How Blockchain Technology is Revolutionizing Business and the Law

January 24, 2018

Scott Kimpel, Partner
Tyler Maddry, Partner
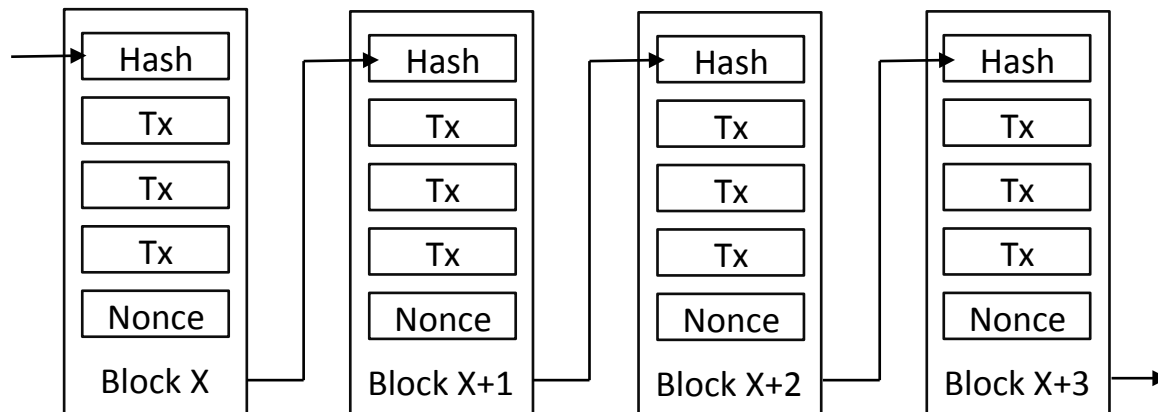**Mayme Donohue, Associate**
Hunton & Williams LLP

Joseph McNamara,
Senior Associate General
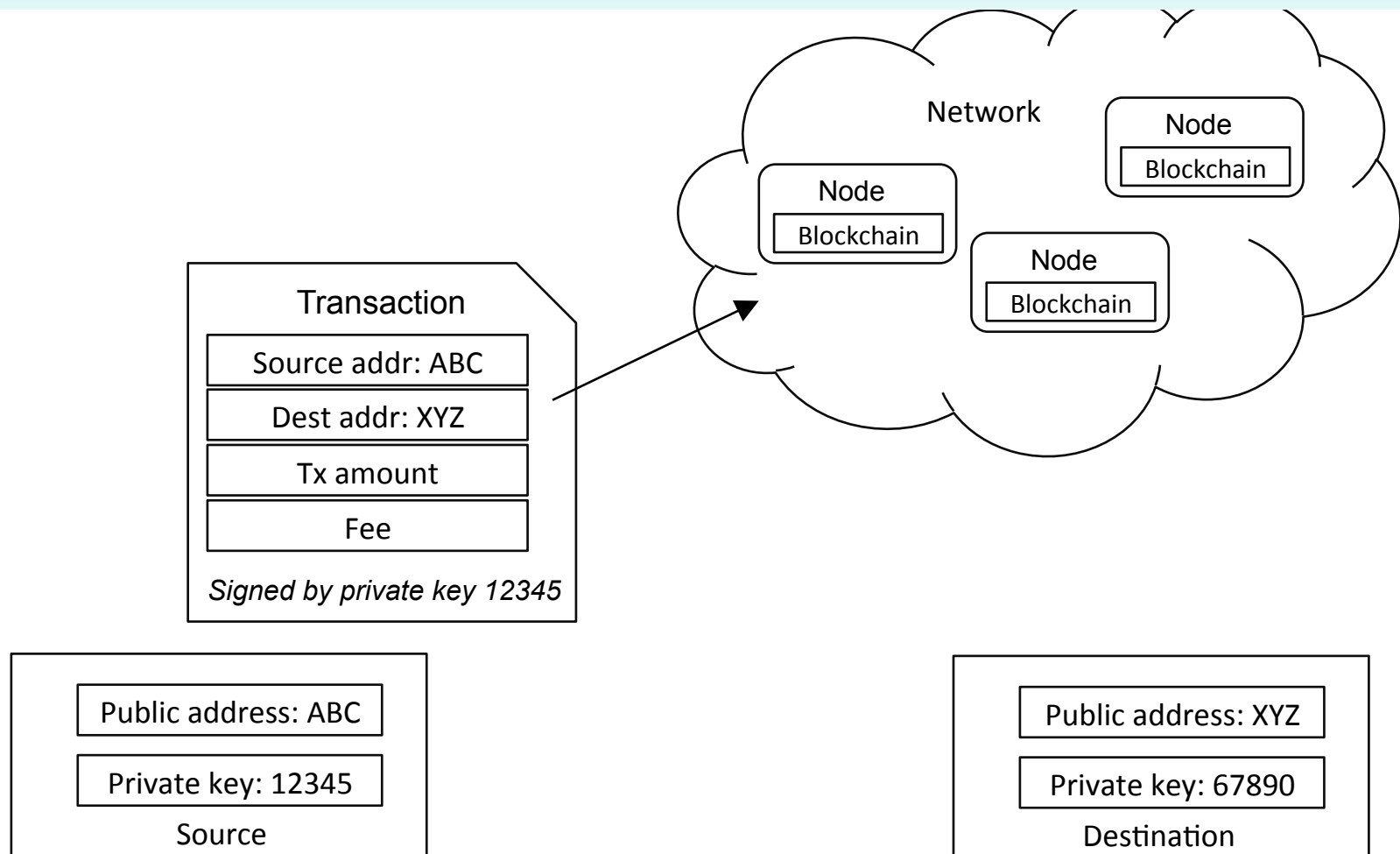**Counsel**
Nasdaq, Inc.

