Blockchain Technology and Systems

(SEZG569/SSZG569)

BITS Pilani
Pilani Campus

Dr. Ashutosh Bhatia
Department of Computer Science and Information Systems

Why a course on Blockchain?

What is all the excitement about?

1) **Basic application:** a digital currency (stored value)
   - Current largest: Bitcoin (2009), Ethereum (2015)
   - Global: accessible to anyone with an Internet connection

2) **Beyond stored value:** decentralized applications (DAPPs)
   - **DeFi:** financial instruments managed by public programs (examples: stablecoins, lending, exchanges, ….)
   - **Asset management (NFTs):** art, game assets, domain names.
   - **Decentralized organizations (DAOs):** (decentralized governance) DAOs for investment, for donations, for collecting art, etc.

3) **New programming model:** writing decentralized programs

What is a blockchain?

Abstract answer: a blockchain provides

- coordination between many parties,
- when there is no single trusted party

if trusted party exists ⇒ no need for a blockchain

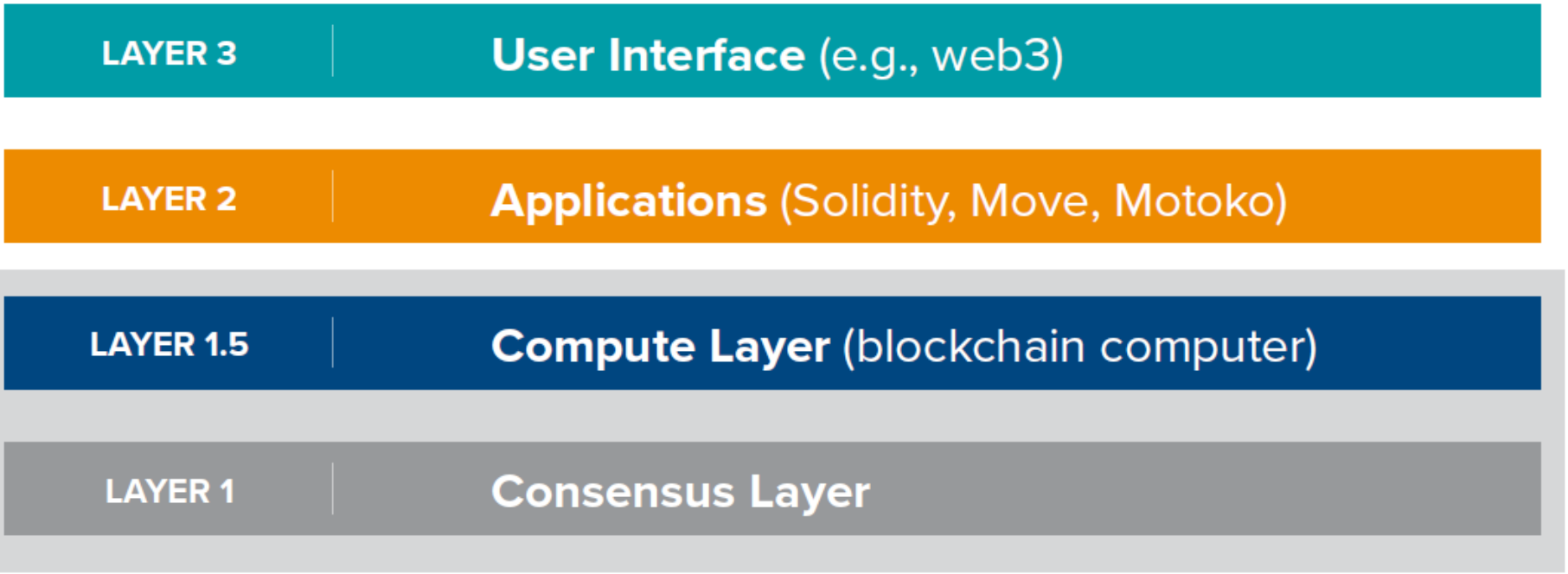
[financial systems: often no trusted party]

What is Blockchain?

- A Linked List
  - Replicated
  - Distributed
  - Consistency maintained by Consensus
  - Cryptographically linked
  - Cryptographically assured integrity of data

- Used as
  - Immutable Ledger of events, transactions, time stamped data
  - Tamper resistant log
  - Platform to Create and Transact in Cryptocurrency
  - log of events/transactions unrelated to currency

What is a blockchain?



