MIDDLEWARE SYSTEMS
RESEARCH GROUP
MSRG.ORG

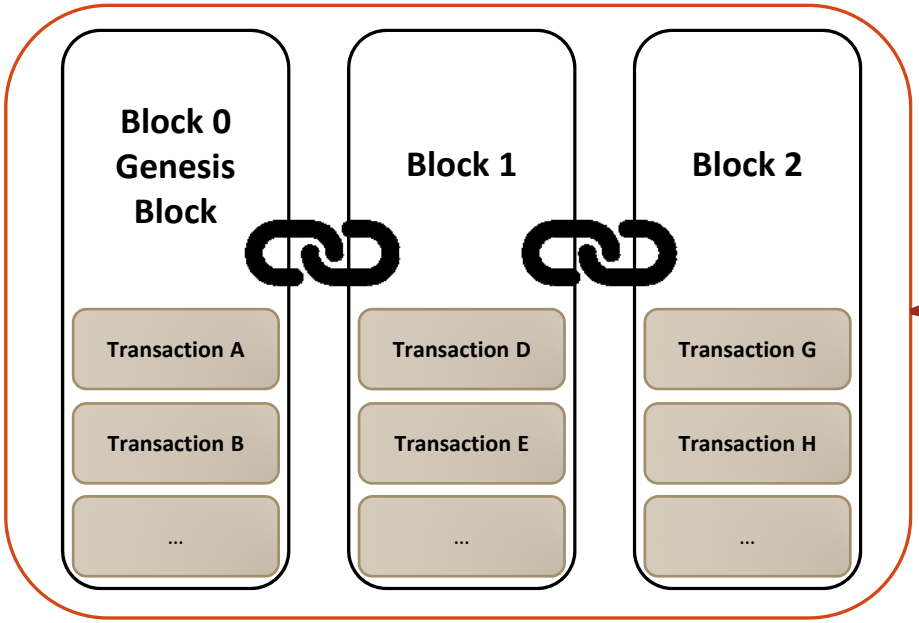
Deconstructing Blockchains: Concepts, Systems and Applications

INTRODUCTION

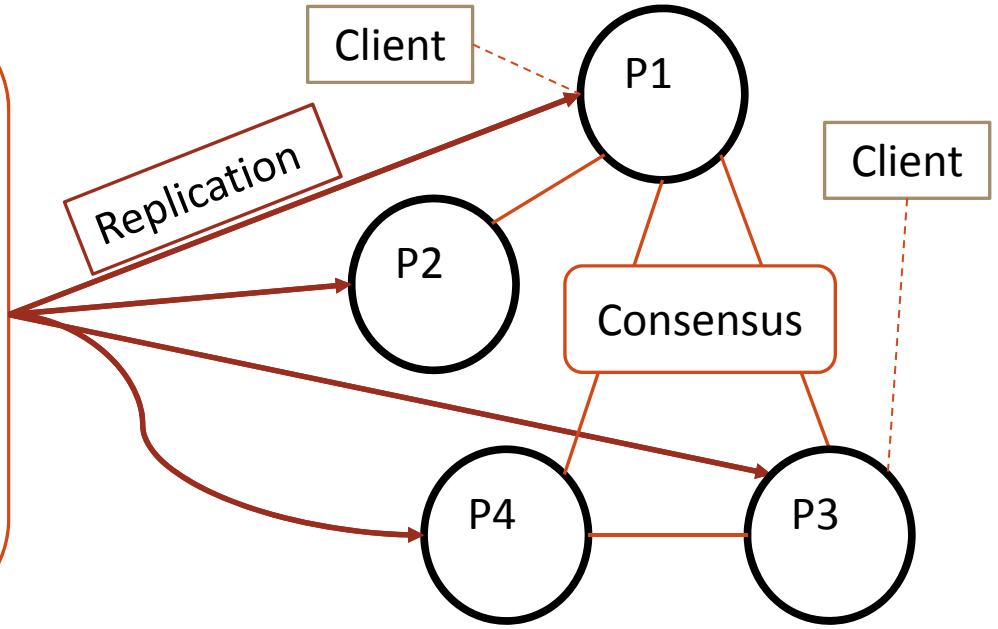
Understanding Blockchains

Blockchain 101: Distributed Ledger Technology (DLT)