Overview

➢ What is Blockchain?

➢ Bitcoin and cryptocurrency

➢ ICOs and Token Sales

➢ Delaware Corporate Law

➢ Blockchain's Practical Applications

➢ Smart Contracts

➢ Intellectual Property Rights

➢ Cybersecurity

➢ Nasdaq's Approach to Blockchain

➢ Q&A

What is Blockchain?

➢ Generally, blockchain = a data store (or *distributed ledger)* that:
  ➢ contains transactions (arranged in "blocks" -- "chained" together);
  ➢ is replicated across a peer-to-peer network in real-time;
  ➢ uses cryptography to prove identity / control access; and
  ➢ is immutable (i.e., it's difficult to change historical records).

➢ There are many distinct blockchain implementations.
  ➢ Many blockchain-based platforms allow for *smart contracts.*

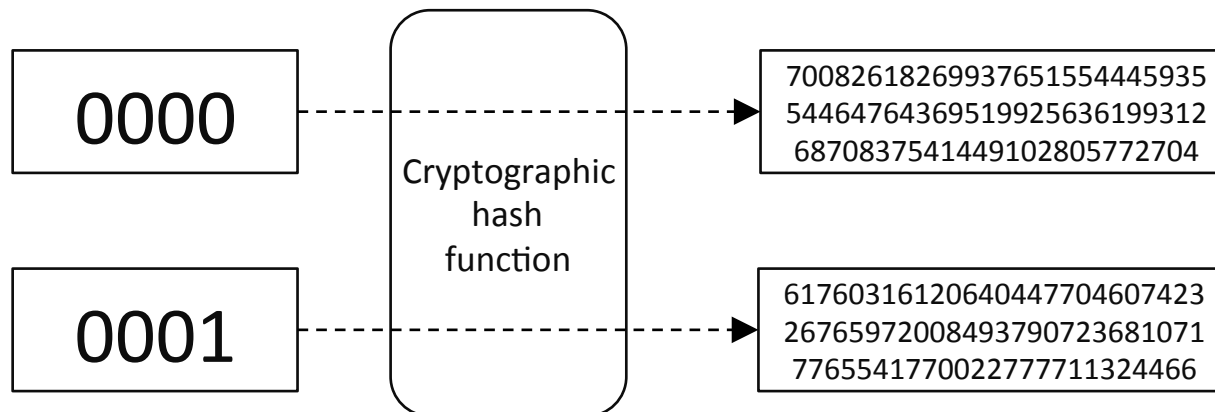| Hash		Hash		Hash		Hash
Tx		Tx		Tx		Tx
Tx		Tx		Tx		Tx
Tx		Tx		Tx		Tx
Nonce		Nonce		Nonce		Nonce
Block X		Block X+1		Block X+2		Block X+3

