Blockchain Technology

Its potential impact

Law/regulation is stated as of November 2017, is intended as general guidance only and should not be relied on in respect to any specific matter. Views expressed are those of the individual presenters and not those of Jones Day or their respective clients.


Can we agree?
The Internet has changed the world…
Globalization
Interconnectedness
How Our Clients Operate
How Services are Provided
How We Communicate
How We Learn

Can we also agree?

We will not discuss*:
Hashes, Keys,
Wallets, Cryptography, Bitcoin
or other Mumbo Jumbo

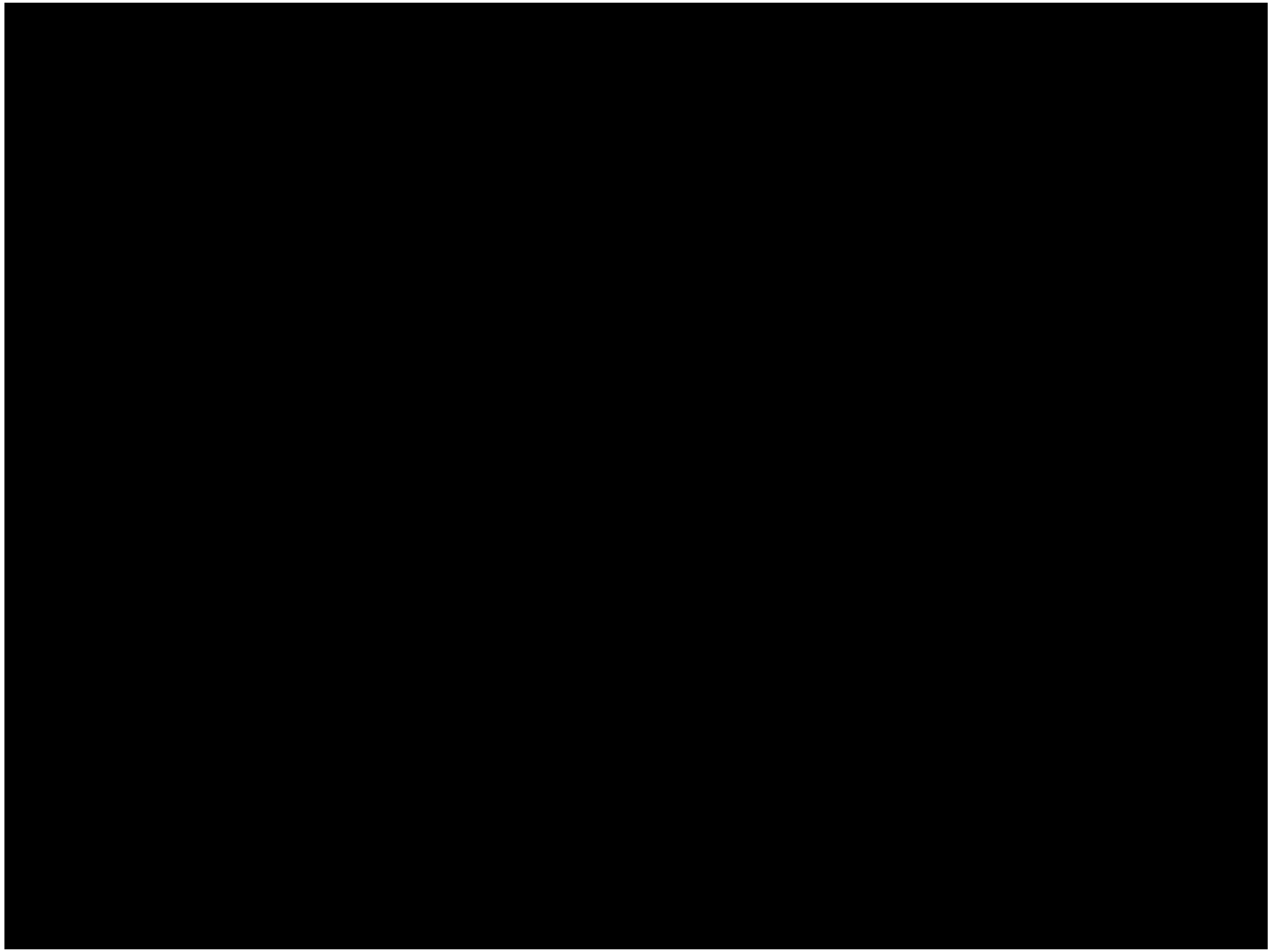
*** unless you ask us to…**

JONES DAY®

Why should you care?

- Nearly **nine out of 10** senior executives in Finance and IT believe that blockchains will be used on a daily basis in the finance industry by 2026
- In a recent survey of European financial services firms, **96%** of business leaders have invested in blockchain or plan to invest in the next 24 months

JONES DAY®



JONES DAY®

What we will cover

- What is Blockchain?
- What problems does Blockchain aim to solve?
- Blockchain applications
- Challenges to implementation
  - Appendix A – How does Blockchain work?
  - Appendix B – Sources and other materials

What is Blockchain?

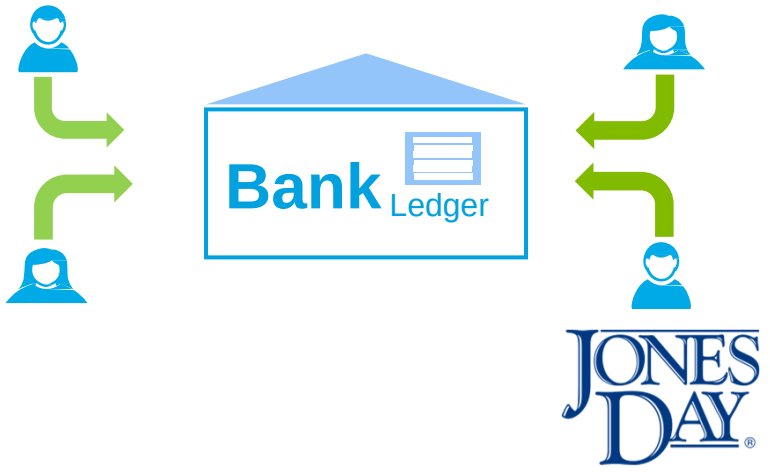
Blockchain is a technology for storing information, based on a distributed ledger concept.

It is also referred to as “DLT”.

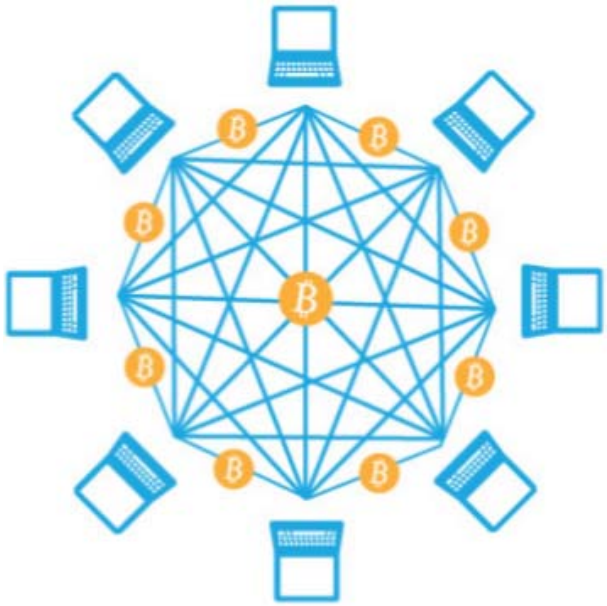
Today's centralized systems

- A **central intermediary** (e.g., a bank) transfers actual value between two parties and is normally the final authority
- All parties involved in a transaction have to rely on **their own ledger** (which is not the central, authoritative ledger)
- When a party loses its ledger (IT failure, physical disaster, malware attack) information is lost due to the **single point of failure**

Typical examples of centralized databases are relational databases we are all familiar with. When Financial Institution A buys an asset from Financial Institution B, both parties A and B will have separate records of their transaction in their separate databases.



