A BRIEF INTRODUCTION TO BLOCKCHAIN

NANCY LIAO '05

JOHN R. RABEN/SULLIVAN & CROMWELL EXECUTIVE DIRECTOR

YLS ASSOCIATE RESEARCH SCHOLAR IN LAW

Yale Law School Center for
the Study of Corporate Law

“BLOCKCHAIN” HAS MANY MEANINGS

“To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general.”

The Trust Machine, THE ECONOMIST, Oct. 31, 2015

“BLOCKCHAIN” HAS MANY MEANINGS

Phone

- The idea of a phone network
- A specific phone network (e.g., AT&T)
- A specific use of the phone network (e.g., fax)

Blockchain

- The idea of blockchain
- The specific blockchain that underlies Bitcoin or another coin offering
- Bitcoin or another cryptocurrency

WHAT IS BLOCKCHAIN?

A technology that:

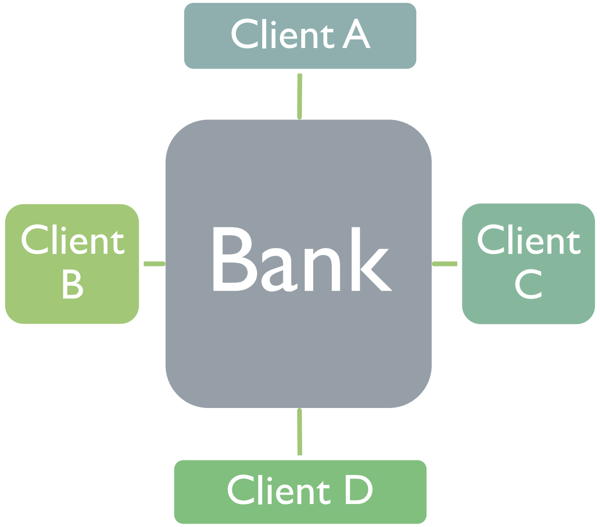
permits transactions to be gathered into blocks and recorded;

cryptographically chains blocks in chronological order; and

allows the resulting ledger to be accessed by different servers.

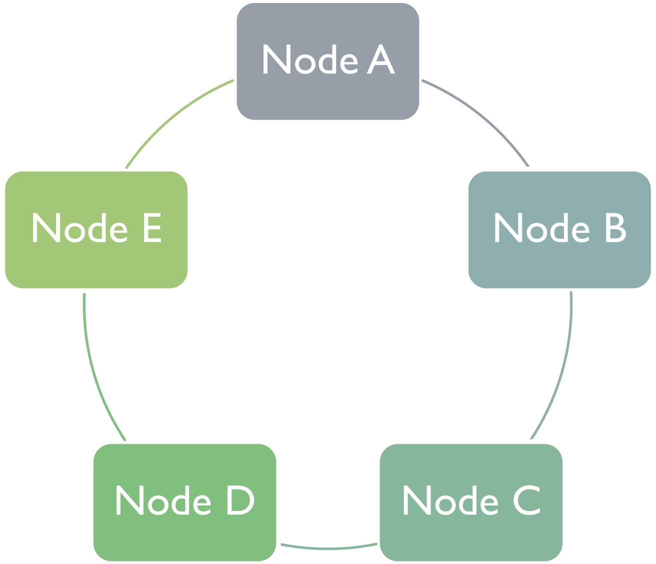
WHAT IS A DISTRIBUTED LEDGER?

Centralized Ledger



- There are multiple ledgers, but Bank holds the "golden record"
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if discrepancies arise