Blockchain Transactions

Building the Chain

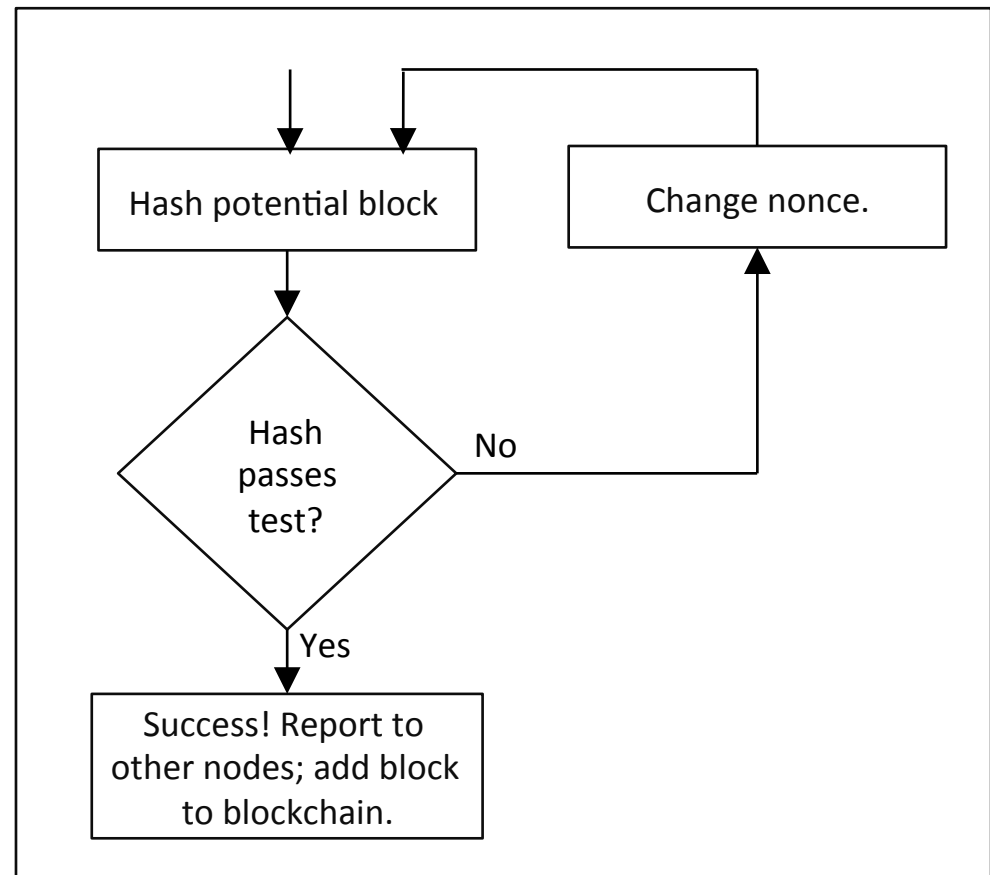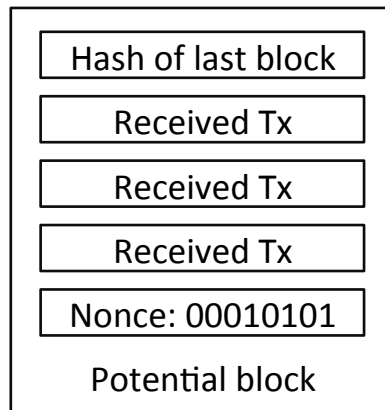## Adding ("mining") blocks - cryptographic hash functions

➢ One-way function: input cannot be derived from output, but output can be verified if input is known.

➢ Small changes in input result in changes to output that are (generally) impossible to predict.

➢ If you want to find an output value with given characteristics, "brute force" is (generally) the only way to find the right input.

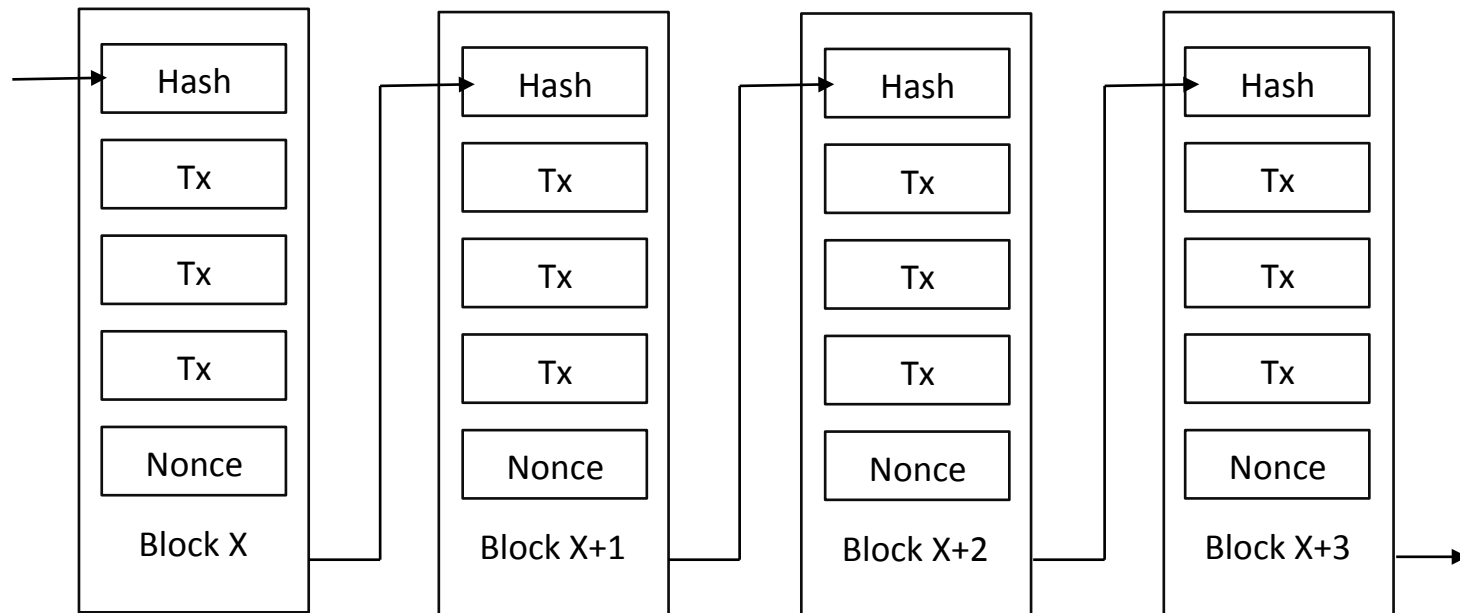| 0000 | → | Cryptographic hash function | → | 70082618269937651554445935 54464764369519925636199312 68708375414491102805772704 |
| 0001 | | | → | 61760316120640447704607423 26765972008493790723681071 77655417700227777711324466 |