Blockchain's decentralized systems



Think of a group of financial institutions sharing information on a network regarding a series of transactions.
Each institution in this group has its own copy of the ledger where it records every new transaction among group participants.
Each institution in this group independently verifies every new transaction before recording it into the ledger. New transactions are immediately replicated into all ledgers at the same time.

Permissioned network (Intranet)

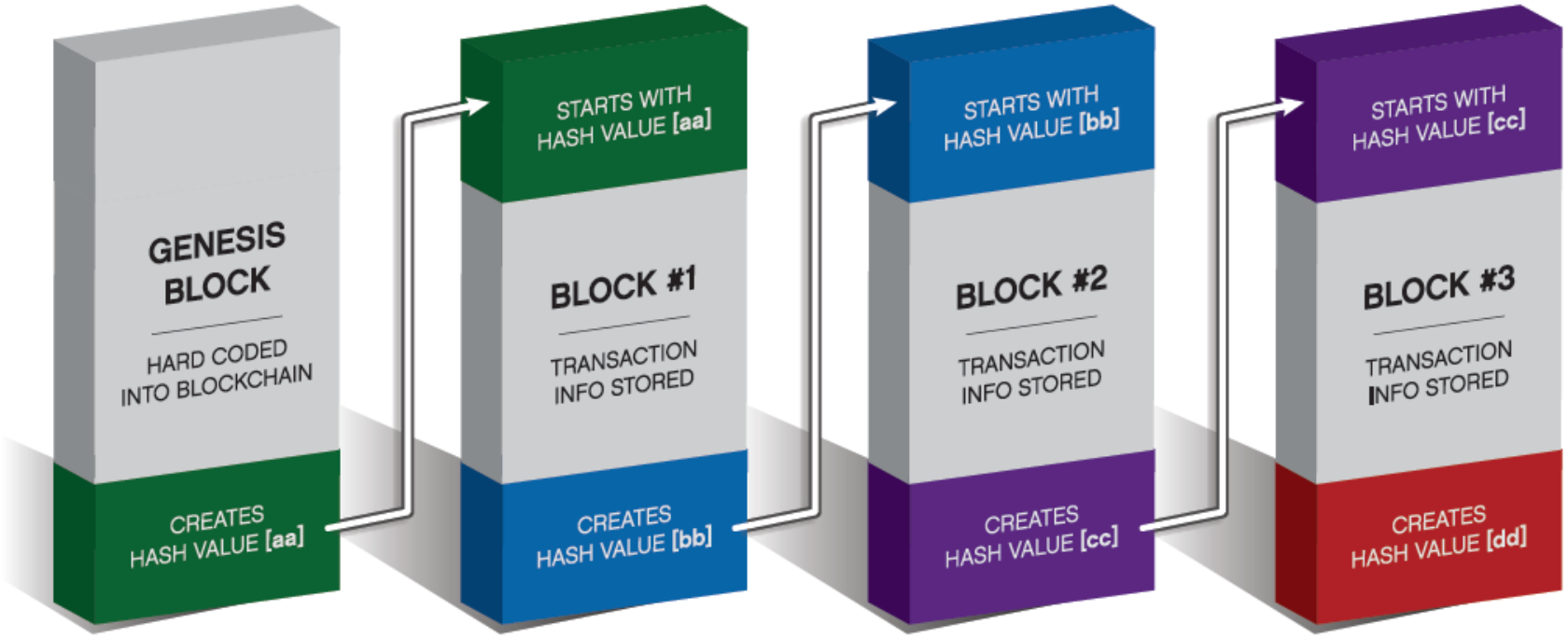
Open network (Internet)

JONES DAY®

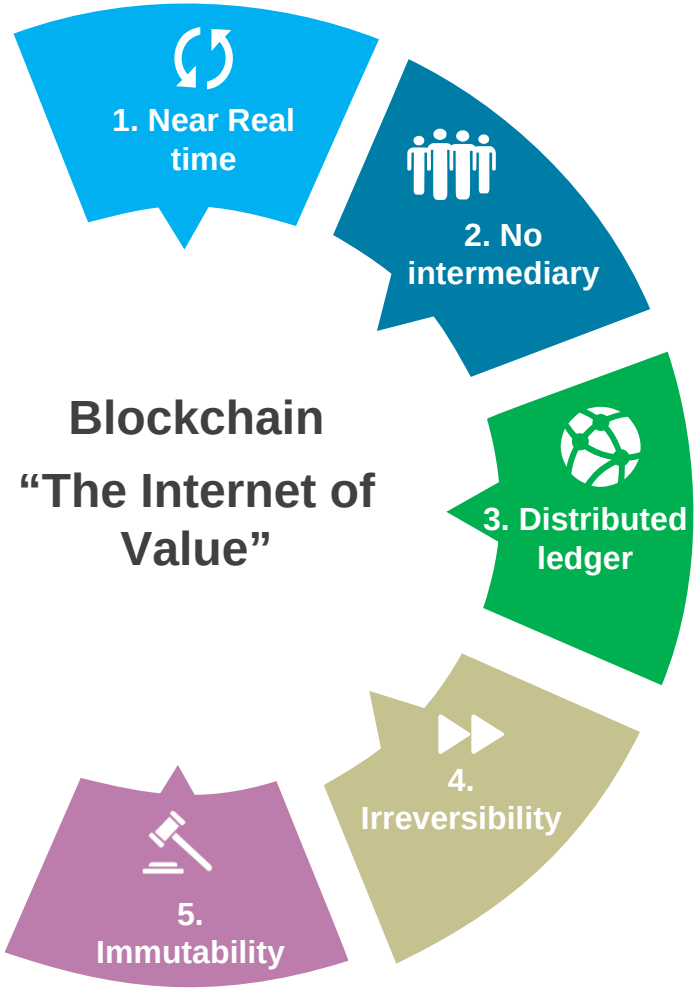
What is Blockchain?

- Blockchain is a technology for storing and sharing information, based on a **distributed ledger** concept. It comprises:
  - A shared list of **sequential records** called “Blocks”
  - Each Block contains a **validated record/data**
  - Blocks are **linked together**
  - Stored information **cannot be changed** without disrupting the links between blocks

What is Blockchain?



Advantages of Blockchain



1. Near real time – Efficiency

Blockchain enables the near real time settlement of recorded transactions.

