MAYER·BROWN

Digital Ledgers and Cybersecurity

David Beam
Partner

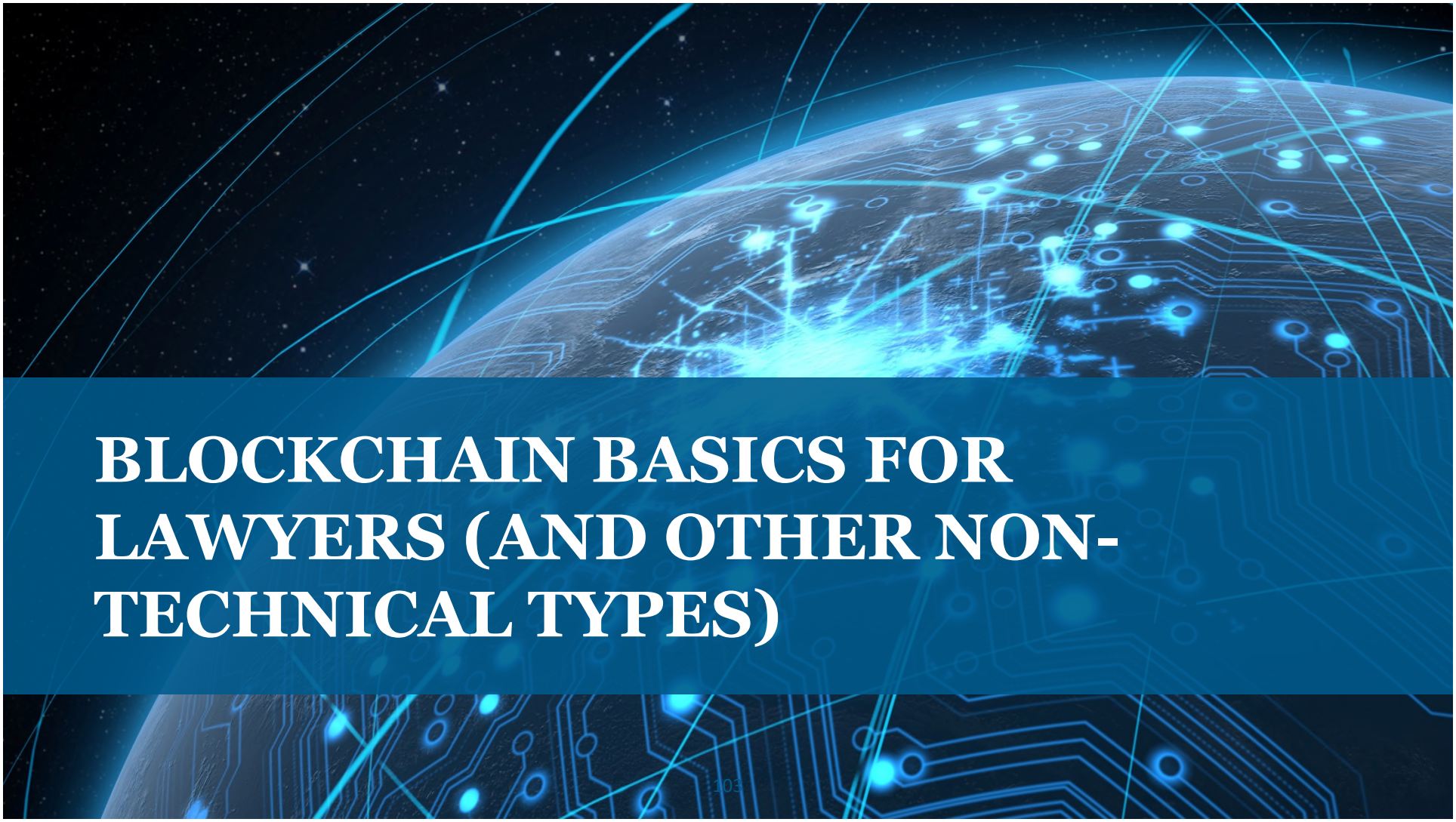
1 202 263 3375
dbeam@mayerbrown.com

Speakers

David Beam

Partner – Washington DC

MAYER·BROWN



BLOCKCHAIN BASICS FOR LAWYERS (AND OTHER NON-TECHNICAL TYPES)

Blockchain Versus Distributed Ledger

- Distributed Ledger: "A distributed ledger is a database that is consensually shared and synchronized across [a] network spread across multiple sites, institutions or geographies." (http://www.investopedia.com/terms/d/distributed-ledgers.asp)
  - Each "site, institution, or geography" that is part of the network is a "node."
- Many, but not all, distributed ledgers are structured with blockchain technologies.
- Most applications of blockchain technologies involve the creation of a distributed ledger, but there might be other applications.
  - Generally correct to say that all blockchains are distributed ledgers, but not all distributed ledgers are blockchains.

