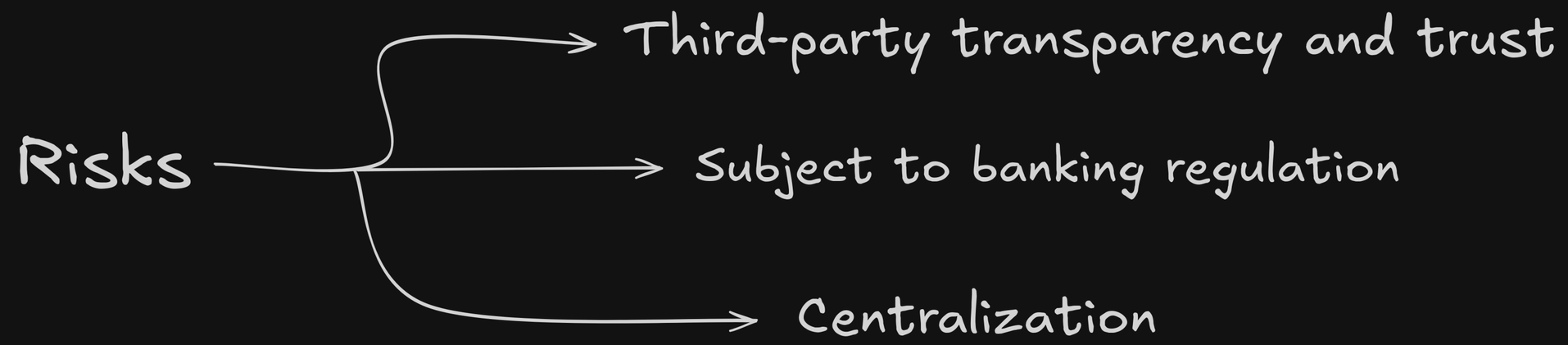
Algorithmic stablecoins ⟶ Decentralized but very risky

Fiat-collateralized stablecoins

Each token is backed by a reserve of fiat currency, typically US dollars.

Hold appropriate amount of dollars in bank accounts for every token being circulated.

Major players are USDT by Tether and USDC by Circle



Crypto-collateralized stablecoins

Backed other cryptocurrencies → ETH/BTC
→ Other currencies treated as assets

User locks crypto assets in a smart contract vault. Smart contract mints stablecoins.

DAI by MakerDAO is the major player

Risks →
- Too many volatile affecting factors
- Risk of Overcollateralization
- Volatility

Commodity-collateralized stablecoins

Backed by real-world commodities → Gold (PAXG, XAUT)
→ Oil
→ Other raw materials

Tokens are pegged to the market value of the commodity.

Risks → Less liquid than fiat-backed stablecoins
→ Custody Risk of Commodities
→ Transparency

Algorithmic stablecoins

No backing of any collateral → Algorithms & Smart contracts
→ Without any collateral

Algorithmic stablecoins typically use a dual-token model → Stablecoin
→ Volatility-absorbing token

UST (Terra) Collapse

Risks → No Factor of Real-World Backing
→ Risky Design
→ Algorithm must be impeccable
Peg can collapse quickly