2. No intermediary – Disintermediation

Blockchain technology is based on cryptographic proof instead of trust, allowing any two parties to transact directly with each other.

3. Distributed ledger – Audit trail

The peer-to-peer distributed network records a transparent history of transactions.

4. Irreversibility – Audit trail

The Blockchain contains certain and verifiable records of every single transaction ever made.

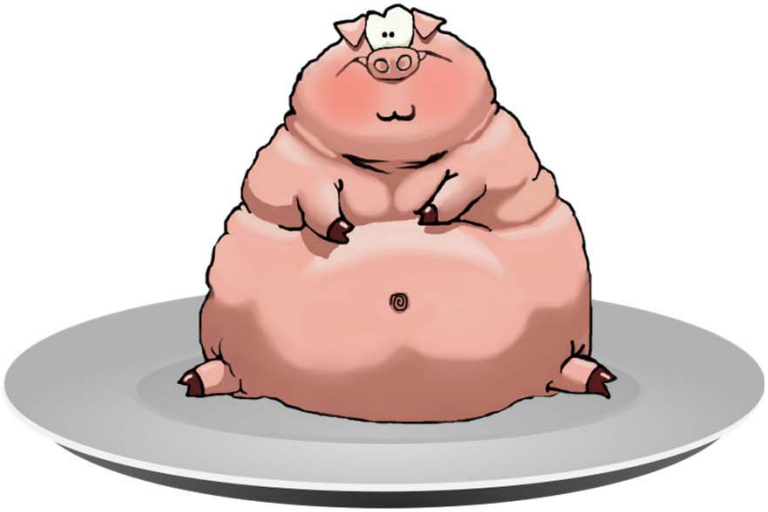
5. Immutability – Audit trail

The daisy-chained cryptographic framework prevents past blocks from being altered.

JONES DAY®

Blockchain in action

- Tracking
- Value transfers/transactions



Dealing with Real World Assets

Smart Contracts

- Smart Contracts **build off** of Blockchain, like macros to an Excel file
- Automated contracts
- Working with real-world assets, when a **pre-programmed condition** is triggered the smart contract executes the corresponding contractual clause (life insurance payout upon death)

```
? pragma.syntax("0.8")
# E sample
def makeCoveredCallOption(timer,                # access to a real-world time service
                          escrowedStock,        # reserves stock while offer is OPEN
                          escrowedMoney,        # intermediate money-transfer purse

                          # The 3 args above are from broker. The 4 below  from options-writer

                          stockSrc,             # provides the stock offered for sale
                          deadline :int,        # time until which the offer is OPEN
                          moneyDest,            # where the seller receives payment
                          strikePrice :int      # price demanded  per share of stock
) :any {
    def numShares :int := stockSrc.getBalance()  # how many shares are offered
    escrowedStock.deposit(numShares, stockSrc)   # escrow all the shares in stockSrc

    var state := "OPEN" # one of OPEN, CLOSED, or CANCELLED

    def cancel() :void {
        if (state == "OPEN") {
            stockSrc.deposit(numShares, escrowedStock) # return stock to seller
            state := "CANCELLED"
        }
    }
    timer.whenPast(deadline, cancel) # after deadline, call cancel()

    def coveredCallOption {
```

Dealing with Real World Assets

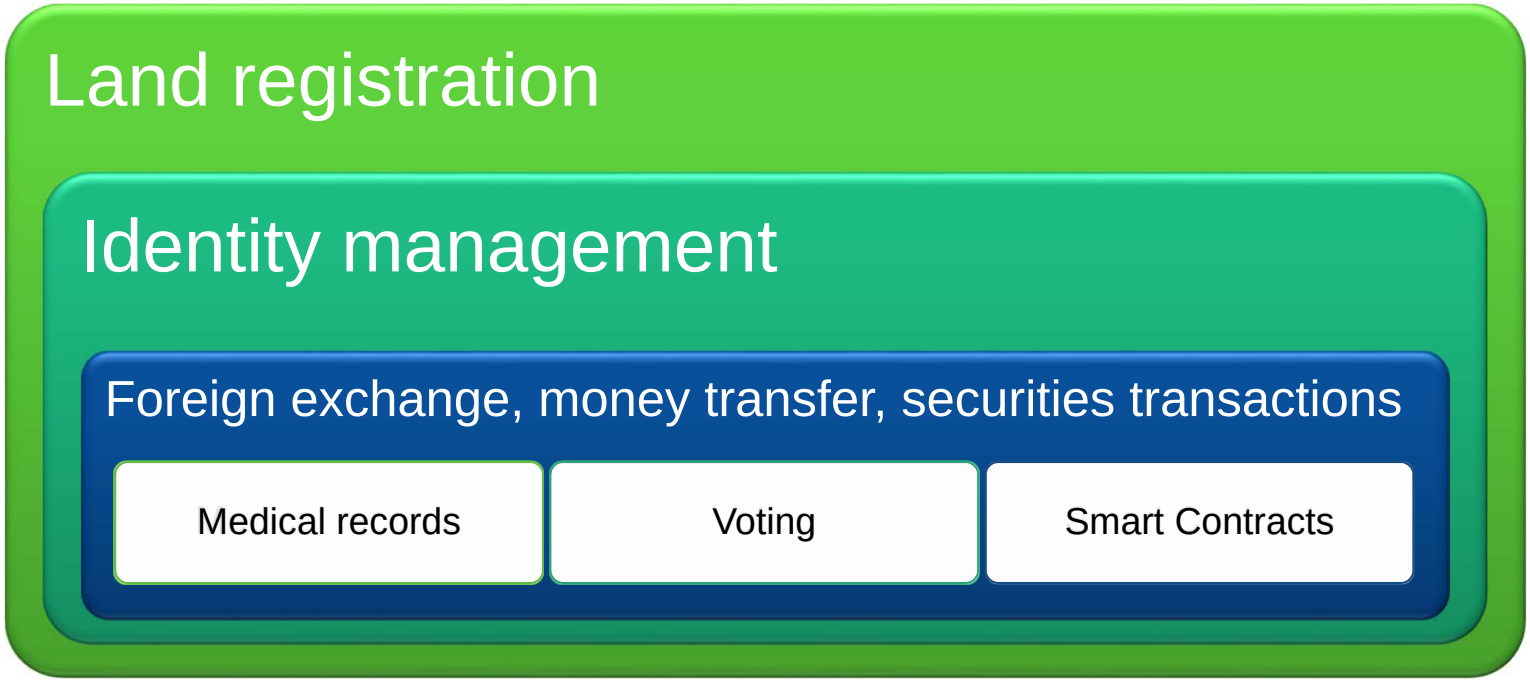
A smart contract between a bank and a car buyer provides legal ownership to the buyer as long as the person makes loan payments to the bank.

An external trigger in the shape of a late payment will automatically block use of the car by black-box engine communication.

In case the buyer fails to make up the payment default, the smart contract automatically returns the legal ownership of the car to the bank.

The processes are transparent, absolutely clear, and automatically executed.