Building the Chain

Adding ("mining") a block

➤ Nodes run "consensus algorithm."

➤ Successful miner receives fees + "block reward."

➤ Possible hash outputs > 1e+77 possibilities

  ➤ Bitcoin nonce: > 4 billion possibilities

  ➤ Ethereum nonce: > 1.8e+19 possibilities

➤ *Why do this?*

Potential block
Hash of last block
Received Tx
Received Tx
Received Tx
Nonce: 00010101

Flowchart:

Hash potential block → Hash passes test?
- No → Change nonce. → (back to Hash potential block)
- Yes → Success! Report to other nodes; add block to blockchain.
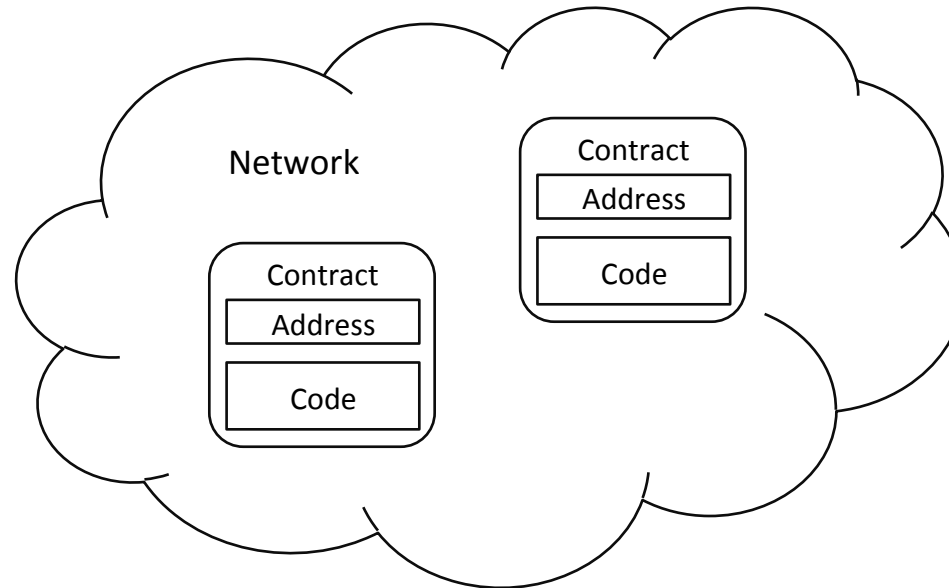
Immutability

Blockchain immutability – and why it's a block*chain*

Blockchain and Smart Contracts

➢ Smart contract = code running on nodes in the network.

    ➢ Distributed applications ("dApps") can use smart contracts.

➢ A contract has an address and can participate in transactions.

➢ Compute power paid for in virtual currency.

➢ *Why smart contracts*?

<u>Types of Blockchains – Benefits</u>

➢ Variations: public / private; different consensus algorithms; etc.

➢ Where can blockchain technology provide the greatest benefits?

  ➢ Multiple participants <--> important to validate activity on the network.
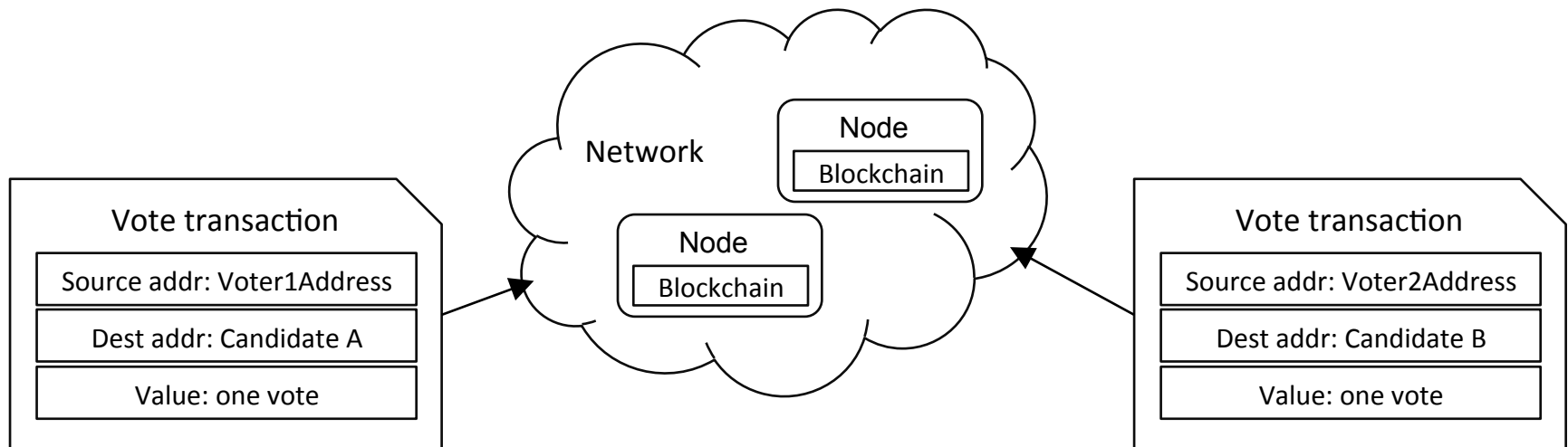
What is Cryptocurrency?

➢ AKA "Digital Currency" and "Virtual Currency"

➢ IRS definition:
- A digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value.
- In some environments, it operates like 'real' currency, but it does not have legal tender status in the U.S.
- Virtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency, is referred to as "convertible" virtual currency.
- Bitcoin is one example of a convertible virtual currency.
- Bitcoin can be digitally traded between users and can be purchased for, or exchanged into, U.S. dollars, Euros, and other real or virtual currencies.

What is Bitcoin?

➢ Created in 2008 by a person or group that used the pseudonym "Satoshi Nakamoto"

➢ Is "pseudonymous" (i.e., partially anonymous) in that an individual is identified by an alpha-numeric public key/address.

➢ Relies on cryptography for security based on public and private keys and complex mathematical algorithms.

➢ Runs on a decentralized peer-to-peer network of computers.

What is Bitcoin?

➤ "Miners" operate on open-source software; validate and irrevocably log transactions on a permanent public distributed ledger visible to the entire network.

➤ By solving complicated mathematical problems, miners can earn new Bitcoin.

➤ Solves the lack of trust between participants who may be strangers to each other.

➤ Enables the transfer of ownership without the need for a central intermediary.

What is an ICO?

➤ Acronym for "Initial Coin Offering"

➤ Form of financing technique in which a company (typically operating in the digital currency space) makes a "token" available for sale.

➤ The token gives the purchaser some future right in the business or other benefit.

➤ ICO promoters prepare white paper describing token technology and market the offering on the basis of the white paper.
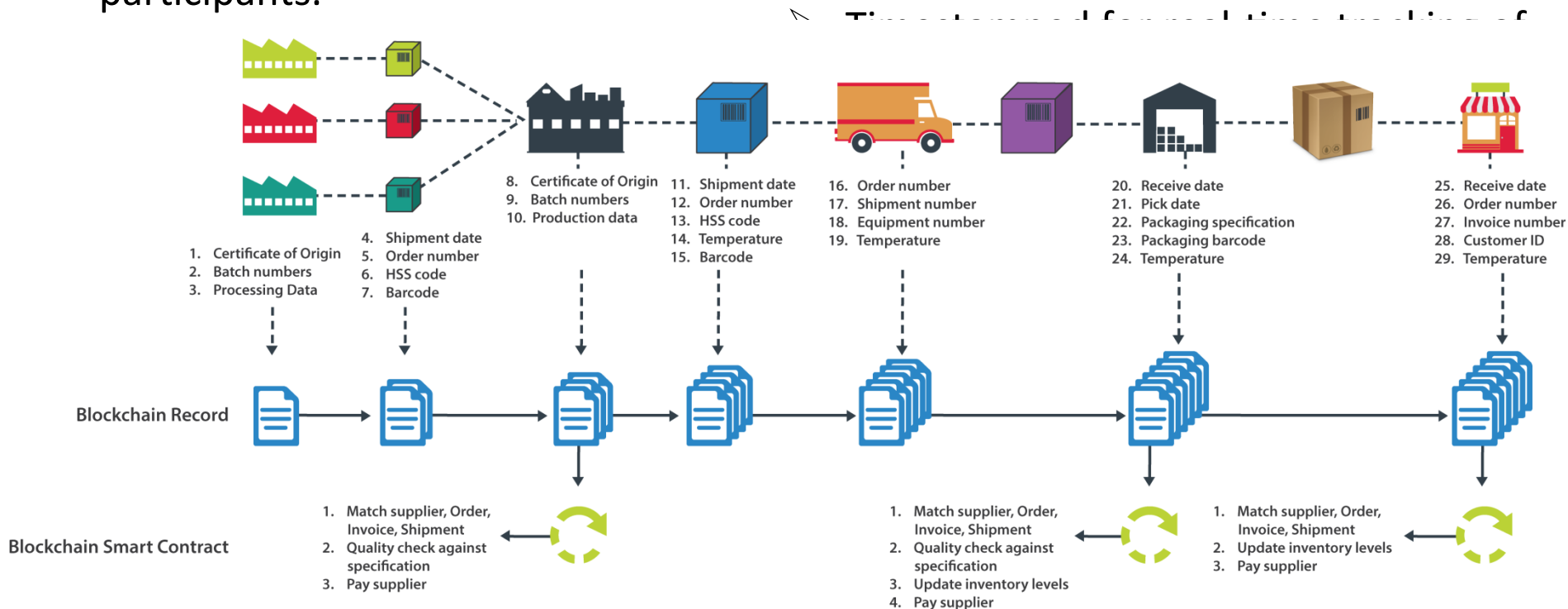
<u>Regulation of ICOs</u>

➢ SEC and CFTC have both taken the position that "tokens" may be securities or commodities subject to their respective jurisdictions.

➢ China and other countries have moved to ban ICOs.

➢ SEC, states and private plaintiffs have begun suing ICO promoters.

Practical Applications of Blockchain

➢ Initial blockchain applications were developed for finance and banking.

➢ Financial transactions are just one type of transaction that can be recorded and settled using blockchain.

➢ Blockchain solutions are being developed across industries to solve inefficient systems.

➢ BUT – beware of the hype. It is not the solution for everything.

Supply Chain Management

➢ Permanent record of the journey of the assets.

➢ Shared among all network participants.

➢ Timestamped for real-time tracking of

Blockchain Record

1. Certificate of Origin
2. Batch numbers
3. Processing Data

4. Shipment date
5. Order number
6. HSS code
7. Barcode

8. Certificate of Origin
9. Batch numbers
10. Production data

11. Shipment date
12. Order number
13. HSS code
14. Temperature
15. Barcode

16. Order number
17. Shipment number
18. Equipment number
19. Temperature

20. Receive date
21. Pick date
22. Packaging specification
23. Packaging barcode
24. Temperature

25. Receive date
26. Order number
27. Invoice number
28. Customer ID
29. Temperature

Blockchain Smart Contract

1. Match supplier, Order, Invoice, Shipment
2. Quality check against specification
3. Pay supplier

1. Match supplier, Order, Invoice, Shipment
2. Quality check against specification
3. Update inventory levels
4. Pay supplier

1. Match supplier, Order, Invoice, Shipment
2. Update inventory levels
3. Pay supplier

Source: Resolve Solution Partners

Food and Product Safety

➤ Traces the origin and source of each item at retail.

➤ Faster identification of contaminated or defective products.

Source: Resolve Solution Partners
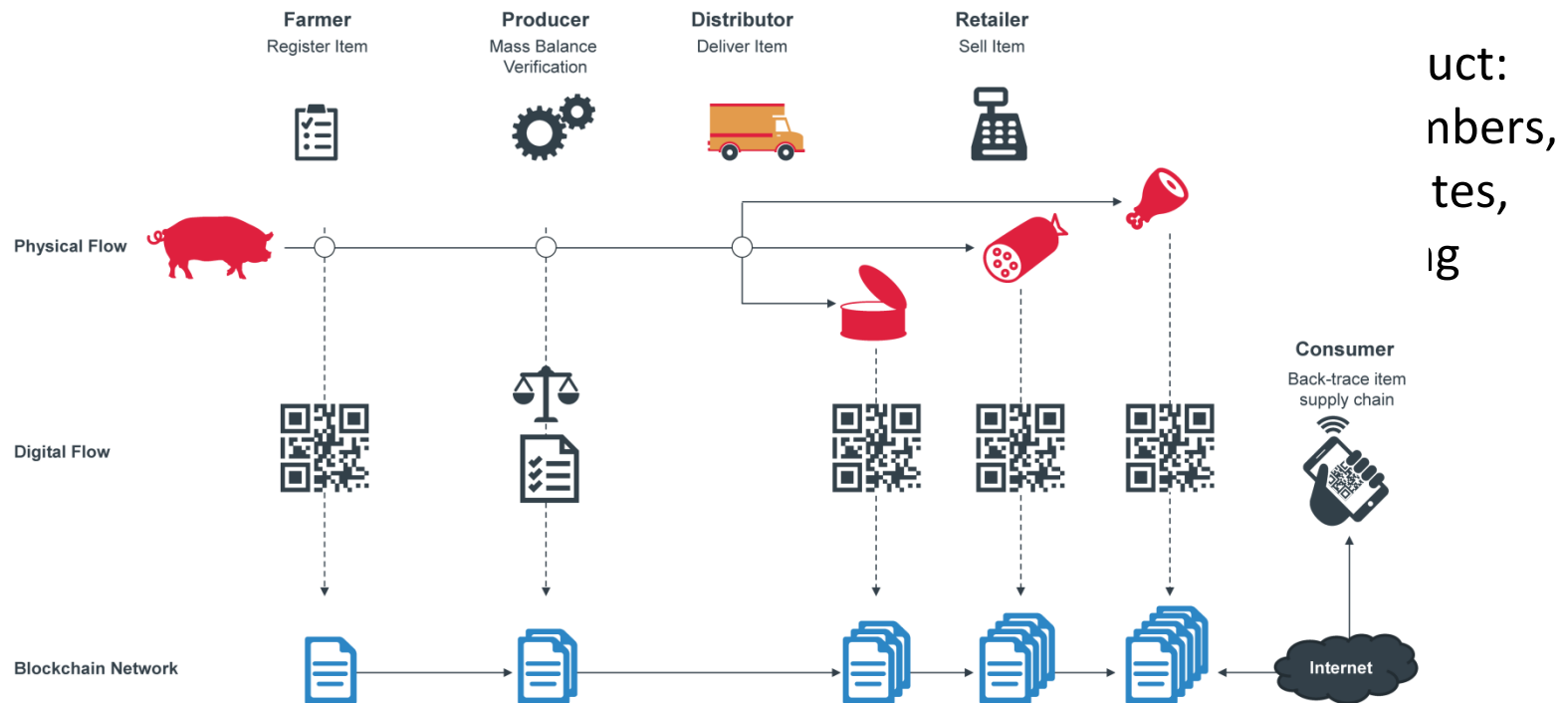
Healthcare