Layer 1: Consensus Layer (Informal)

achieved by replication

A **public** append-only data structure:

- **Persistence**: once added, data can never be removed*
- **Safety**: all honest participants have the same data**
- **Liveness:** honest participants can add new transactions
- **Open(?)**: anyone can add data (no authentication)

This Not a New Problem …

State machine replication: studied since the 1980s

Google, Amazon, Banks, all have lots of servers:

- need to ensure state is consistent across all servers
- Known # of servers, and all are authorized.

New aspect: open consensus

- Anyone can write new data to the blockchain
- Was shown to be impossible! [Barak, Canetti et. al 05]
- Nakamoto [2008]
  - A way to bypass the bound using proof of work

Open Consensus: How?

PROOF-OF-WORK

First party to solve puzzle creates next block

- sybil resistant selection of a random party

Problems:

- slow, wastes energy

bitcoin

ethereum

PROOF-OF-STAKE

Fast block creation

No energy waste

But more complex

ethereum

Tendermint

DFINITY

celo

Algorand

PROOF-OF-SPACE

chia

Filecoin

MANY MORE IDEAS

SOLANA

Layer 1.5: The blockchain computer

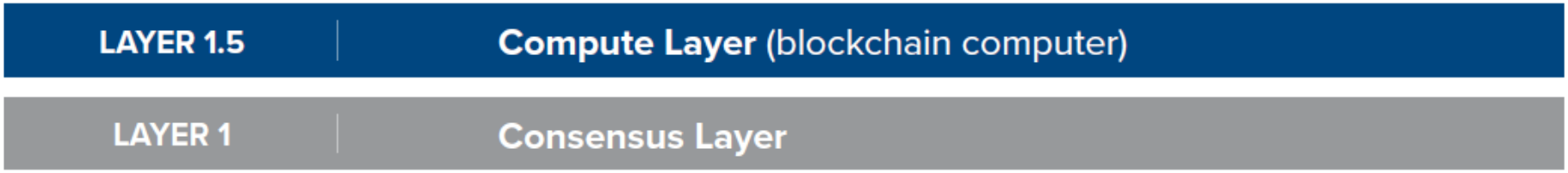
APP logic is encoded in a program that runs on blockchain

- Rules are enforced by a public program (public source code)

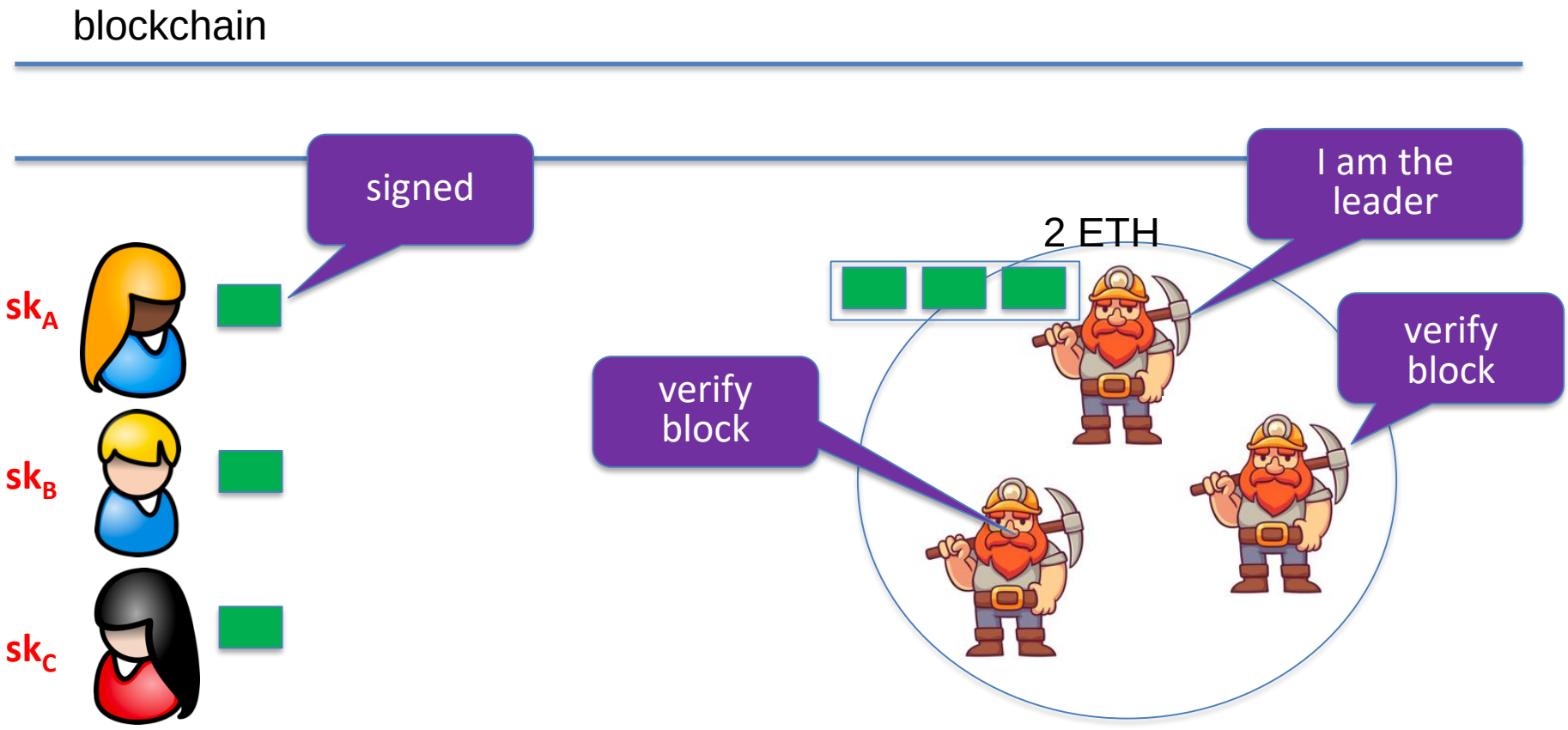
  ⇒ **transparency**: no single trusted 3rd party