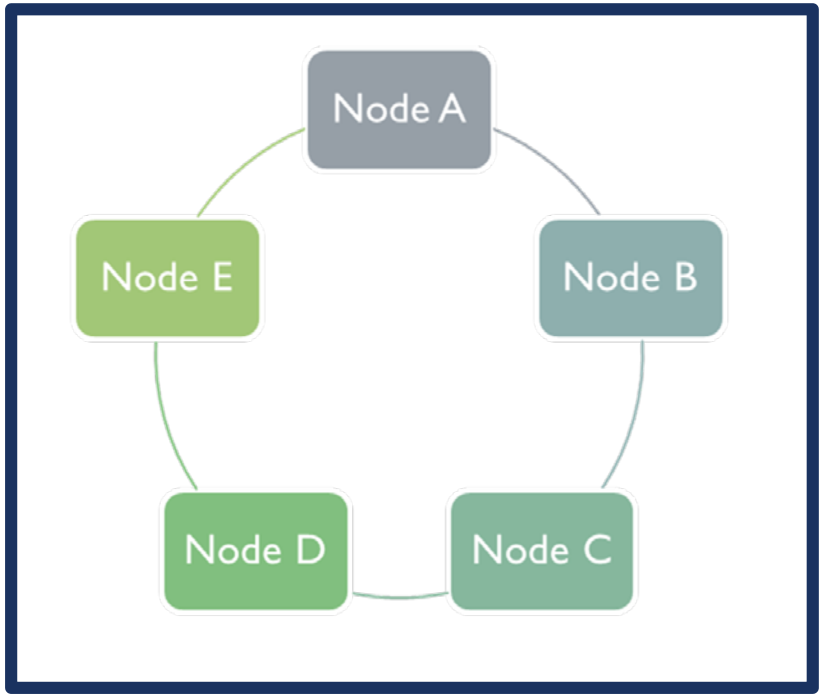
Distributed Ledger



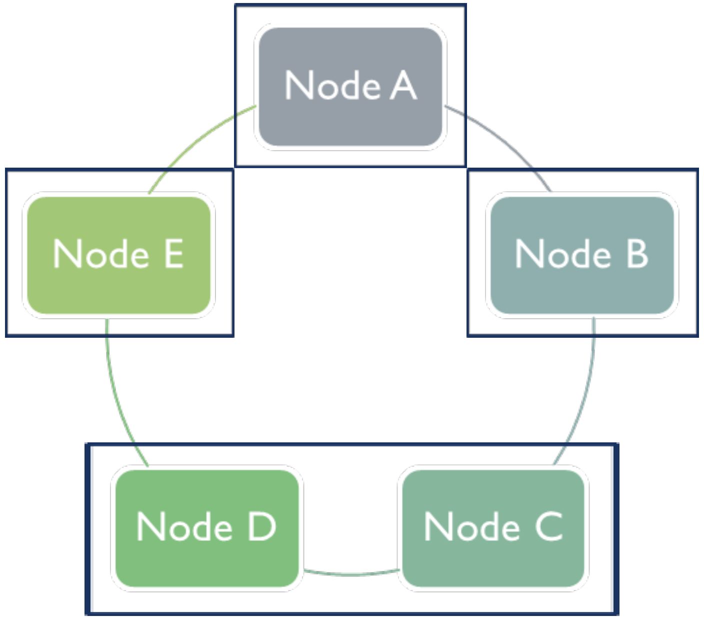
- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving consensus."

WHAT IS A DISTRIBUTED LEDGER?

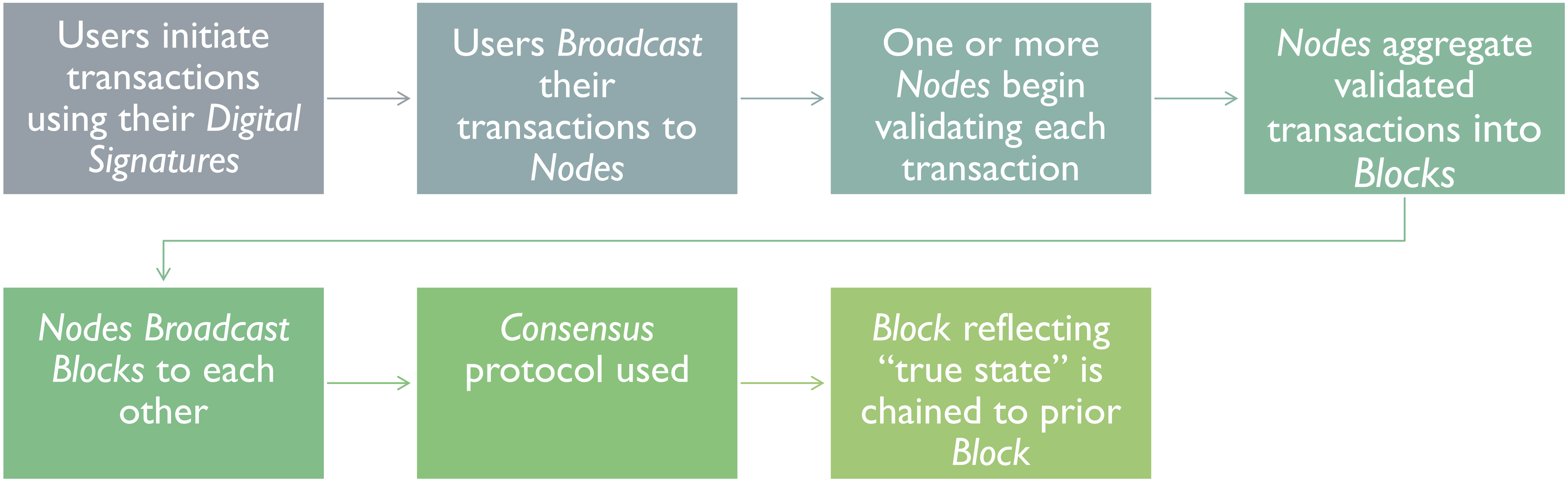
Single Entity



Multiple Entities



HOW MIGHT A DISTRIBUTED LEDGER WORK?