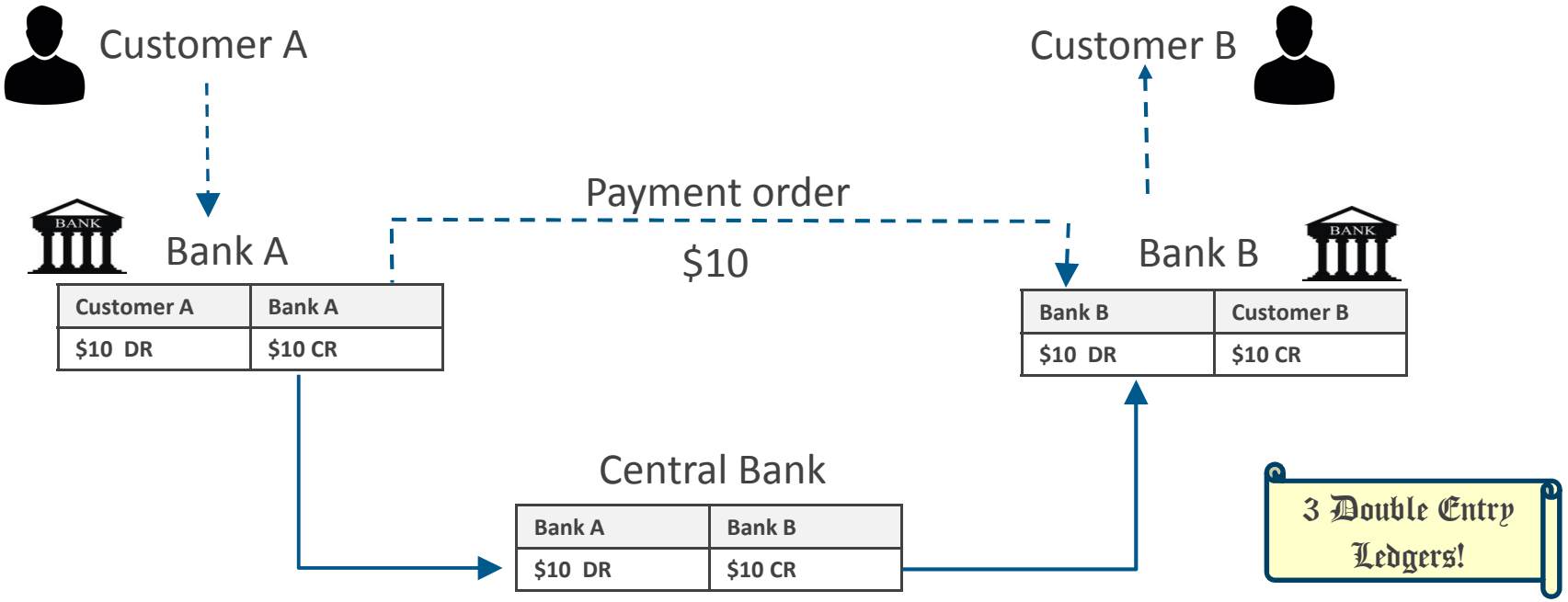
"Blockchain" Defined

- Technically Correct Definition: "A software protocol which validates and records transactions on a distributed ledger."
- Common, but imprecise, uses:
  - A ledger that uses such technology.
    - "The consortium used a blockchain to track transactions."
    - People will know what you mean, but avoid in formal writing.
  - Sometimes used generically to refer to blockchains (or distributed ledgers) in general.
    - "We can put this information on the blockchain."
    - Analogous to the term "cloud" in computing.

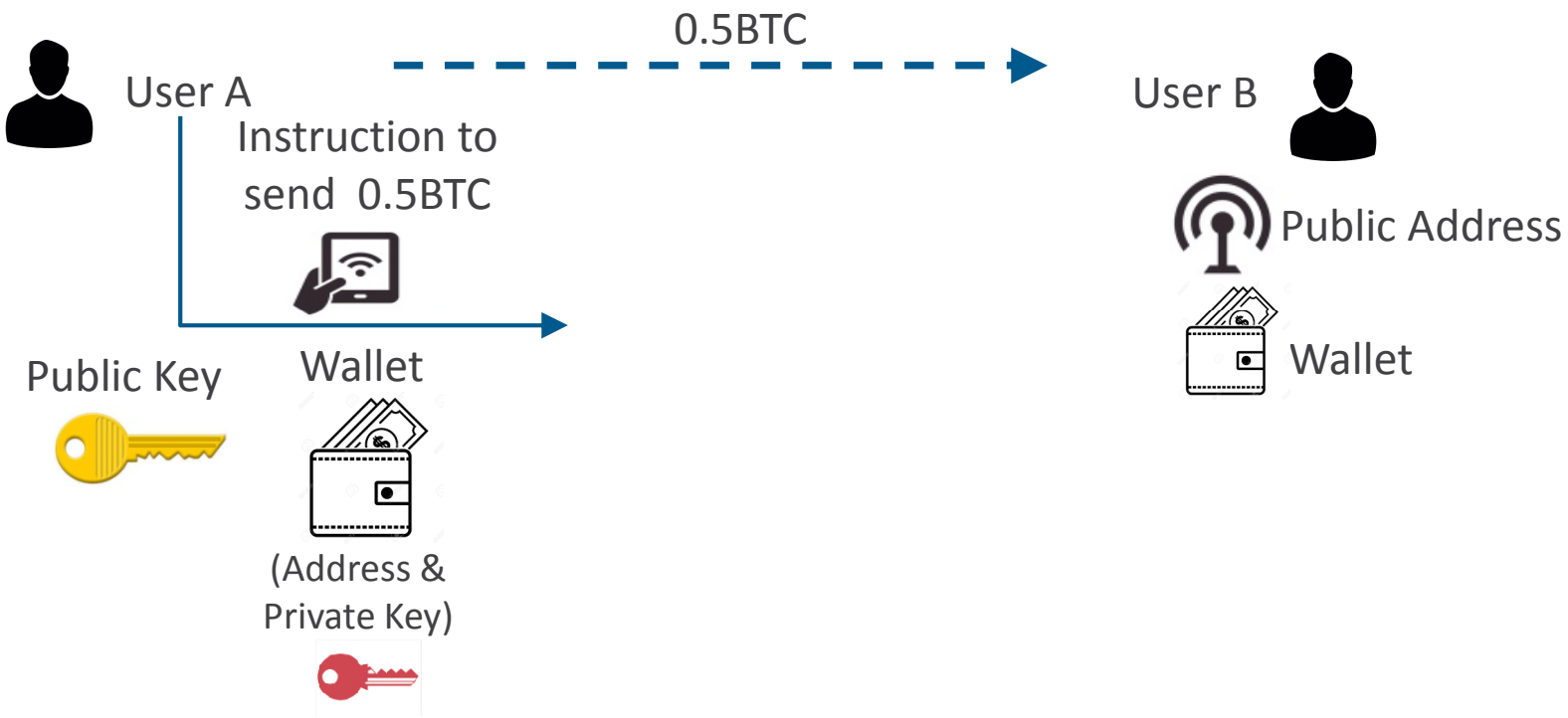
Blockchain Versus Bitcoin

- Bitcoin is a unit of value—a currency not backed by any government or government-sponsored entity.
- The world's inventory of bitcoins is recorded on—in fact, exists on—a distributed ledger that runs on blockchain technology. This ledger also tracks ownership of bitcoins.
- The creator of Bitcoin used blockchain and distributed ledger technology to solve the "double-spending problem," which is what had theretofore prevented the deployment of an electronic currency not administered by a central authority.

Traditional Centralized Ledger
(e.g., Cleared Banking Transaction)



Distributed Ledger
(e.g., Bitcoin Transfer)



MAYER·BROWN

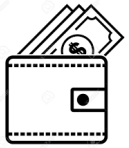
Distributed Ledger
(e.g., Bitcoin Transfer)

User A

Instruction to send 0.5BTC

Public Key

Wallet



(Address & Private Key)

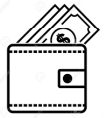
Pending Transactions

Sender	Recipient	Amount
…	…	…
A	B	0.5BTC
…	…	…

Validated by computers/ nodes

User B

Public Address



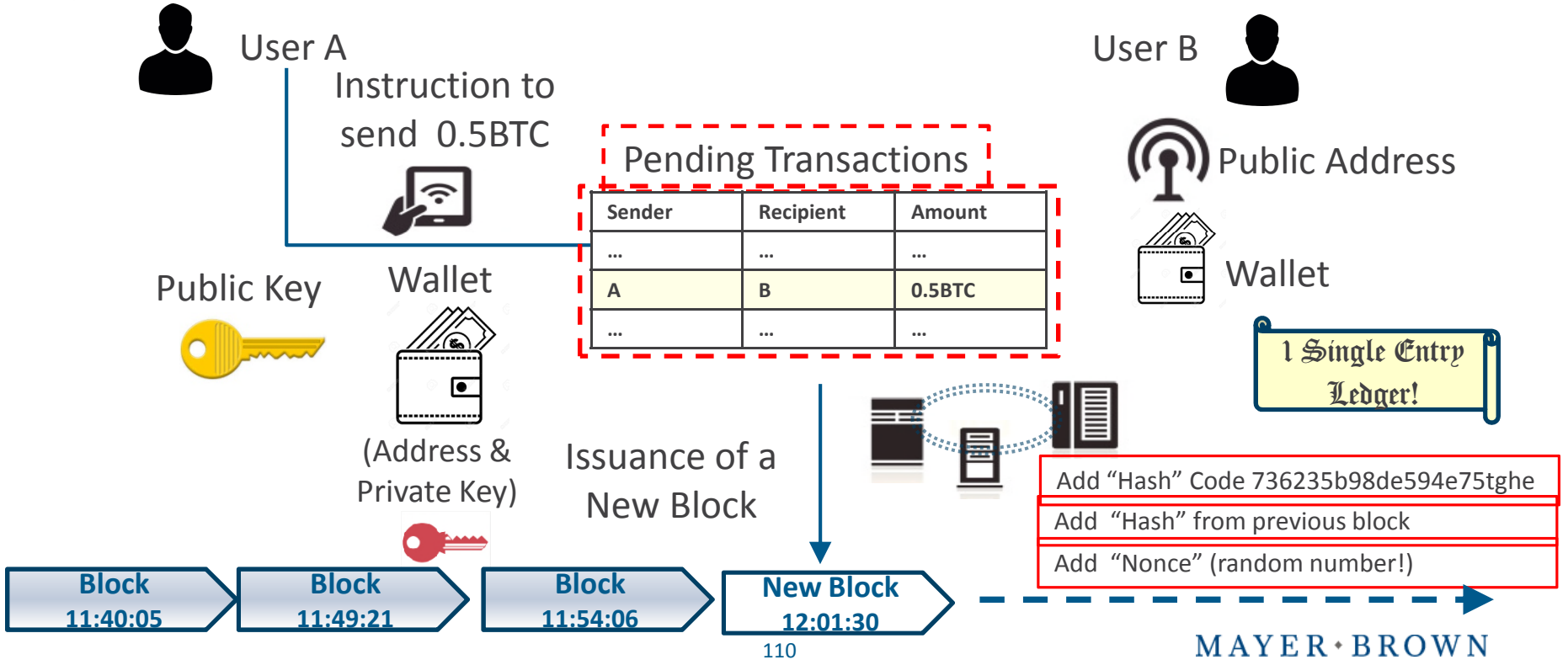
Wallet

Add “Hash” Code 736235b98de594e75tghe

Add “Hash” from previous block

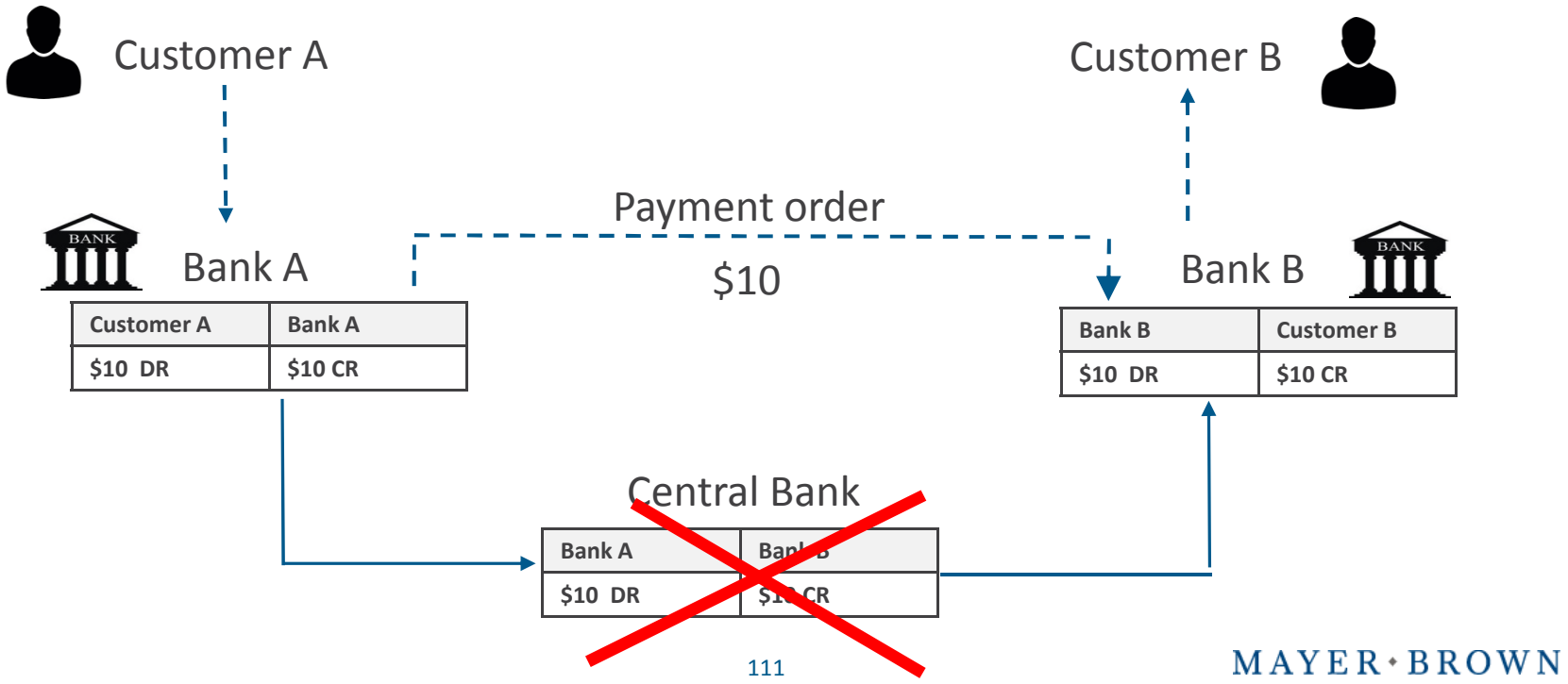
Add “Nonce” (random number!)

Distributed Ledger
(e.g., Bitcoin Transfer)



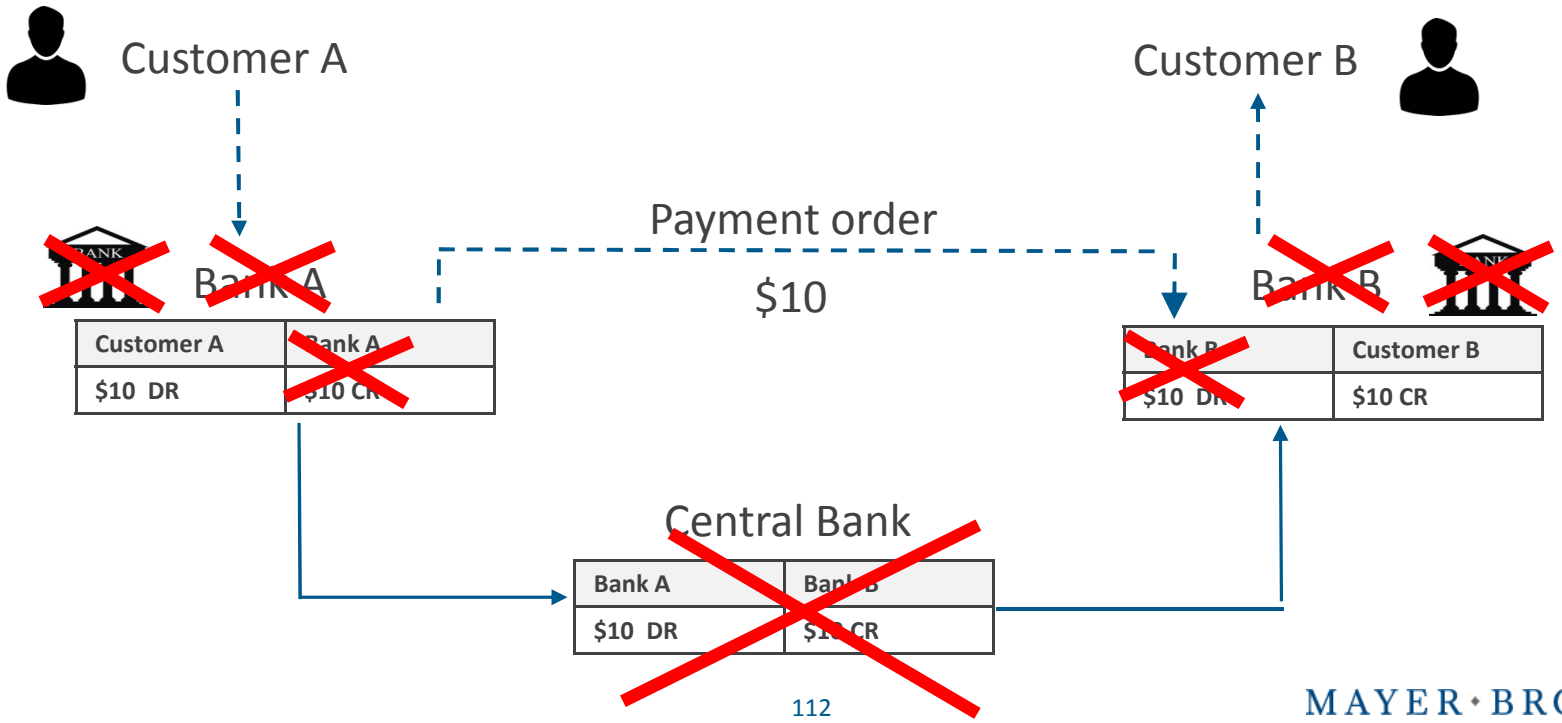
MAYER·BROWN

Comparison with Traditional Centralized Ledgers



MAYER·BROWN

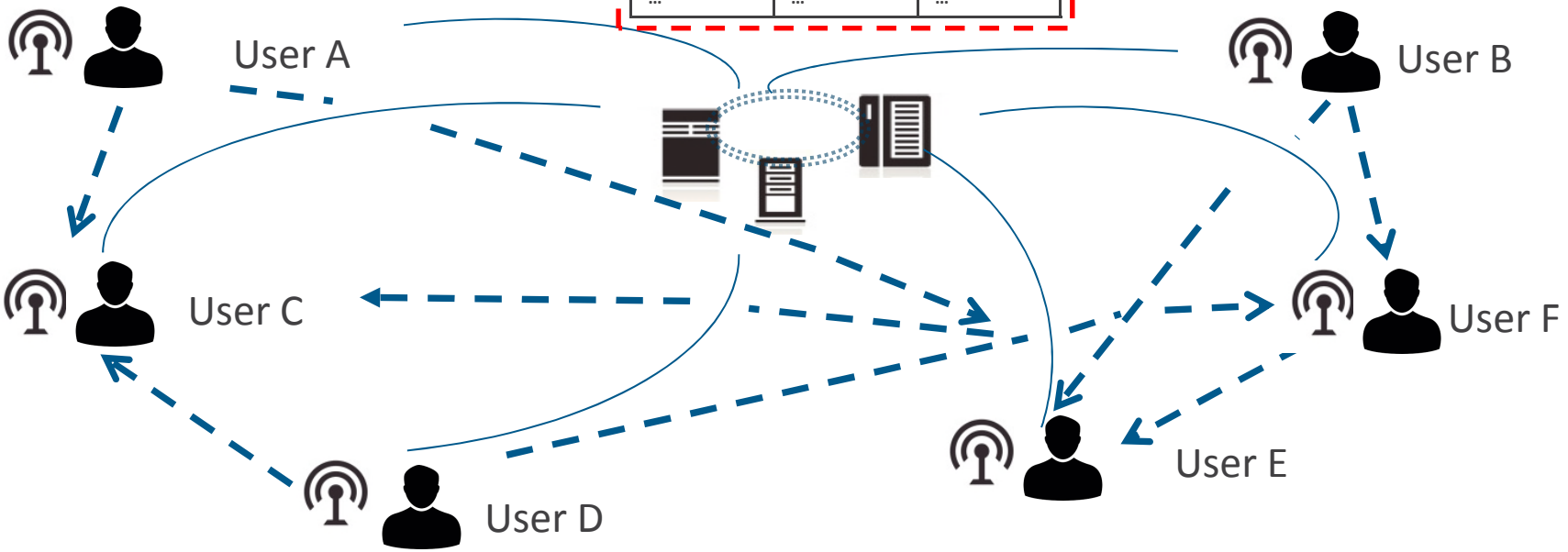
Comparison with Traditional Centralized Ledgers



MAYER·BROWN

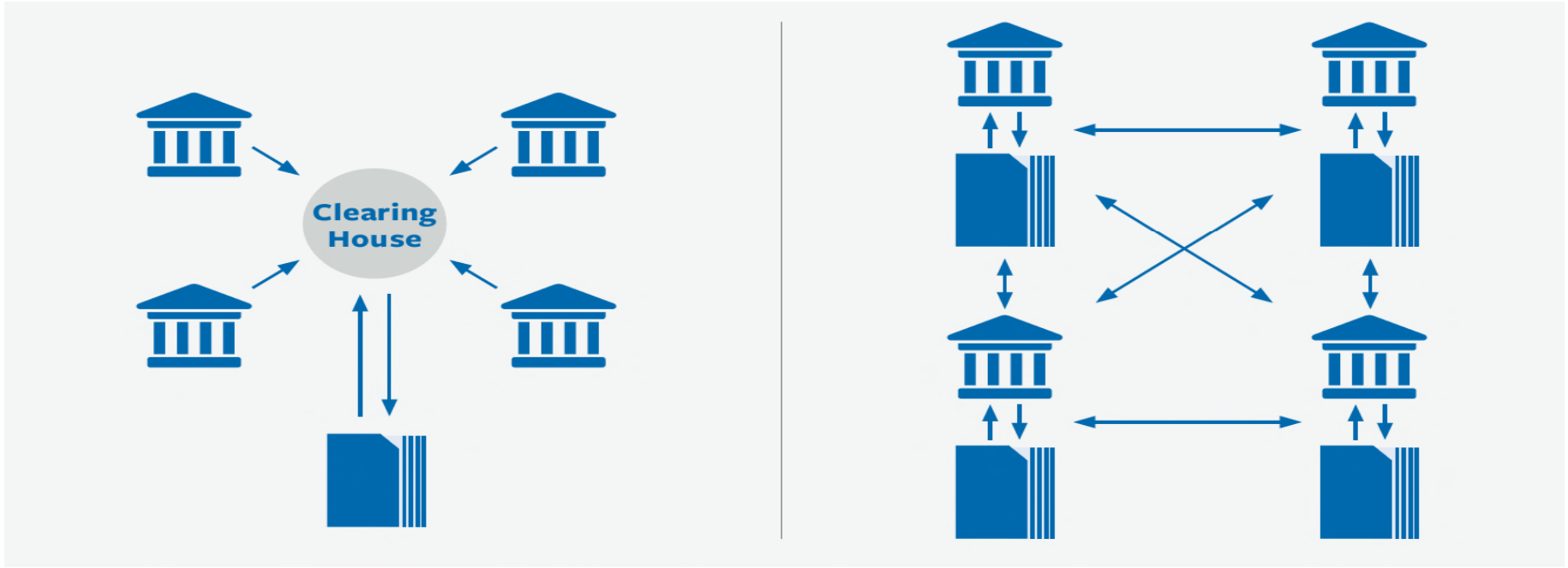
Distributed Ledger

Sender	Recipient	Amount
…	…	…
A	B	0.5BTC
…	…	…



MAYER·BROWN

Overview: What is a distributed ledger?



Left: A centralized database acting as a single point of control and a single point of failure.
Right: A distributed ledger recording ownership through a shared registry.

Overview: How does blockchain and other distributed ledger technology work?

STEP 01 A wants to send an asset to B

STEP 02 Each transaction will be represented as a 'block'

STEP 03 The block is transmitted to each party in the network

STEP 04 Those in the network confirm the transaction

STEP 05 The block is then added to the chain

STEP 06 The asset transfers from A to B

Use Cases for Distributed Ledger Technologies

- Digital currencies:
  - Peer to peer payments (Circle)
  - Digital currency backed by fiat currency (for inter-bank domestic payments – R3, e-Dinar (Tunisia), eCFA (Senegal))
  - Cross-border payments to offset currency fluctuations (Ripple / XRP - Santander, CIBC, Unicredit)
  - Digital currencies for use in settlement between banks (Utility Settlement Coin - UBS, DB, Santander, BNYM, Clearmatics)
- KYC, AML and digital identity management (KYC-Chain, R3, Netki)
- Smart contracts:
  - Letters of credit (R3 Corda)
  - Over the counter share trading (Swisscom, Zurich Cantonal Bank)
  - Self-paying instruments (UBS “smart bonds”)
  - Private smart contract platforms (JPM Quorum)
  - Insurance (Vrumi, SafeShare)
- Asset / collateral management (Deloitte, ConsenSys), post-trade clearing and settlement (Setl, DTCC & Axoni), payment (ASCAP, PRS), supply chain (IBM, Gem) and reference data management (R3)
- Corporate Actions

Technical Challenges with DLT Projects

- Defining the objectives: Establishing the problems to be solved
- Scalability of DLT and data storage requirements
- Maturity of technology vs sophistication of requirements (e.g., smart contracts)
- Interconnecting different DLT solutions
- Validating transactions and addressing privacy requirements (encryption, selective sharing)
- Enabling smart contracts to deal with changes in laws
- Obtaining critical mass to adopt the solutions

CYBERSECURITY CONSIDERATIONS FOR DIGITAL LEDGERS

Cybersecurity and Distributed Ledgers Overview

- Cybersecurty advances two objectives:
  - Ensuring that data is protected from unauthorized corruption, alternation, or destruction;
  - Preventing unauthorized access to confidential or sensitive data.
- Many institutions are subject to regulations that impose minimum cybersecurity requirements or dictate what they must do in response to certain cybersecurity events. E.g.:
  - Various privacy laws (HIPPA, GLBA) require institutions to manage access to covered information and adopt adequate technical safeguards to prevent unauthorized access;
  - Most US states, and many countries around the world, have laws that require companies to provide notice to affected individuals of certain cybersecurity events.
- DLT promoters argue that the design of distributed ledgers advances the first cybersecurity goal better than most non-distributed alternatives. But putting data covered by a privacy law on a distributed ledger can raise a number of issues.

Issues to Consider Under Privacy Laws

- Privacy laws and confidentiality provisions in contracts might restrict your ability to put certain information on a distributed ledger or impose requirements on you if you do.
- Is it permissible to put certain covered information on a distributed ledger at all, regardless of the protections?
  - In some instances, laws might need to be changed to accommodate this. Privacy laws limit with whom certain information may be shared, and some of the people with access to the ledger might not qualify.
- Barring that, you must know the following for all covered data that you put on a ledger:
  - Who will have access to unencrypted data?
  - Are there consortium/system rules that impose appropriate limitations on how those persons may use the data and what they must do to protect it from unauthorized access? How is compliance with these rules monitored and enforced?
  - If a data breach occurs through one of the nodes, who will have the notification obligation under applicable breach notification laws—the party that put the data on the ledger or the party that got hacked (or both)? How will all the parties with this obligation be notified in time for them to satisfy it?

DLT and Record Retention Requirements

- Are you going to rely on the ledger for record retention?
  - If you keep a complete set of your own records, then it doesn't matter if the ledger meets recordkeeping standards.
    - Consider how you will do this, though. Do you really have "offline" records for all data points that you are required to maintain?
  - Will system rules permit you to maintain offline copies of ledger information?
  - Does this make the nodes your service provider?
- Do the ledger protocols ensure that all the data points for which I am required to maintain records will be preserved on the ledger?
- How can I ensure that the ledger will retain historical data for the time period I am required to maintain it?
  - Can access rules change, such that I will lose access to historical data without warning and an opportunity to preserve a copy for my own records?

DLT and Record Retention Requirements (con't.)

- Will I be a node—i.e., maintain an official copy of the ledger that it automatically updated—or am I merely an observer?
- Do the applicable recordkeeping requirements mandate that my records be kept in a defined location or do I need regulator approval for the recordkeeping location?
  - "The cloud" isn't a location, and neither is "the blockchain."
- Recordkeeping requirements may impose specific security requirements that don't mesh with DLT's security principles.
  - Back up Records: Sometimes the solution is just a back up.

QUESTIONS?

David Beam
Partner

1 202 263 3375
dbeam@mayerbrown.com