- The DAPP program is executed by parties who create new blocks

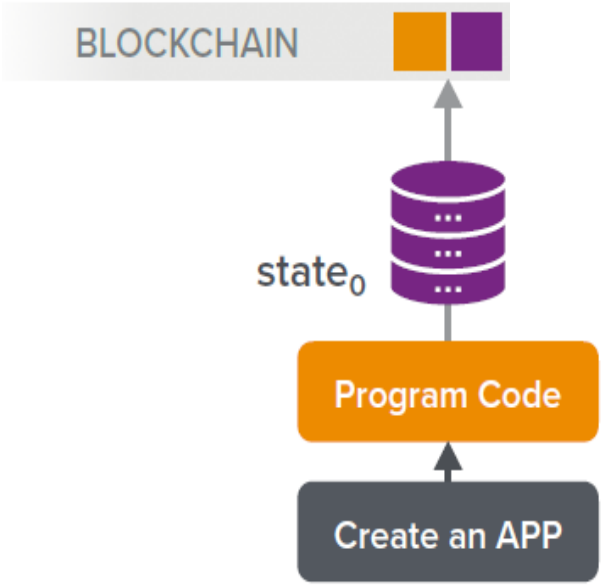
  ⇒ **public verifiability**: everyone can verify state transitions



How are blocks added to chain?



Running Programs on a Blockchain (APPs)



LAYER 1.5	**Compute Layer** (blockchain computer)
LAYER 1	Consensus Layer

Execution Environment

innovate achieve lead

BITCOIN SCRIPT

LIMITED COMPUTING ENVIRONMENT

- Limited instruction set (no loops)
- Sufficient for some tasks:
  - atomic swaps
  - payment channels, …