Dealing with Real World Assets



Application to securities transactions

- Overstock preferred offering using Blockchain
- Eliminates T+3 and DTC, now T0
- Track and confirm shares, holders, and transactions

T ZERO

Symbol History | Balance by Symbol | Balance by Address | Holders by Symbol

*All dates and times Eastern

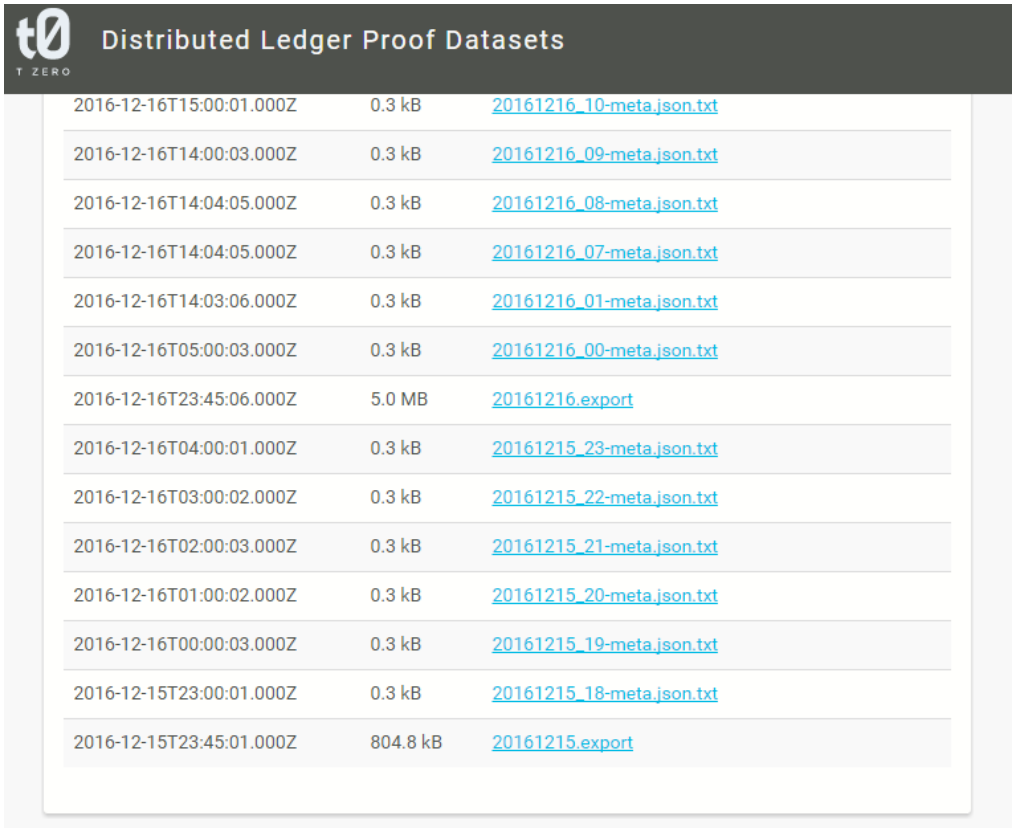
Track the history of symbol OSTKP
between start of day (12:00 AM Eastern) on 2017-02-10
and end of day (midnight Eastern) on 2017-02-10 GO

Timestamp	Type	Address	Change
Feb 10th, 09:54:41	**Committed Security**	0x8ce59e99928287ee3c6812c822d25919246d6512	-700 OSTKP
Feb 10th, 09:54:41	Sell 700 OSTKP @ 17.50	0x144ea72a4116db80cf421f218e65321df3e44839	+700 OSTKP
Feb 10th, 09:54:27	**Committed Currency**	0x8ce59e99928287ee3c6812c822d25919246d6512	-11,900.00 USD
Feb 10th, 09:54:27	Buy 700 OSTKP @ 17.00	0x144ea72a4116db80cf421f218e65321df3e44839	+11,900.00 USD