Blockchain Data Structure



Peer-to-Peer Network



Cryptography is used to…

*…**encrypt data, prevent modification, insert new blocks, execute transactions, and query…***

the distributed ledger

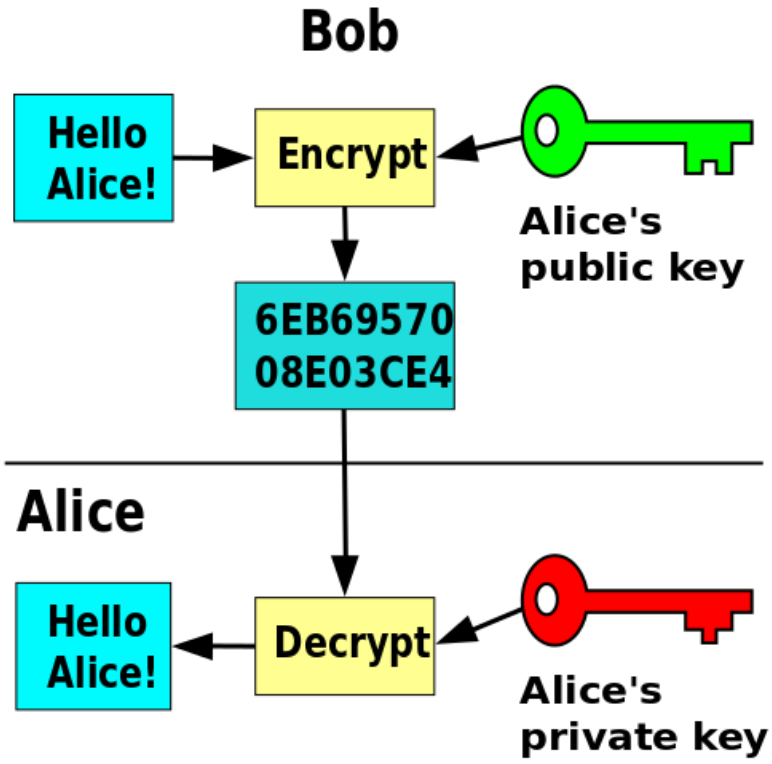
Comparison with Databases

	Single Machine DBMSs	Distributed Databases		
		OLTP	OLAP	
Logically centralized (Single entity)	MySQL, Oracle, …		ted a uses	Relational
			uce	Non-relational
Decentralized (Public/Private)		Distributed Ledgers (DLT)		Blockchain

The key distinction is the use of *cryptography* to enable operation in a decentralized trustless environment.

Public Key Cryptography
(Asymmetrical Cryptography)

- Recipient's **public key** is used to **encrypt** the plaintext to ciphertext
- Recipient's **private key** to **decrypt** the ciphertext to original plaintext
- **No one can use the public key to decrypt the ciphertext to plaintext**



Outline

What?

- Concepts: Mining, proof-of-work, smart contracts
- Case studies: Bitcoin, Ethereum, Hyperledger

Why?

- Blockchain applications
- Why study blockchains?

How?

- The six layers of blockchain systems
- Research directions

What is a Blockchain?

*A blockchain-based **distributed ledger** is:*

- ✓ *An **append-only** log* storing transactions
- ✓ *Fully **replicated*** across a large number of peers (called miners)
- ✓ Comprised of ***immutable*** blocks of data
- ✓ ***Deterministically verifiable*** (using the *blockchain* data structure)
- ✓ Able to execute transactions ***programmatically*** (e.g., Bitcoin transactions and smart contracts)
- ✓ Fully ***decentralized***, does not rely on a third party for trust

Immutability using Hashing

Blockchain data structure maintained at every peer