ETHEREUM

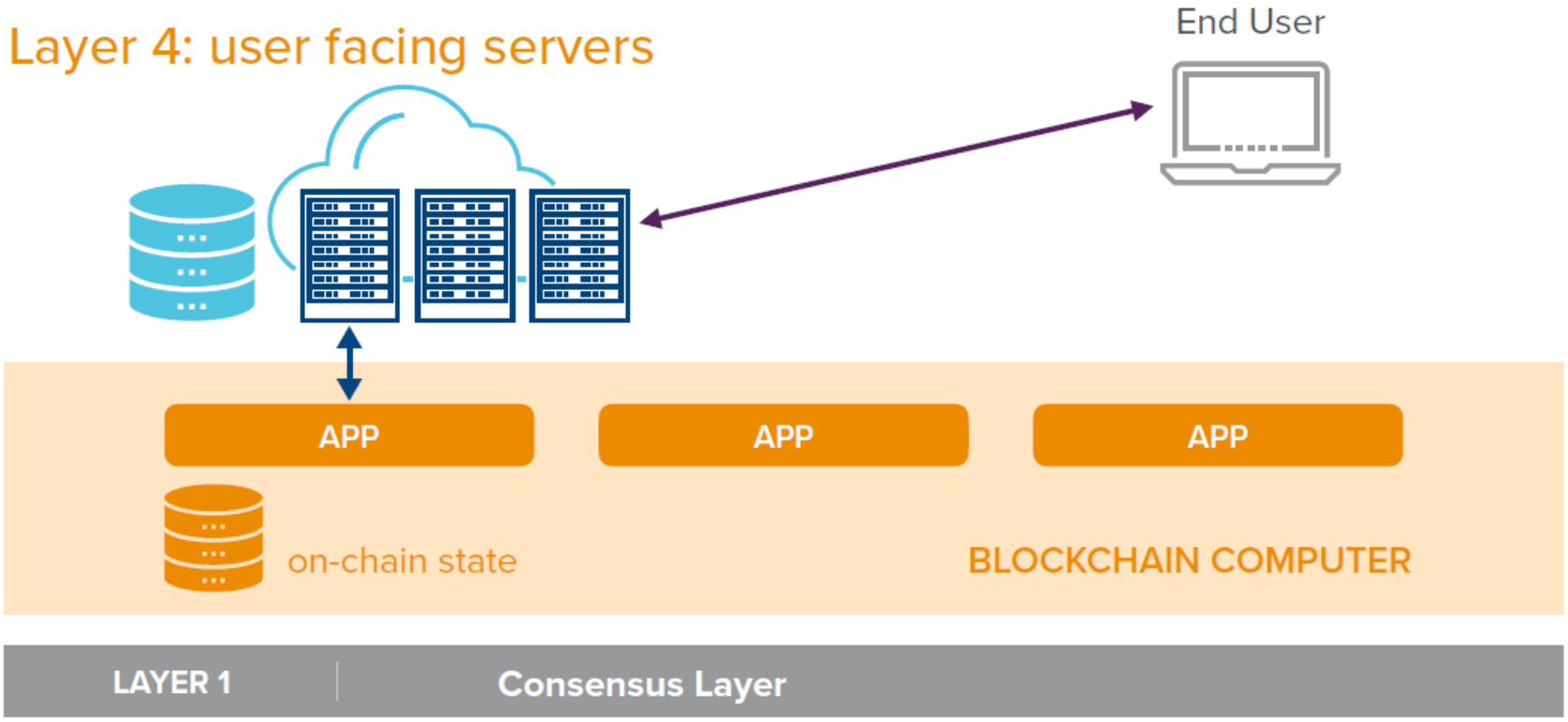
GENERAL PROGRAMMING ENVIRONMENT (SOLIDITY)

- EVM is a general purpose computing environment
- APP code updates internal state in response to transactions
- Calling APP costs fees (gas)
  - prevents DoS on miners
  - **storing on-chain state costs fees**