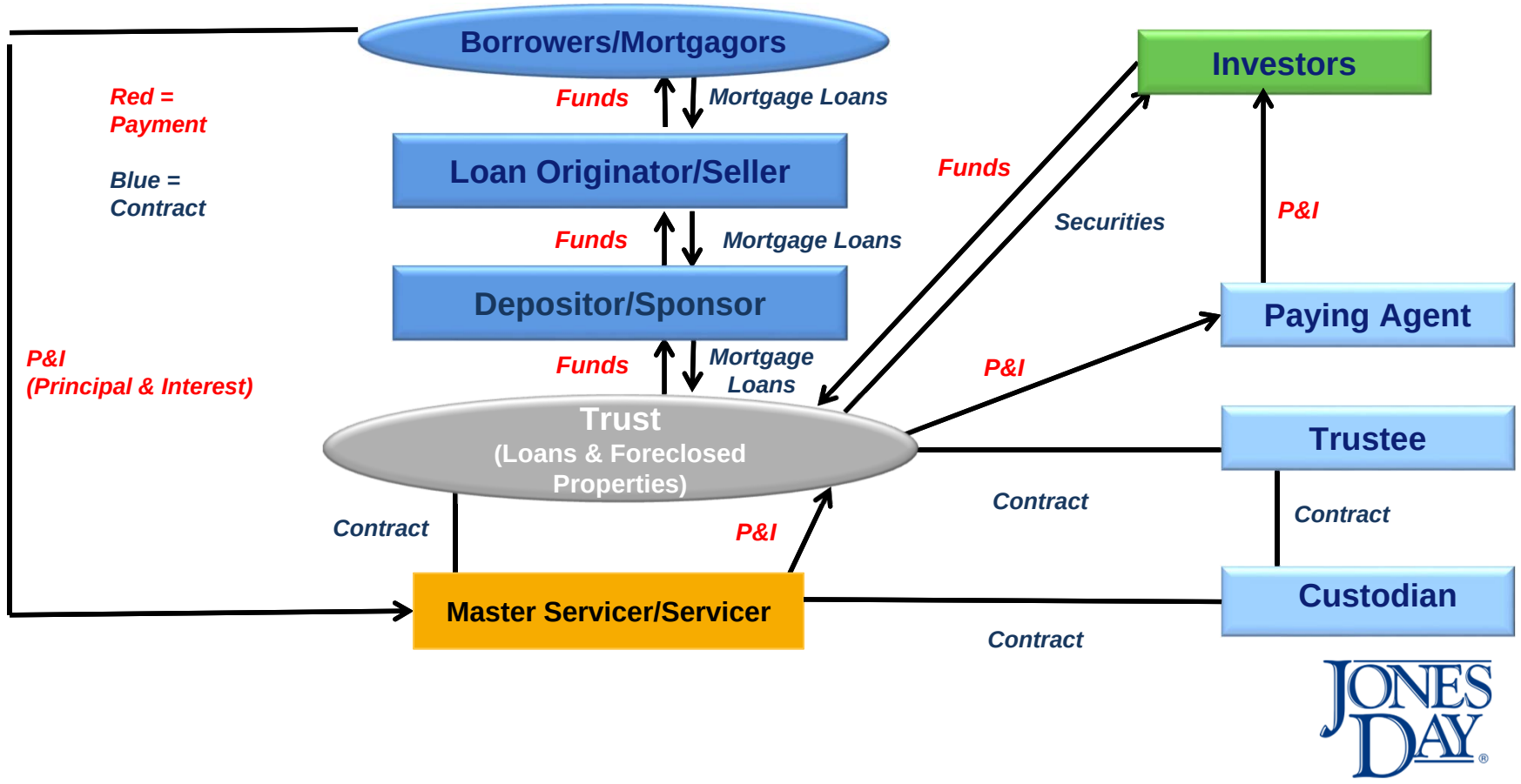
JONES DAY®

Application to securities transactions

- Proof datasets/distributed ledger created hourly



Application to securitizations

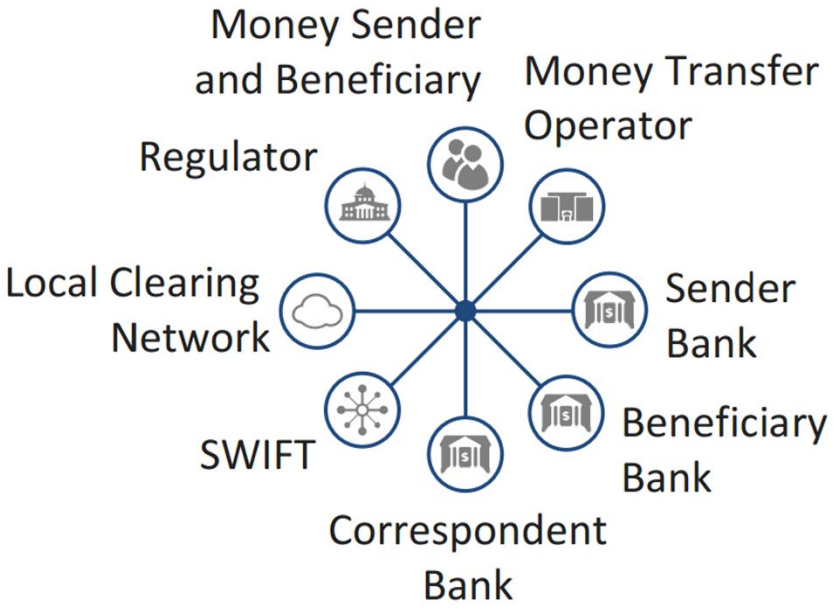


Application to securitizations

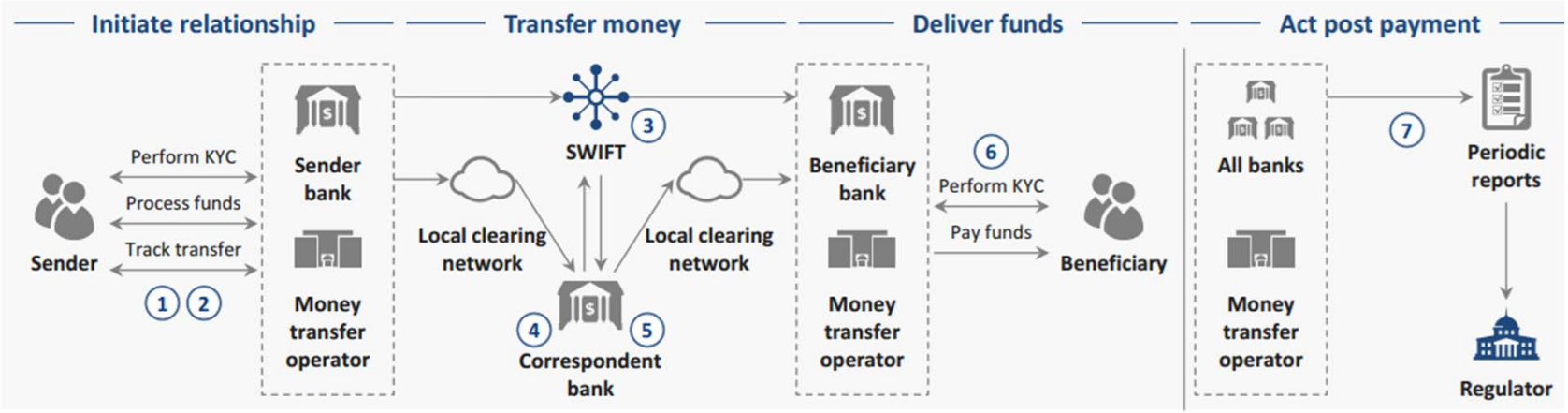
	Primary Issuance	Secondary Market Client Transactions	Post Trade Processing	Asset Servicing & Custody	Principal & Income
CHALLENGE	• Cost of issuance is typically high	• Requires booking of complex, multi-legged transactions	• Manual process with high FTE per capita ratio	• Manual processing corporate action events & client position mapping	• Payments process is fragmented and error prone
SOLUTION	• Issuance straight onto a Blockchain ledger • **Certificate register**	• Single platform with golden source record for all transactions • **Certificate transfer**	• Potential for automation of many post trade processes • **Certificate transfer**	• Automated client position data. Smart contracts triggered based on corporate action events • **Notices & other information**	• Smart contracts can automate **waterfall and investor payments** • Removes need for reconciliation
BENEFITS	• Reduced cost of issuance	• Front to back view of all transactions on a single platform	• Reduced FTE dependency • More scalable solution	• Reduction in operational risk. Automation of critical processes	• Automation of payment triggers and payment process

Application to payments

- Conducting international money transfers on Blockchain could provide real-time settlement and reduce costs, enabling new business models (e.g., micropayments), and institute newer models of regulatory oversight