➢ Pharmaceuticals supply chain – MediLedger – built to the requirements of the U.S. Drug Supply Chain Security Act.

➢ Testing applications for Electronic Medical Records.

➢ Health insurance applications and payer administration.

➢ Healthcare provider licensure and credentialing – being tested by Illinois with the Hashed Health consortium.

➢ Revenue cycle management and fraud prevention.

Energy

➢ Improved grid management.

- Sun Pacific recently integrated blockchain into its renewable energy grid management.

➢ Peer-to-Peer Energy Trading.

- Brooklyn Microgrid allows participants to generate, store, buy and sell energy at the local level.

➢ Energy Commodities Trading.

- BP, Shell and Statoil are working on a blockchain-based digital platform for post-transaction management of physical energy commodities trading.

Consumer Confidence and Loyalty

➢ Verify authenticity of rare and valuable products.

- Same concept as the supply chain and food safety uses.
- Allows customers to scan barcodes in the retail environment and verify the origin and other key features of products

➢ Consumer rewards programs.

- Issue, track and spend rewards points on blockchain.
- Reduces balance of unspent or unused rewards.
- Improve targeted communications based on individual behavior.

Real Property Registry and UCC Filings

➢ Register title to real property assets.

- Cook County Recorder of Deeds Blockchain Pilot Program – *"designed a blockchain real estate conveyance software workflow that can be a framework for the first legal blockchain conveyance in Illinois (and possibly the US)."*

- Projects underway in other countries – examples like Georgia, Sweden and the Ukraine.

➢ UCC Filings.

- Delaware Blockchain Initiative – "smart UCC" filings intended to (1) automate the release or renewal of UCC filings and related collateral, (2) increase the speed of searching UCC records, (3) reduce mistakes and fraud and (4) cut cost.

Smart Contracts

➢ What is a Smart Contract?

- • Computer code stored in a block

- • Consent between two or more parties

- • Code is fixed, state changes

- • Code is automatically executed in each node upon trigger event

- • Ensures performance through automation

➢ Ethereum Platform, Solidity and EVM

Smart Contracts vs Conventional Contracts

➢ How is a Smart Contract different from a conventional contract?

- In many cases, only discrete elements of a contract can be automated

- Applicable to situations where performance can be verified objectively by reference to an information source

  - No human judgment or intervention

  - Oracles

- May or may not be legally binding

- Very difficult to amend

  - The DAO example

Blockchain IP

➤ Development of Blockchain Intellectual Property

- Significant increase in patent filings

  - Major Financial Institutions

  - Major Technology Companies

  - Blockchain startups

  - EITC Holdings

- Examples of patents

  - Accenture: rewritable blockchain

  - Nasdaq: data matching system

  - BofA: cryptocurrency exchange

  - CME: mining derivatives

Protecting Your Company's Blockchain IP

➢ Integrate with your development team early to understand development projects and timeline

➢ Ask about what innovative features are being created

➢ Keep track of statutory bars that require early filing of patent application (35 USC 102)

➢ Consider whether expense of patent filing is justified

- How good is the idea?

- How valuable would the patent be?

- Consider other benefits of filing (proof of invention, deterrent effect, negotiations)

➢ Expect some challenges related to patenting of IT-related inventions (*Alice v. CLS Bank*)

➢ Contractual protections (nondisclosure, use restrictions, ownership of developed IP)

Handling Infringement Risks

- ➤ No easy answer, although standard defenses are available
  - Abstract Idea under *Alice v. CLS Bank*
  - Invalidity based on prior art
  - Non-infringement
- ➤ Defensive patent filings
- ➤ Blockchain patent initiatives
  - Blockchain Patents Roundtables
  - Patent pledges by Blockstream and Coinbase
  - Chamber of Digital Commerce

Open Source Licensing Issues

➢ Blockchain platforms commonly use open source software

- Bitcoin uses MIT license

- Ethereum uses GPL, Affero and others

➢ Your implementation on blockchain may involve distribution of code to third parties

➢ OSS licenses are permissive or restrictive, with very different rights and obligations

➢ Key actions include modification, distribution, and combining or linking software code

➢ Implement an OSS policy to understand and comply with OSS licenses

<u>Privacy and Cybersecurity</u>

➢ At a high level, concerns include:

- Privacy and anonymity of information

- Preserving data integrity

- Cybersecurity risks and safeguards

➢ Blockchains may adopt varying levels of "permissions"

- Permissioned blockchains allow for greater privacy

- Bitcoin is an example of a "permissionless" blockchain

Privacy and Cybersecurity

➢ Data integrity is a key security risk that can be managed with blockchain technology

- Data contained in a blockchain is unalterable

- Data can only be added to a blockchain; it cannot be modified or removed

- All systems maintaining the blockchain must agree on changes

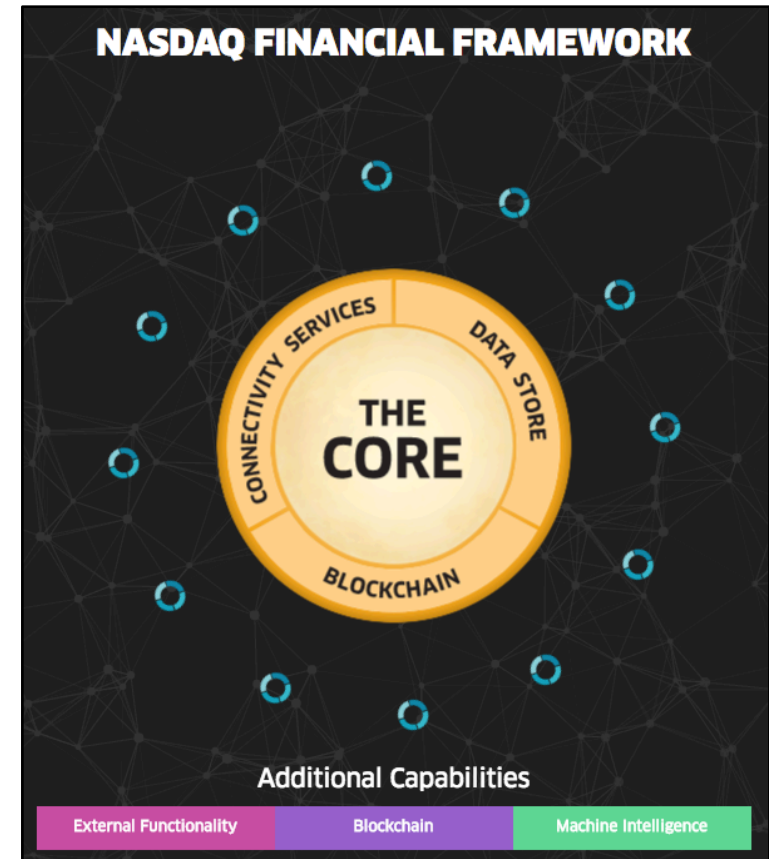- Data stored in a blockchain can be encrypted as an added security layer

Privacy and Cybersecurity

➢ A key benefit of blockchain technology is its security

  • Blockchain is decentralized and transparent

  • These security features reduce blockchain technology's vulnerability to cyberattacks

➢ But key risks still exist

  • Vulnerabilities at the intermediary level—target of hacker attacks

  • Use of blockchain technology to facilitate cyberattacks (such as ransomware) by preserving a bad actor's anonymity

Nasdaq Blockchain Projects

➢ Private securities transactions (Linq)

➢ SIX Swiss Exchange

➢ Share e-voting in Estonia and South Africa

➢ NYIAX: advertising exchange

➢ NFF blockchain service

NASDAQ FINANCIAL FRAMEWORK

CONNECTIVITY SERVICES · DATA STORE

THE CORE

BLOCKCHAIN

Additional Capabilities

| External Functionality | Blockchain | Machine Intelligence |

Questions?

Contacts

Hunton & Williams LLP

➢Scott Kimpel, Partner

➢Tyler Maddry, Partner

➢Mayme Donohue, Associate

Nasdaq, Inc.

➢Joseph McNamara, Senior Associate General Counsel