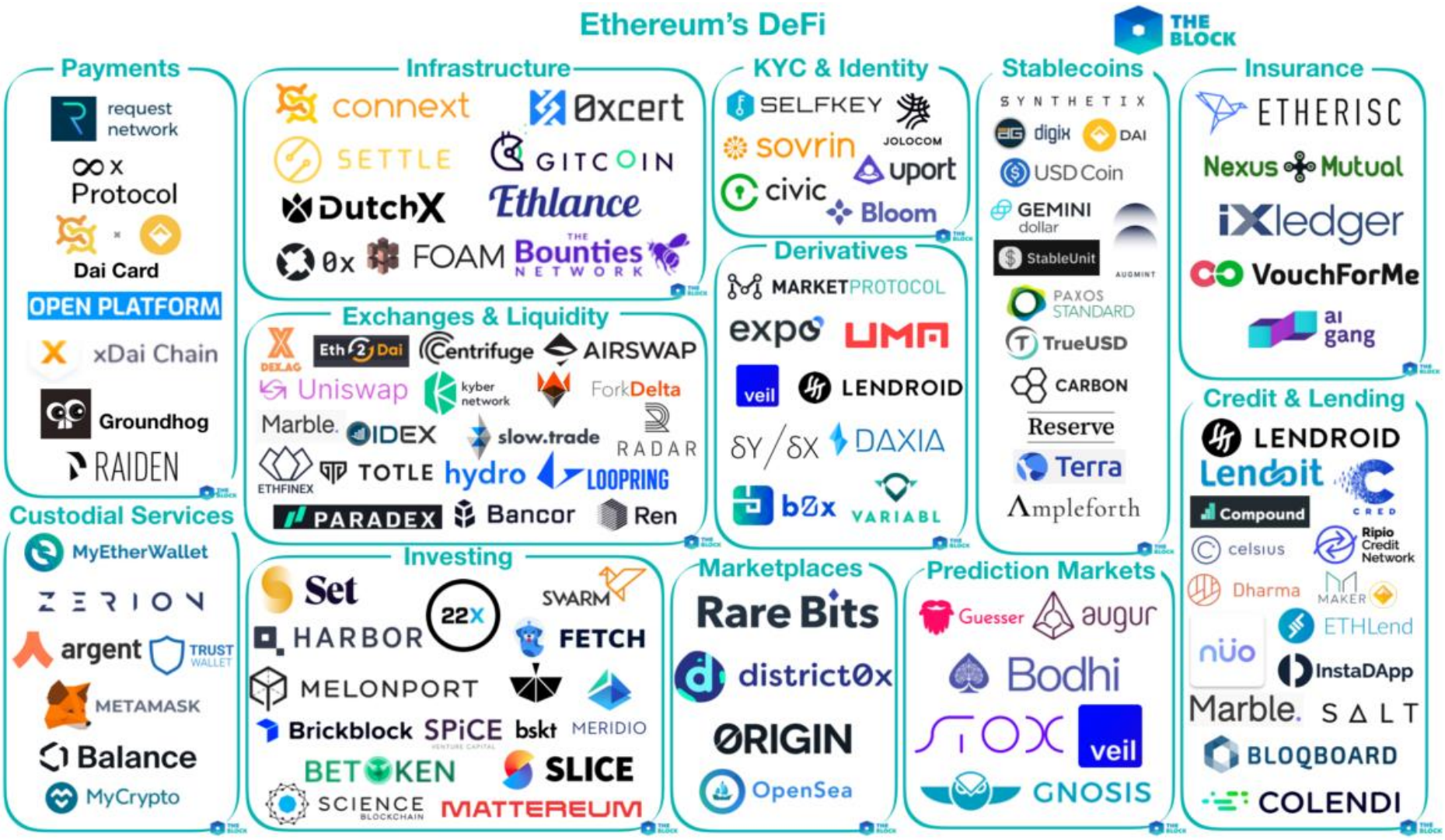
Decentralized Applications (DAPPs)

LAYER 2	**Applications** (Solidity, Move, Motoko)
LAYER 1.5	**Compute Layer** (blockchain computer)
LAYER 1	**Consensus Layer**

Common App Architecture



Ethereum DeFi

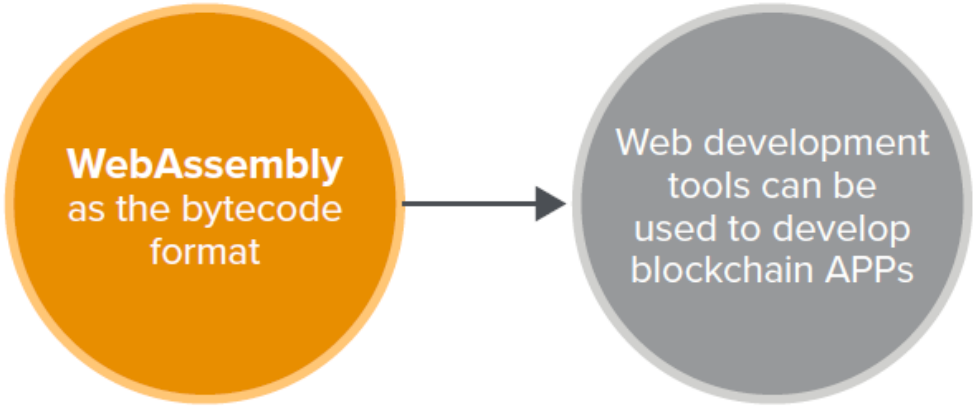


General Execution Environments

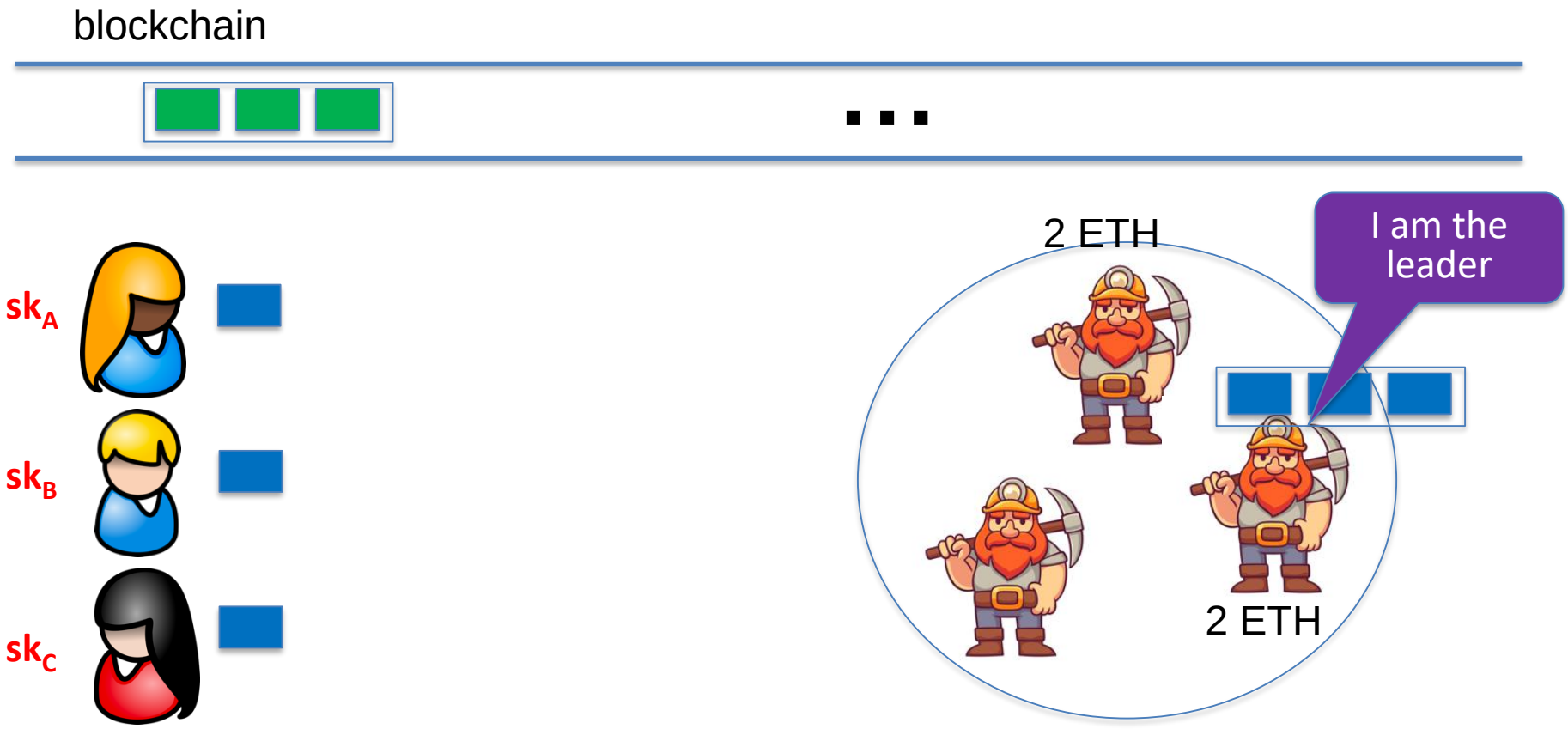
Recent projects

DFINITY

NEAR



How are blocks added to chain?



Decentralized applications (DAPPS)

Run on blockchain computer

applications (DAPPs, smart contracts)

blockchain computer

consensus layer

Common DAPP architecture