Application to payments

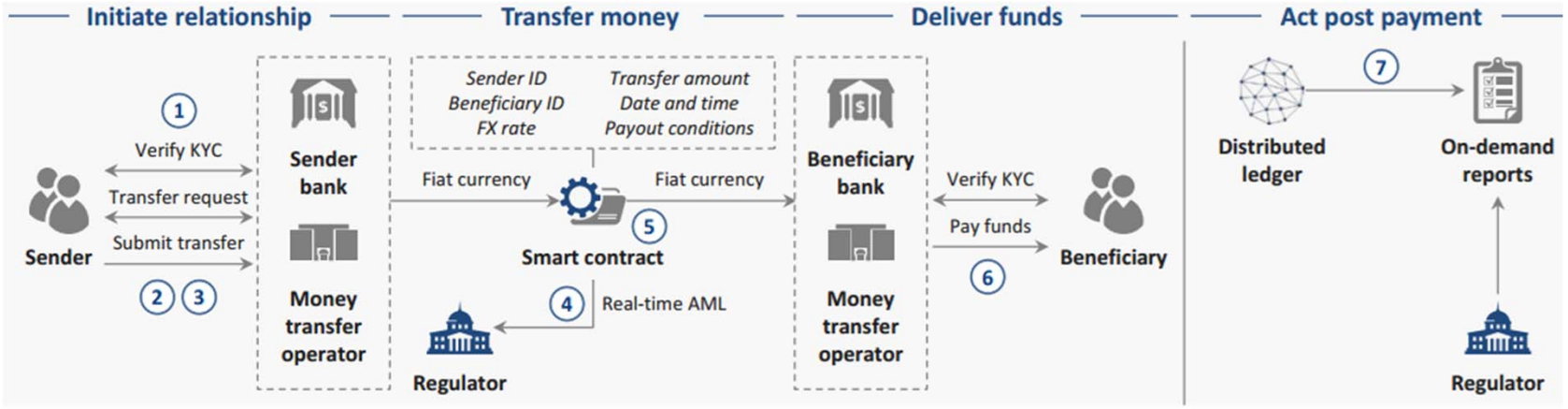


Current-state pain points

1. **Inefficient onboarding:** information about the sender and beneficiary is collected via manual and repetitive business processes
2. **Vulnerable KYC:** limited control exists over the veracity of information and supporting documentation, with various maturity levels across institutions
3. **Cost and delay:** payments are costly and time consuming depending on route
4. **Error prone:** information is validated per bank/transaction, resulting in high rejection rate
5. **Liquidity requirement:** banks must hold funds in nostro accounts, resulting in opportunity and hedging costs
6. **Vulnerable KYC:** similar to #2, limited control exists over the veracity of information and supporting documentation, with various maturity levels across institutions
7. **Demanding regulatory compliance:** due to various data sources and channels or origination, regulatory reports can require costly technology capabilities in addition to complex business processes (often supported by multiple operation teams)

The future of financial infrastructure, WEF (August 2016)

Application to payments



Future-state process description

1. Trust between the sender and a bank or money transfer operator is established either via traditional KYC or a digital identity profile
2. A smart contract encapsulates the obligation to transfer funds between sender and beneficiary
3. The currency conversion is facilitated through liquidity providers on the ledger
4. The regulator can monitor transactions in real time and receive specific AML alerts through a smart contract
5. A smart contract enables the real-time transfer of funds with minimal fees and guaranteed delivery without the need for correspondent bank(s)
6. Funds are deposited automatically to the beneficiary account via a smart contract or made available for pickup after verifying KYC
7. The transaction history is available on the ledger and can be continuously reviewed by regulators

JONES DAY®

The future of financial infrastructure, WEF (August 2016)

What are some of the challenges to implementation?

- Blockchain will NOT happen overnight
- But it is coming…
  - "Nearly nine out of 10 senior executives in financial services and information technology believe that blockchains will be used on a daily basis in the finance industry by 2026"

What are some of the challenges to implementation?

Practical

- **Translation** to different business functions
- **Adoption** by major market players
- **Cost** of systems & implementation
- Integration into **risk management** framework
- **Talent** acquisition and development

Technological

- Cyber **security**
- Systems **acquisition & licensing**
- Replacement of **legacy systems**
- **Interoperability** with internal & external users
- **Data storage** requirements

Regulatory/Legal

- Cyber security **standards & compliance**
- Regulatory **recognition or rules**
- **Nature of the asset** (property v. personal rights; documentary intangibles; possession, delivery or ownership)
- **Courts** differing views on the nature of the asset and enforceability of agreements.

JONES DAY®

What are some of the challenges to implementation?

Jurisdictional	• Governing Law? • Place of performance? • Nature of asset transferred?
Liability	• Enforceability • Technology or design failure • Performance
Regulated Products	• In or out of regulation? • Reporting • The rise of ICOs and issues with securities laws
Cybersecurity & Data Privacy	• Ensuring compliance with state and federal regulations • Data and verification breaches?
Intellectual Property	• Patent acquisition • Patent litigation • Open source

Legislation/Licensure

- Arizona
- Delaware
- New Mexico
- New York
- Vermont
- Washington

SEC: Initial Coin Offerings/Token Sales & ETFs

- SEC investigative report
  - Offers/sales of digital assets subject to federal securities laws
    - "Initial Coin Offerings" and "Token Sales"
  - Issuer of blockchain based securities must register
  - Securities exchanges must register
  - SEC concerns about disclosures to consumers
- Ongoing consideration of Bitcoin/Ethereum ETFs

More regulation and legislation is coming…

Questions?

Thank you!

- These slides will be circulated along with appendices including details as to how Blockchain works and additional materials for your review
- Please feel free to contact our team with any questions
  - Steve Obie (NYC)
    - sobie@jonesday.com, (212) 326-3773

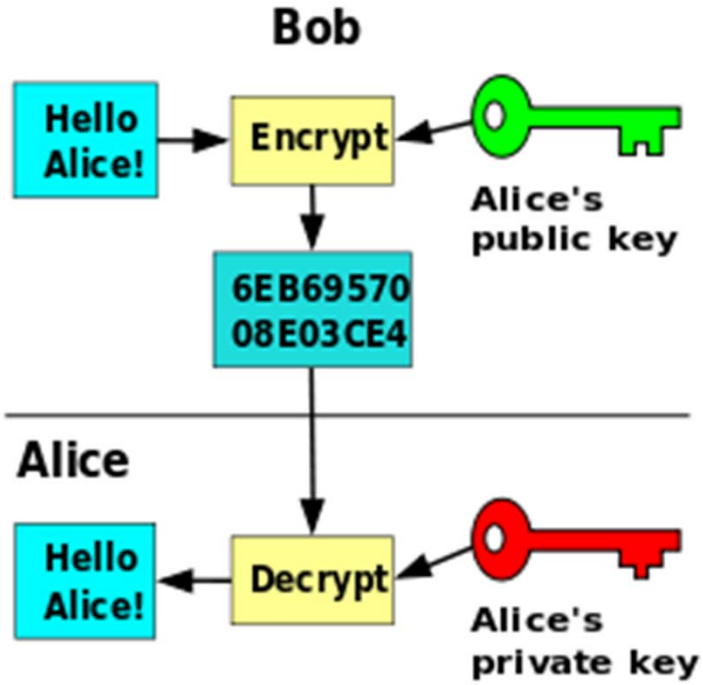
Appendix A
How does Blockchain work?

How does Blockchain work?

- A Blockchain transaction has several components
  - Encryption
  - Hash functions
  - Blocks
  - Blockchain
  - Distribution and use

How does Blockchain work? Encryption

- Encryption is a separate technology that can be used with Blockchain
- “Public key cryptography” is the usual system used
- A user has both a “private” and “public” key
- If Bob wants to send data to Alice, he uses Alice’s public key to encrypt the data and only Alice’s private key can decrypt it
- A similar system is used to digitally sign transaction to verify the source



How does Blockchain work? Hash functions

- Blockchains are built around “hash functions” and “hash values”
- A hash function always outputs the same hash value for a given input
- No two sets of data have the same hash value when using the same hash function – it is like a fingerprint

How does Blockchain work? Hash functions

- Using the SHA256 hash function, for example, when “Hello!” is the input, the output will always be the same 64-character hash value: “334d016f755cd6dc58c53a86e183882f8ec14f52fb05345887c8a5edd42c87b7”
- If “Hello Sam!” or “Hello Dolly!” is the input, the 64-character output would be an entirely different hash value

How does Blockchain work? Blocks

- For Blockchain to work, each Block must be validated or signed somehow
- One way is to say that the hash value for every Block in the chain must contain a certain sequence
- Users can agree in the first instance that for a Block to be validated or signed its hash value must start with four zeros
    - For our Block containing “Hello!” to be validated, the first four characters of its hash value must begin with “0000”