Users initiate transactions using their *Digital Signatures*

Users *Broadcast* their transactions to *Nodes*

One or more *Nodes* begin validating each transaction

Nodes aggregate validated transactions into *Blocks*

Nodes Broadcast Blocks to each other

Consensus protocol used

Block reflecting "true state" is chained to prior *Block*

WHERE MIGHT BLOCKCHAIN USE CRYPTOGRAPHY?

Initiation and Broadcasting of Transaction

- *Digital Signatures*
- *Private/Public Keys*

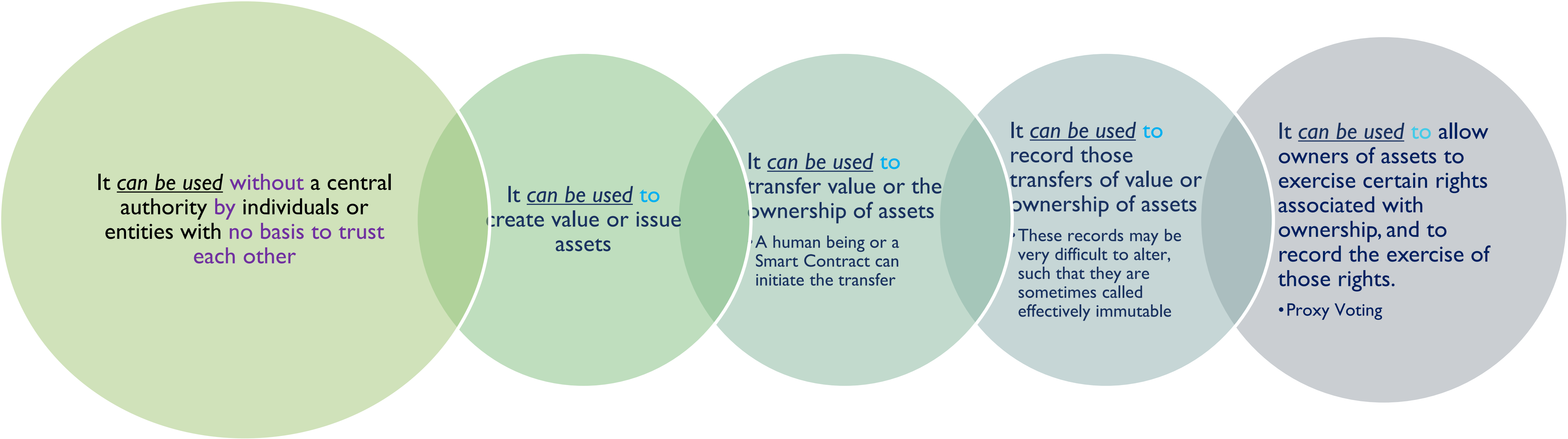
Validation of Transaction

- *Proof of Work and certain alternatives*

Chaining Blocks

- *Hash Function*

THE POWER OF DISTRIBUTED LEDGERS



It *can be used* without a central authority by individuals or entities with no basis to trust each other

It *can be used* to create value or issue assets

It *can be used* to transfer value or the ownership of assets

- A human being or a Smart Contract can initiate the transfer

It *can be used* to record those transfers of value or ownership of assets

- These records may be very difficult to alter, such that they are sometimes called effectively immutable

It *can be used* to allow owners of assets to exercise certain rights associated with ownership, and to record the exercise of those rights.

- Proxy Voting

The degree of trust between users determines the technological configuration of a distributed ledger.

HOW MIGHT DISTRIBUTED LEDGER PROPOSALS DIFFER?

Participation	*Open*	*Closed*
Permission	*Permissionless*	*Permissioned*
Ledger Design	*One ledger*	*One ledger or Segregated ledgers*
Validation	*Methodology depends on degree of trust between nodes. Where there is no basis for trust, may be achieved through proof of work, which requires the algorithmic solving of a cryptographic hash.*	
Consensus Mechanism	*Mechanism depends on degree of trust between nodes. Where there is no centralized authority, consensus may be determined algorithmically.*	

QUESTIONS?

Nancy Liao

nancy.liao@yale.edu