SHOOK
HARDY & BACON

Beginning Blockchain

Legal Issues and Developments
in the New Smart Economy

Agenda

Fun Facts

What is Distributed Ledger Technology ("DLT")?

Attributes of Distributed Ledger Technologies

Cryptoeconomics

Smart Contracts

How does the U.S. Government Classify "Cryptocurrency?"

The New "Smart" Economy

Relevance to Legal Practitioners

How does it work? Centralized vs. Decentralized

Recap: Attributes of Distributed Ledger Technologies

Questions?

Fun Facts

Bitcoin (BTC)

Miner's block reward

12.5 BTC ≈ $95,662.25*

Ethereum (ETH)
ICO 2014
2000 ETH ≈ $500 USD
(25 cents/ETH)

2000 ETH ≈ $1,205,680.00*

*based on June 8, 2018 data from coinmarketcap.com

Fun Facts

Binance Exchange

- Opened operations in 2017
- Binance is now more profitable than Deutsche Bank (world's most profitable bank)

Q1/18 - $200M vs. $146M

Bitcoin Mining Power Expend*iture*

- 2.6GW of power
  - Power consumption of Ireland
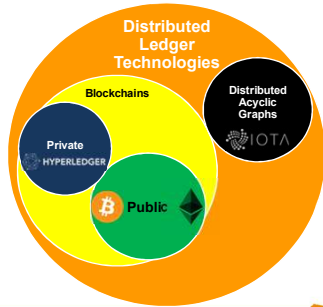- Estimated 7.7GW by end of 2018

4

Update of the Law CLE   June 14, 2018

What is Distributed Ledger Technology?

Distributed Ledger Technologies

Blockchains

Distributed Acyclic Graphs
IOTA

Private
HYPERLEDGER

Public

Attributes of D.L.T.

- A distributed ledger is a growing list of records shared and maintained by each computer (node) of a distributed network.

Distributed Ledger

Immutable
Secure
Tamper-proof

- The use of cryptography ensures that *records cannot be changed*.

Decentralized
No single point of failure

- *Every computer* (node) on the decentralized network *maintains a copy* of the ledger.

Consensus
No need for trusted 3rd party

- Before a transaction can be executed, *majority* of computers (nodes) on the network *must agree that the transaction is valid*.
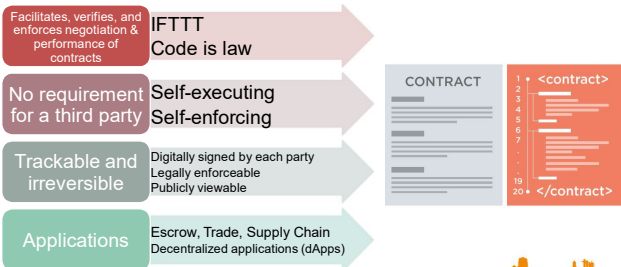
Cryptoeconomics

- Solving the issue of trust between counterparties without reliance on trusted third parties.
  - Trusted third parties (intermediaries) are **inefficient** and **costly**
  - Solution: Distributed Ledger Technologies

Cryptoeconomics

- Blockchains are built on teachings of distributed networks and *applied cryptography* to:
  - Make it economically infeasible for bad actors to cheat
  - Provide incentives to those who maintain and secure the network
  - Make data transparent, provable, and immutable

Smart Contracts: Programs on the Blockchain

Facilitates, verifies, and enforces negotiation & performance of contracts	IFTTT Code is law
No requirement for a third party	Self-executing Self-enforcing
Trackable and irreversible	Digitally signed by each party Legally enforceable Publicly viewable
Applications	Escrow, Trade, Supply Chain Decentralized applications (dApps)

CONTRACT

How does the U.S. Government classify "cryptocurrency?"

A: It depends on which agency you ask.

IRS	**CFTC**	**SEC**	**Treasury**	**???**
Property	Commodities	Securities	Money	Coins Tokens

The New "Smart" Economy

- Supply Chain
- Health & Medicine
- Automotive
- Insurance
- Real Estate
- Entertainment
- Firearms
- Technology

Relevance to Legal Practitioners

- Clients have already begun testing or implementing DLT.

- Disruptor start-ups are continuously looking to upend well-established industries.

- Market forces may demand transparency and decentralization.

Relevance to Legal Practitioners

- Blockchain-focused law firms
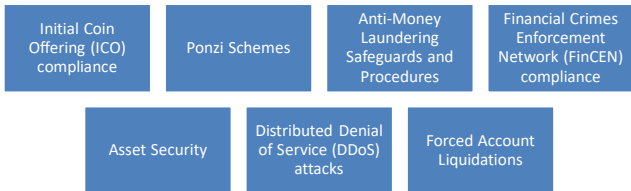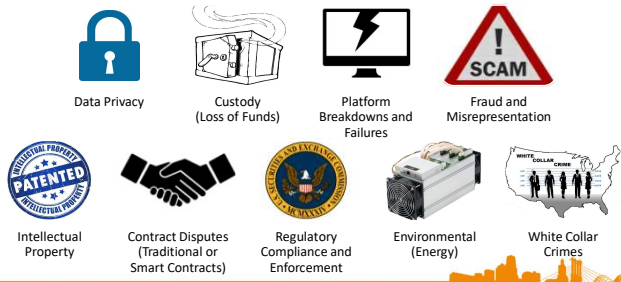 - Emphasis on Initial Coin Offerings (ICOs), Regulatory Guidance, and Smart Contracts.

- Increasing demand for cutting-edge skill sets
  - Writing, reading, or opining on smart contracts.
  - Reviewing and analyzing Blockchain data.