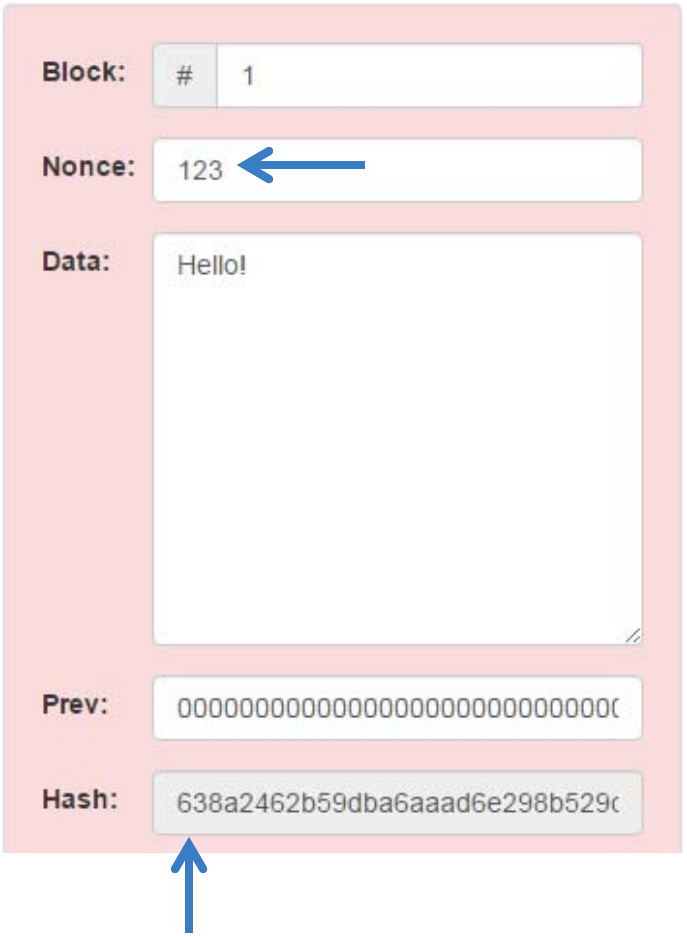
How does Blockchain work? Blocks

- But how do we do that?
  - If “Hello!” is the input to the SHA256 hash function it will always output the hash value “334d016f755cd6dc58c53a86e183882f8ec14f52fb05345887c8a5edd42c87b7” which is not validated
- Solution:
  - We need to add additional inputs into the hash function, along with the original data, for the output to begin with “0000”

How does Blockchain work? Blocks

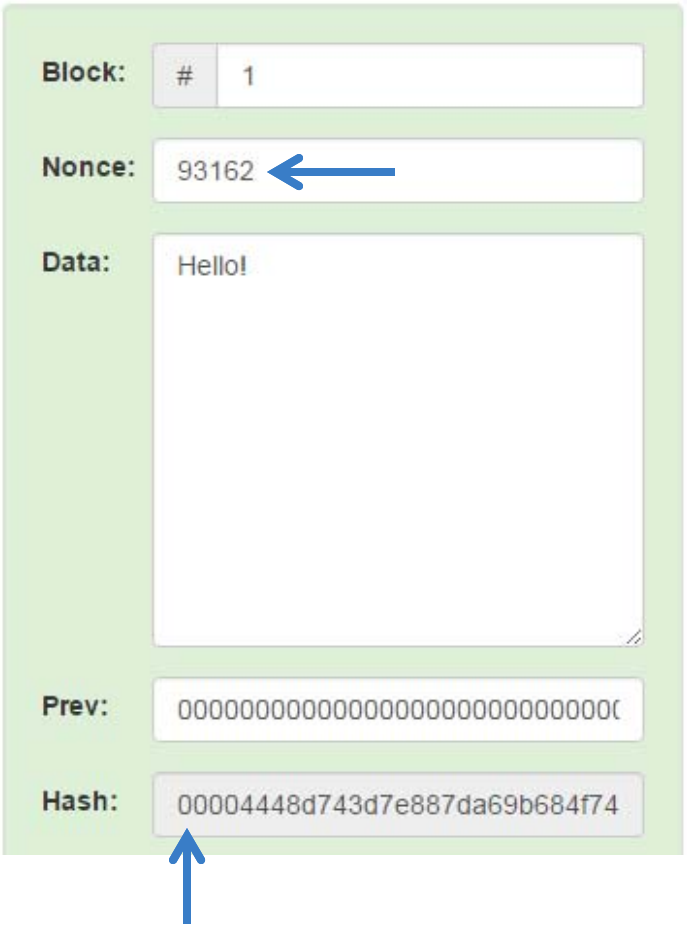
- As such, a Block may consist of:
  - A Block number or timestamp
  - “Nonce” value – a random number
  - The record or data – “Hello!”
  - Hash value of the data from the previous Block
- These are the inputs from a Block into the hash function to create a validated hash value for the Block

How does Blockchain work? Blocks



- Here, given the inputs, the resulting hash value for this Block is not validated – it does not start with “0000”
- To validate the Block, we are permitted to manipulate the nonce input which will change the hash value

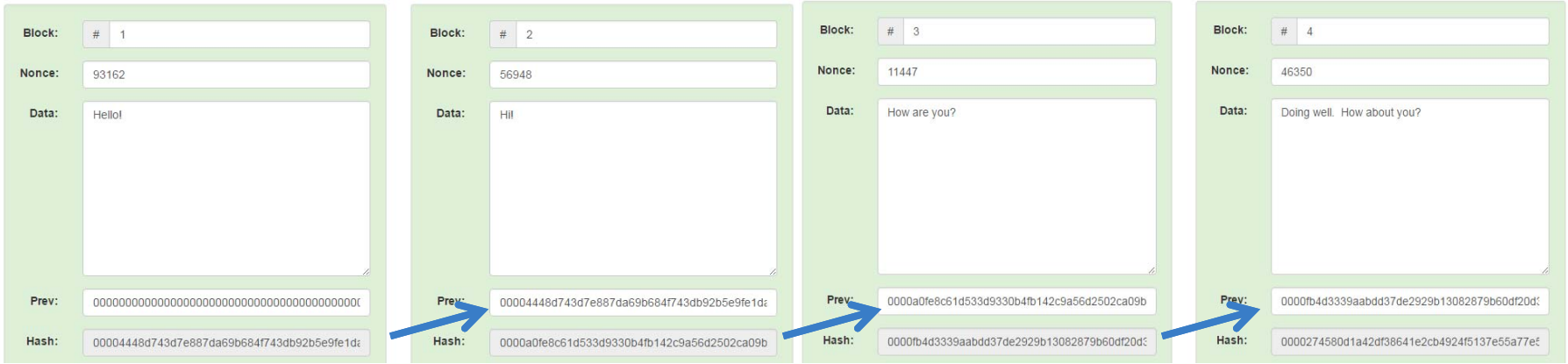
How does Blockchain work? Blocks



- A program checks different nonce values to find the one that outputs a hash value starting with four zeros to validate the Block
- Only this combination of inputs will return this validated hash value

