Decentralized Finance

Introduction to Blockchain technology

-- RECAP --

Instructors: **Dan Boneh**, Arthur Gervais, Andrew Miller, Christine Parlour, Dawn Song

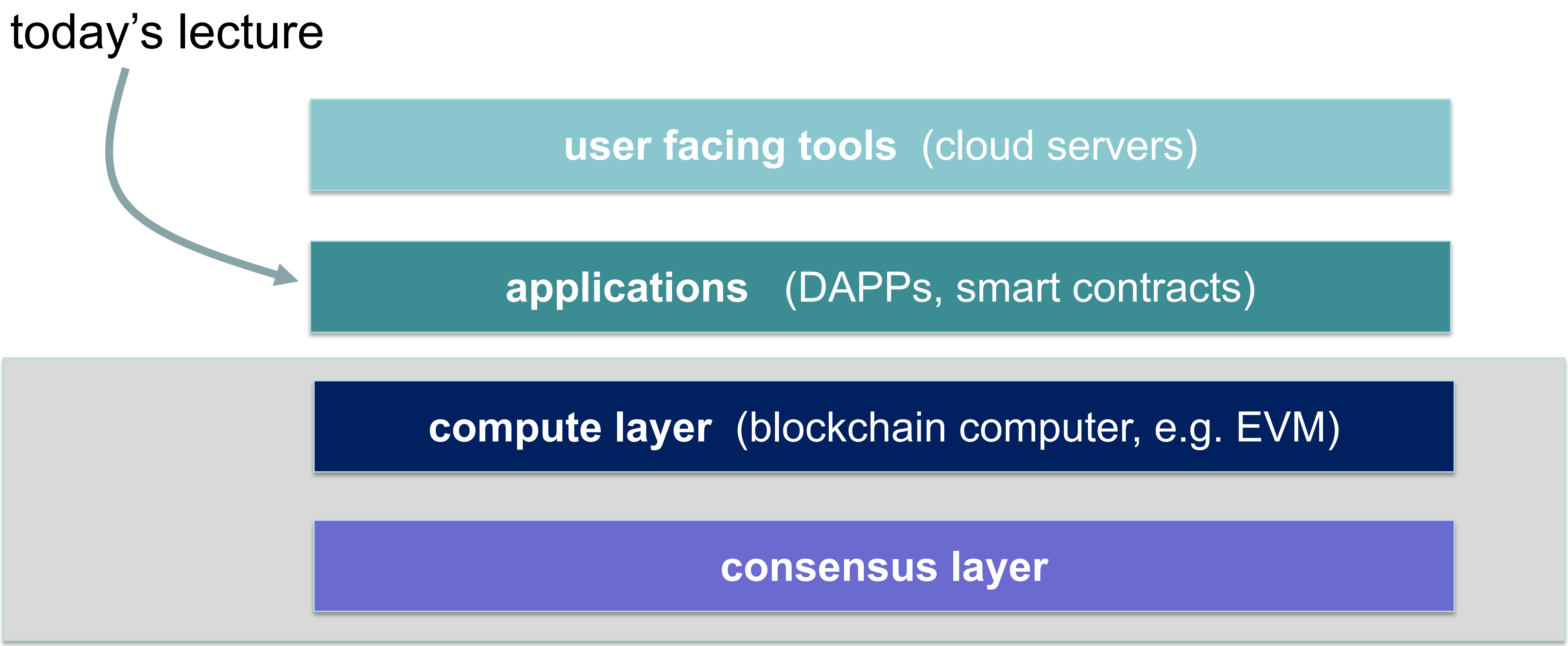
Stanford University

Imperial College London

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Berkeley UNIVERSITY OF CALIFORNIA

What is a blockchain?



today's lecture

user facing tools (cloud servers)

applications (DAPPs, smart contracts)

compute layer (blockchain computer, e.g. EVM)

consensus layer

Blockchain technology: recap

Three cryptographic primitives:

1. Collision resistant hashing: commit to data on a blockchain

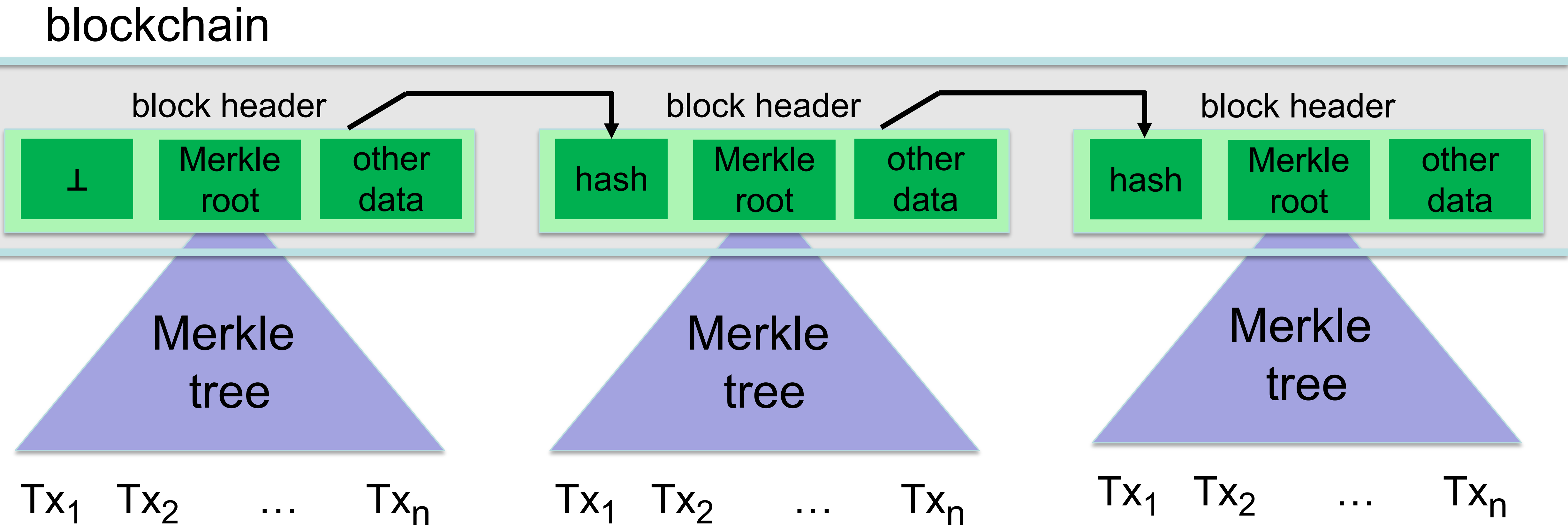
   $\Longrightarrow$ Merkle trees: commit to a list; later open one cell

2. Digital signatures: authorizing actions

3. SNARK proofs: prove that a certain statement is true

   (i) short proof, (ii) fast verification

Abstract block chain



A short Merkle proof proves that a Tx is “on the block chain”

Blockchain technology: recap

Cryptographic primitives: hashing, signatures, SNARKs

Scaling the blockchain: Payment channels and Rollups (L2 scaling)

security

availability

	SNARK validity proofs	**Fraud proofs**
Tx summary on L1 chain	**zkRollup** (e.g., zkSync)	optimistic Rollup (e.g., Arbitrum)
Tx summary off chain	zkPorter	”Plasma”

Blockchain technology: recap

Cryptographic primitives: hashing, signatures, SNARKs

Scaling the blockchain: Payment channels and Rollups

Interoperability:

bridges enable user to move assets from
one chain to another and back

… and now for today’s lecture