Relevance to Legal Practitioners
Current "Hot" Areas of Litigation

Initial Coin Offering (ICO) compliance	Ponzi Schemes	Anti-Money Laundering Safeguards and Procedures	Financial Crimes Enforcement Network (FinCEN) compliance
Asset Security	Distributed Denial of Service (DDoS) attacks	Forced Account Liquidations	

Relevance to Legal Practitioners
Potential Areas of Litigation

Data Privacy	Custody (Loss of Funds)	Platform Breakdowns and Failures	Fraud and Misrepresentation
Intellectual Property	Contract Disputes (Traditional or Smart Contracts)	Regulatory Compliance and Enforcement	Environmental (Energy)	White Collar Crimes

Questions for Legal Practitioners

- Regulatory Issues
  - Initial Coin Offerings (ICO)
    - Under *Howey*, most likely securities
  - ❖ What about tokens that *may have been* securities, but have evolved into something else?
    - Ethereum: ICO in 2014 (a security, maybe)
    - Today, Ether is "expended" as a *transactional gas*

Questions for Legal Practitioners

- General Products Liability / Tort
  - Fraud and consumer protection
  - ICOs: Empty promises, misleading partnership announcements
  - "Crypto" hardware

  - ❖ Who are the deep pockets?
    - Cold storage wallet suppliers/manufacturers
    - Coin/token "foundations"
    - Large-scale mining farms
    - Cryptocurrency exchanges

Questions for Legal Practitioners

- Intellectual Property: Patents
  - 700+ Blockchain-related applications received by the USPTO between January 2011 and April 2018 have been *published*
  - Aggressive patent activity typically attracts litigation

  - ❖ Is Blockchain technology patentable subject matter?
    - Majority of public projects are open source
  - ❖ Who are the target infringers?
    - See previous slide on deep pockets

Questions for Legal Practitioners

- Data Privacy (GDPR)
  - General Data Protection Regulation
    - Enforcement date of May 25, 2018

  - Data controllers must _**erase**_ _**personal data**_ "without undue delay" if the data is _no longer needed, the data subject objects to the processing, or the processing was unlawful._ GDPR, Art. 17.

  - ❖ What does it mean to "erase?"
    - Not defined in the GDPR

  - ❖ What is "**Personal Data**"?
    - "[A]ny information relating to an identified or identifiable natural person ('data subject')." GDPR, Art. 4.

Questions for Legal Practitioners

- Data Privacy (GDPR)
  - ❖ What about encrypted information?
    - _**Pseudonymized**_ personal data, which could be attributed to a natural person by use of **additional information** should be considered to be _information on an identifiable natural person_. GDPR, Recital 26.

    - The "additional information" _must be **"kept separately and ... subject to technical and organizational measures**_ to ensure that the personal data are not attributed to an identified or identifiable person." GDPR, Art. 4.

    - "[T]o ascertain whether means are "reasonably likely" to be used to identify the natural person, account should be taken of all objective factors, such as the **costs** of and the **amount of time required for identification**, _taking into consideration the available technology at the time of the processing and technological developments."_ GDPR, Recital 26.

Questions for Legal Practitioners

- Data Privacy (GDPR)
  - ❖ Blockchain vs. GDPR
  - ❖ How can an immutable ledger be in compliance with GDPR?
    - **Do not store personal data**
    - Destruction of private keys that "link" personal data to encrypted data
    - Consider integration of technologies (e.g., with trusted third-parties) to solve the problem despite perceived drawbacks
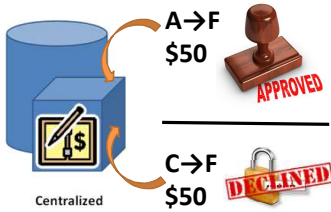
How does it work?

- Centralized vs. Decentralized
  - Simplest explanation is in the financial context

🏛 Centralized 🏛

A→F
$50
APPROVED

C→F
$50
DECLINED

Centralized

LEDGER		
(Record of Transactions)		
Parties	**Amount**	**Status**
B → E	-$25.00	Spent
A → D	-$50.00	Spent
A → Bank	$100.00	Deposit
B → Bank	$50.00	Deposit
C → Bank	$1.00	Deposit

🏛 Centralized 🏛

SINGLE POINT OF FAILURE

Centralized

A→F
$50
APPROVED

C→F
$50
DECLINED

Slide 1

Consensus
No need for trusted 3rd party

Decentralized

Decentralized
No single point of failure

MINING
- Expensive
- Incentivized
- Economically infeasible to cheat
- Better off playing by the rules

Blockchain = Immutable Ledger

⚠ INVALID

Immutable
Secure
Tamper-proof

Distributed Ledger

Slide 2

Decentralized

- Blockchains do not have to be financial.
  - Records
    - Registrations (Vehicles, Real Estate, Firearms)
    - Insurance Claim Information
    - Identity
    - Electronic Medical Records
    - Tracking Information
  - Smart Contracts

Slide 3

Recap: Attributes of DLT

- A distributed ledger is a growing list of records shared and maintained by each computer (node) of a distributed network.

Distributed Ledger

- The use of cryptography ensures that *records cannot be changed*.

Immutable
Secure
Tamper-proof

- *Every computer* (node) on the decentralized network *maintains a copy* of the ledger.

Decentralized
No single point of failure

Consensus
No need for trusted 3rd party

- Before a transaction can be executed, *majority* of computers (nodes) on the network *must agree that the transaction is valid*.

Questions?

@DLTcounsel