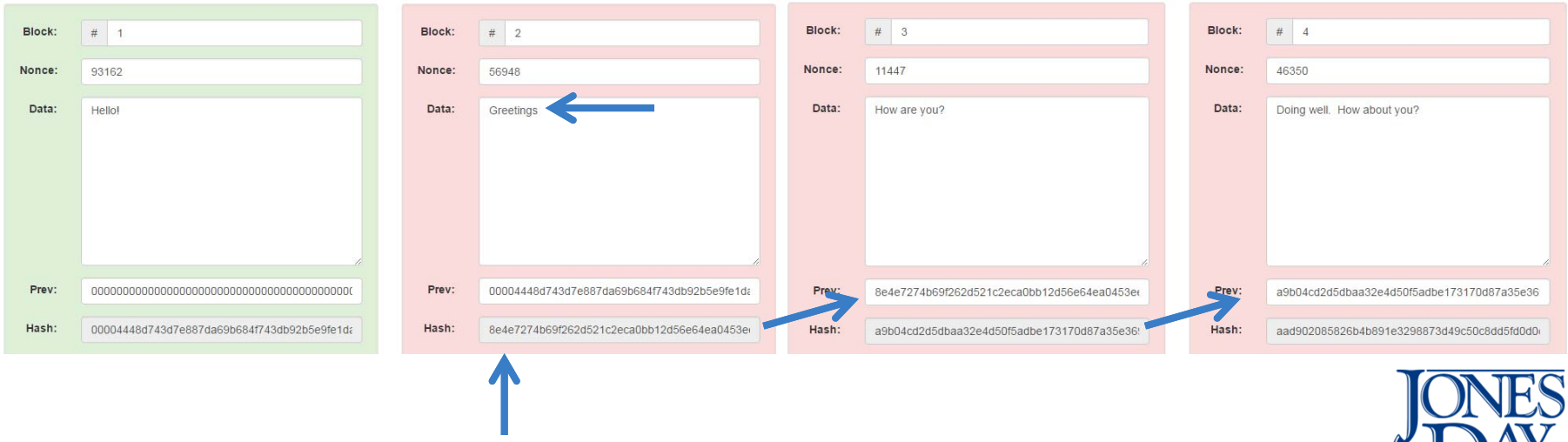
How does Blockchain work?
A Blockchain

- A Blockchain is simply a chain of Blocks
- Each Block refers back to the previous Block in the chain – the hash value of the previous Block serves as an input for the hash value of the new Block
- As other data is inputted, the program changes the nonce to result in a validated hash value



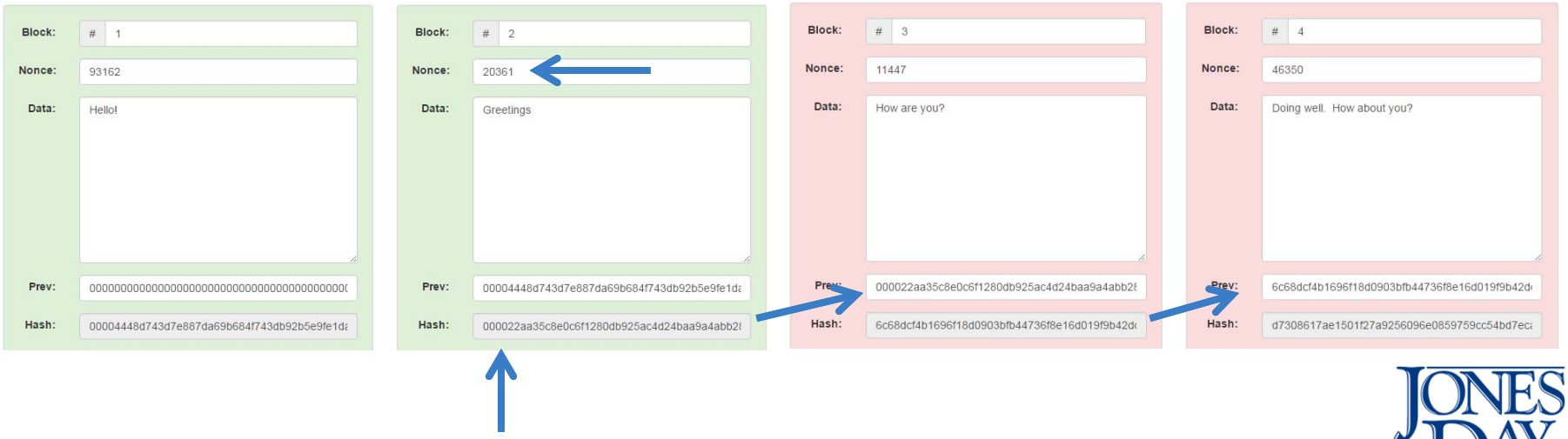
How does Blockchain work?
A Blockchain

- If any part of a Block is later changed then the hash value for that Block changes and becomes invalidated, meaning it does not begin with “0000”
- All the Blocks thereafter also become invalidated
- Here, the data in Block 2 changed from “Hi!” to “Greetings” and the resulting hash value for the Block is invalidated and breaks the balance of the Blockchain



How does Blockchain work?
A Blockchain

- Block 2 with the new data, and each subsequent Block, can be revalidated by changing the nonce value via a program
- While the resulting hash value for Block 2 now starts in “0000,” the hash value is different from that when Block 2 contained the old data, “Hi!,” and the chain is still broken



How does Blockchain work? Distributed Blockchains

- Revalidating the remaining Blocks, we now have a validated Blockchain with the new data in Block 2
- But how do we know this Blockchain has changed?
- Because Blockchains are distributed to all users we can simply compare the last hash value of this Blockchain to that of the other Blockchains
- Where the hash values do not match and the Blockchains are different, digital consensus algorithms determine which Blockchain is the reliable one

Appendix B
Sources and other materials

Sources and other materials

- http://www.investopedia.com/terms/b/blockchain.asp
- http://www.blockchaintechnologies.com/blockchain-definition
- http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
- http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
- http://www.coindesk.com/commonwealth-bank-wells-fargo-test-blockchain-cotton-trade/
- http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/

Sources and other materials

- http://ledgerexplorer.t0.com/static/search.html
- http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts
- https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf
- https://www.ethnews.com/life-insurance-companies-need-transparency-for-beneficiaries-sake
- https://www.americanbanker.com/news/corporate-boards-are-on-board-with-blockchain-survey-finds
- https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html?_r=1

Sources and other materials

- http://www.coindesk.com/citi-nasdaq-partner-blockchain-payments-solution/
- https://thefinanser.com/2016/08/applying-blockchain-payments.html/
- https://cardozo.yu.edu/faculty-intellectual-life/bitcoin-under-uniform-commercial-code
- https://www.ethnews.com/blockchain-apps-will-transform-p2p-payments
- https://www.finextra.com/blogposting/13033/blockchain-payments-disruption-use-cases-and-real-world-examples-recent-developments

Sources and other materials

- https://www.occ.treas.gov/about/who-we-are/occ-for-you/alumni/supervisions/top-stories/sup-nov-2016-compt-announces-launch-of-office-of-innovation.html
- https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-152.html
- https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf
- https://anders.com/blockchain/
- https://www.sec.gov/news/press-release/2017-131
- https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings