Internet of (Every)Things:
Emerging Technologies and Their Legal Implications

Geof Vickers, Partner

Tori M. Silas, Partner

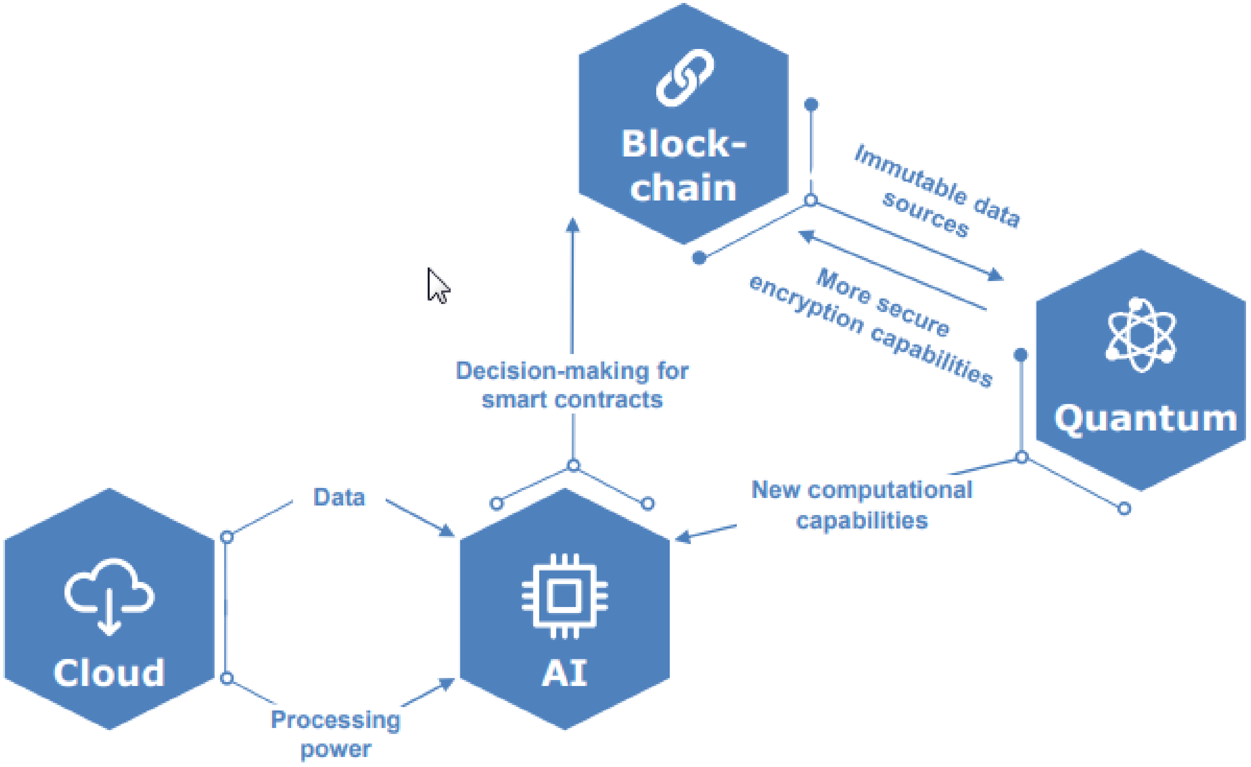
NELSON MULLINS

Introduction

- Emerging Technologies – Next Internet Revolution
  - Business Disruption
  - Altering Business Operations
  - Outpacing the Legal & Regulatory Environment
  - Mutually Reinforcing

Emerging Technologies at a Glance

1. Internet of Things (IoT)
2. AI & Machine Learning
3. Blockchain
4. Smart Contracts
5. Additional Considerations

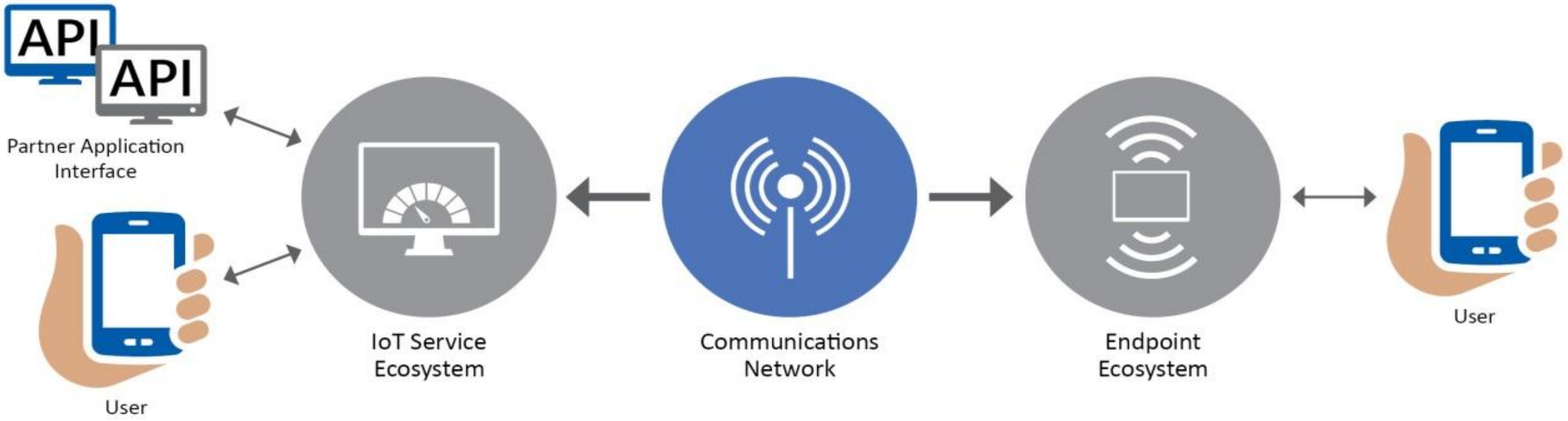


Block-chain
Immutable data sources
More secure encryption capabilities
Quantum
Decision-making for smart contracts
New computational capabilities
Data
Cloud
AI
Processing power

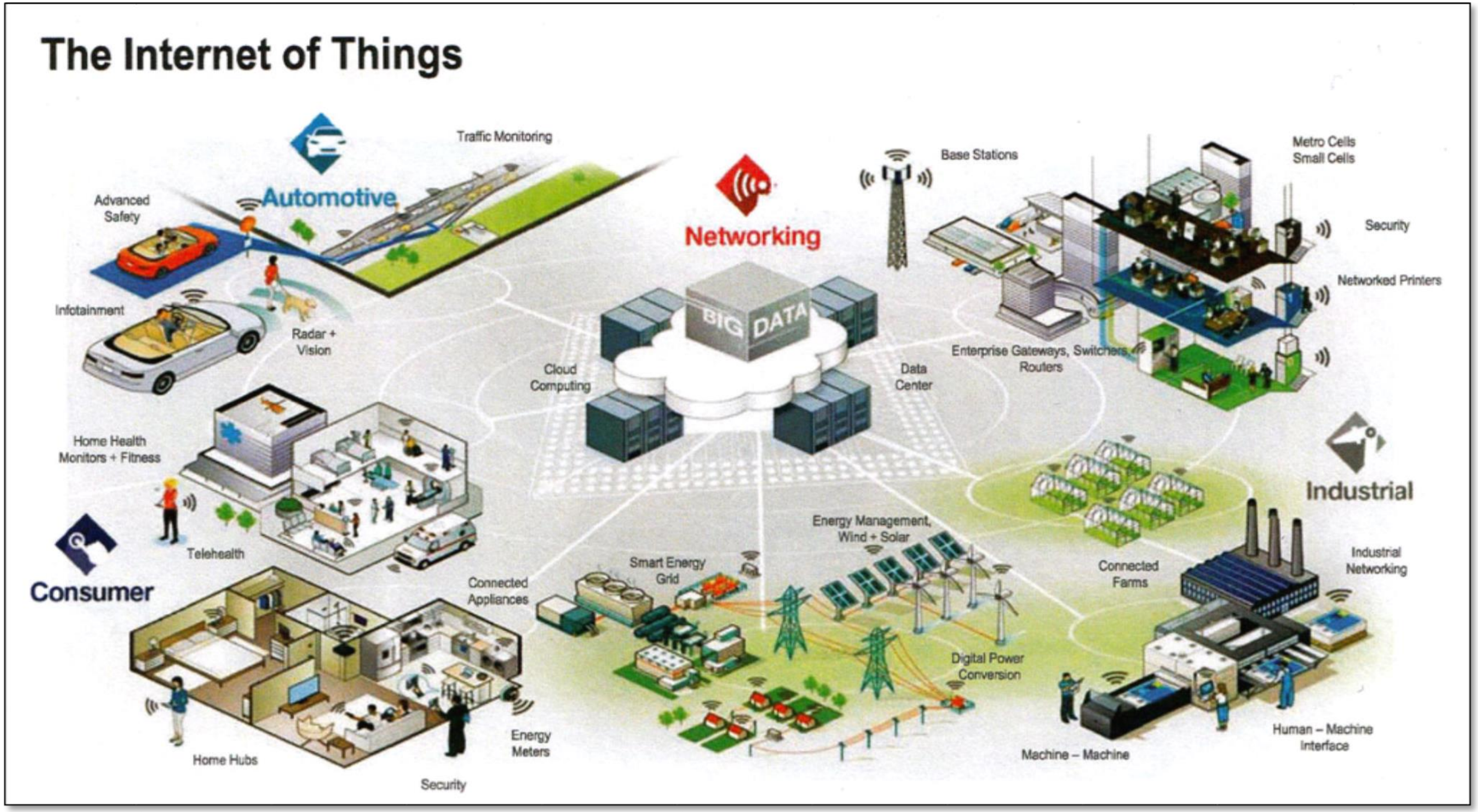
What is the Internet of (Every)Things?

- Internet of Things (IoT) - a network of connected sensors embedded in everyday objects for the purpose of collecting and sharing data via the Internet.

- IoT-related sensors and devices will reach 20 billion by 2020.



The Landscape



NELSON MULLINS

IoT Devices

amazon
theranos
one tiny drop changes everything.
Samsung
SMART TV
SIGNATURE
APPS
BROWSE
Gillette
GLAD
Tide
Picasa
36
epi
31
nest
IN 25 MIN
72

Risks Involved with IoT Devices

- IoT devices are networked and subject to hacking.
  - Components that make IoT vulnerable include sensors, computers, and Artificial Intelligence.
  - The imbedded intelligence observes and detects any change (e.g., climate, health-related, etc.)
- Outsourcing – IoT devices are updated by private companies, and users are dependent on these third parties to protect and secure the devices.
- IoT generates BiG Data

Risks Involved with IoT Devices & Regulatory Issues

- Privacy and data security concerns
- No comprehensive regulatory framework for connected devices
  - Laws and regulations vary based on platform and data type
- Over-regulation reduces utility, financial viability or operational effectiveness

Risks Involved with IoT Devices & Regulatory Issues

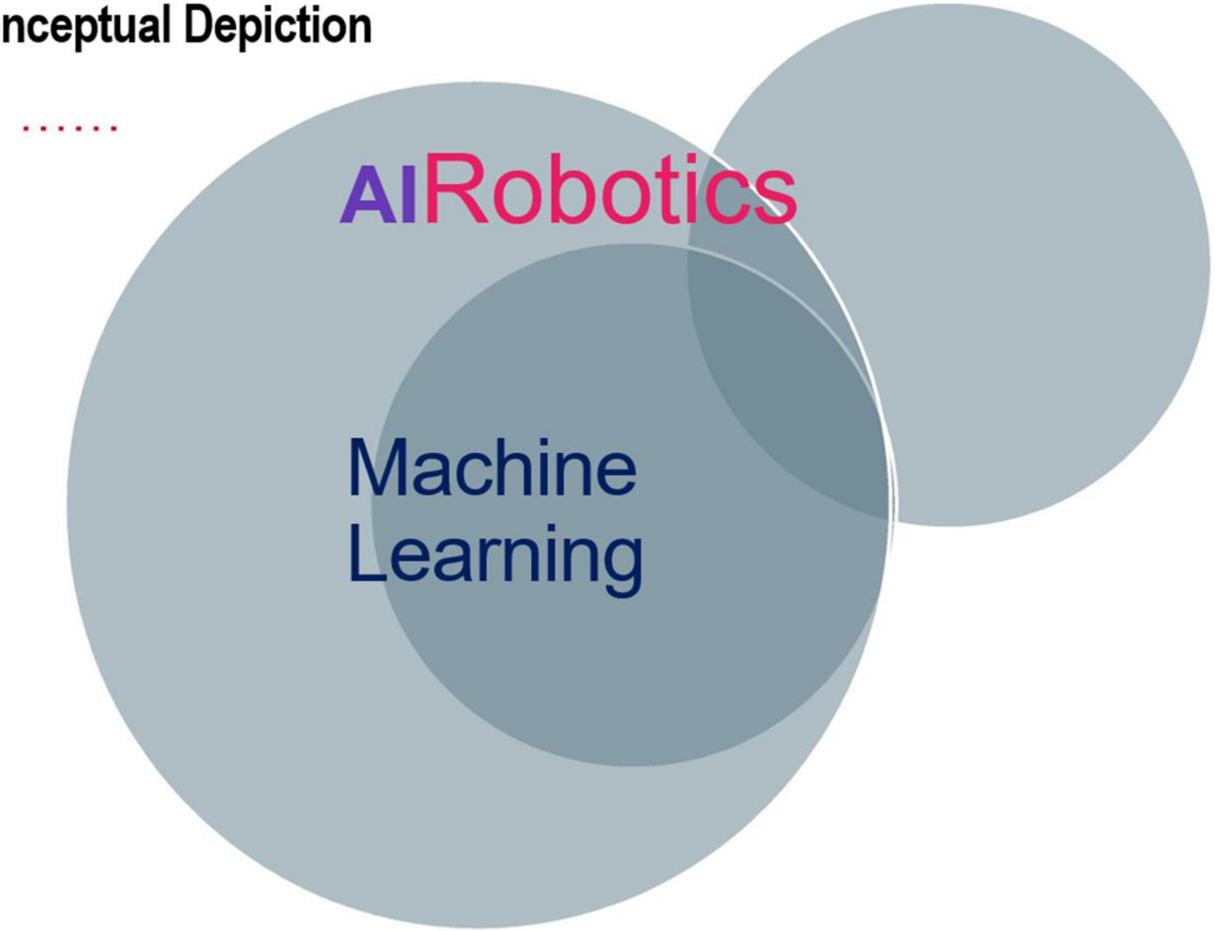
- Regulation of IoT – Who's on First?
    - Regulation by government or quasi-government agencies
    - Self-regulation by industry
    - Domestic vs. International regulations
- Congressional hearings on SMART IoT Act (May 2018)
- Litigation and privacy & security considerations

IoT and the FTC

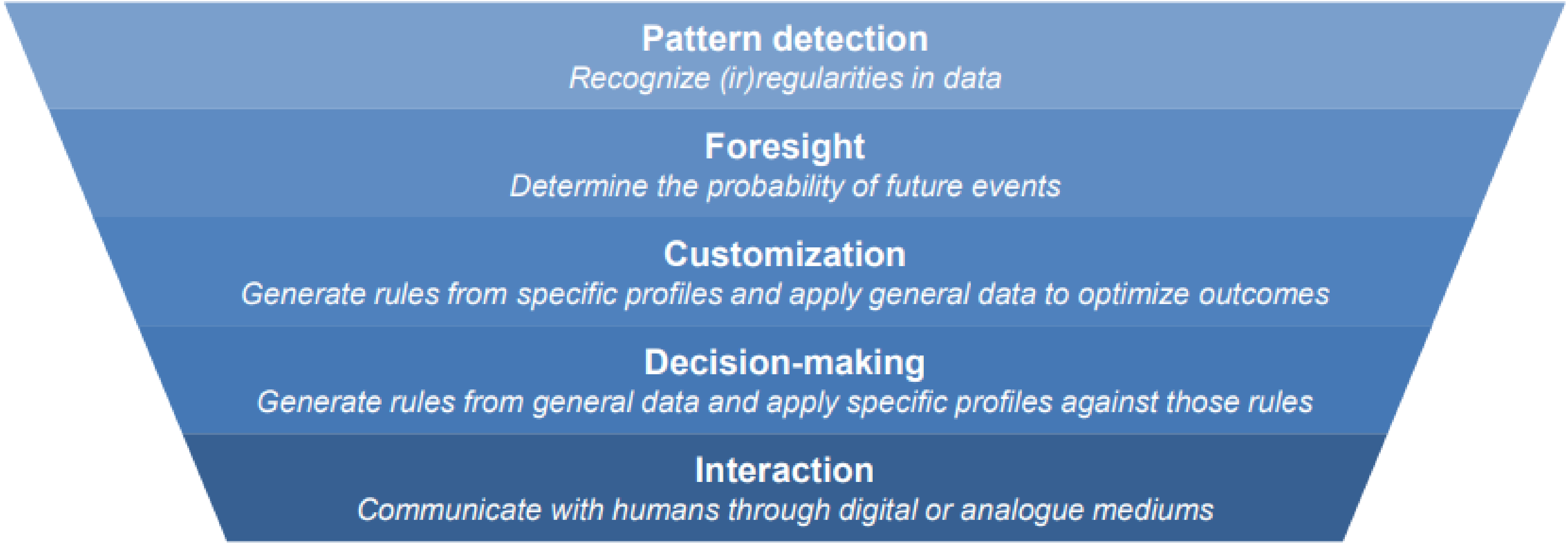
- FTC v. Aura Labs, Inc. (2016)
  - Aura Labs marketed the Instant Blood Pressure app – determined BP from placing a fingertip on a smartphone's camera. App claimed that it measured BP as accurate as traditional BP cuffs and served as a replacement.
  - FTC alleged Violation of FTC Act Section 5, which prohibits unfair or deceptive acts or practices based on Aura Labs' misrepresentation of ability to (a) replace traditional BP cuffs; and (b) measure BP as accurately as traditional cuff.
  - Consent decree: cease misrepresentations and deceptive endorsements
- FTC v. D-Link (2017)
  - FTC alleged company made deceptive claims about the security of its products and engaged in unfair practices that put consumers' privacy at risk. D-Link headlined its routers as EASY TO SECURE and ADVANCED NETWORK SECURITY.
  - Routers allegedly susceptible to easily preventable flaws like hard-coded login credentials in its camera software (username: "guest"; password: "guest"). Deceptive trade practices claims upheld.

AI & Machine Learning

Conceptual Depiction



AI-Enabled Capabilities



Pattern detection

Recognize (ir)regularities in data

Foresight

Determine the probability of future events

Customization

Generate rules from specific profiles and apply general data to optimize outcomes

Decision-making

Generate rules from general data and apply specific profiles against those rules

Interaction

Communicate with humans through digital or analogue mediums

AI & Machine Learning

- Artificial Intelligence - machines imitate (intelligent) human behavior

- Traditional AI systems were programmed to attempt to simulate human intelligence (e.g., IBM’s Deep Blue)

- Machine Learning - a subset of AI involving a system that learns from data without rules-based programming (e.g., Google Deepmind’s AlphaGo)

ARTIFICIAL INTELLIGENCE

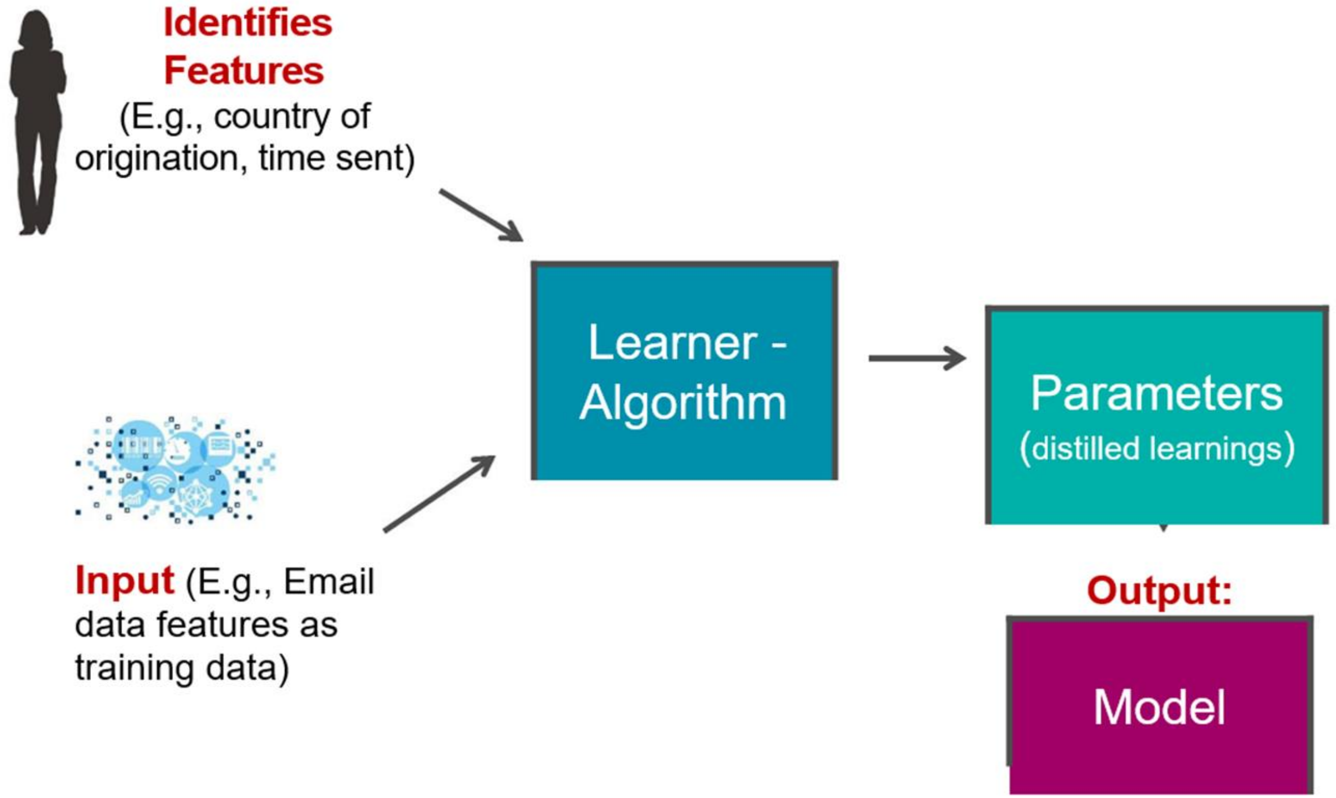
MACHINE LEARNING

AI & Machine Learning

- How does Machine Learning differ from traditional software?
  - Traditional software requires hand-coding with specific instructions to complete a task.
  - A ML system learns to recognize patterns and make predictions using large amounts of data .
  - EXAMPLE:
    - Spam the old way: “if the email contains the word ‘Patriots,’ then ...”
    - Spam the new way: ML system learns from training data to identify if email is spam

AI & Machine Learning

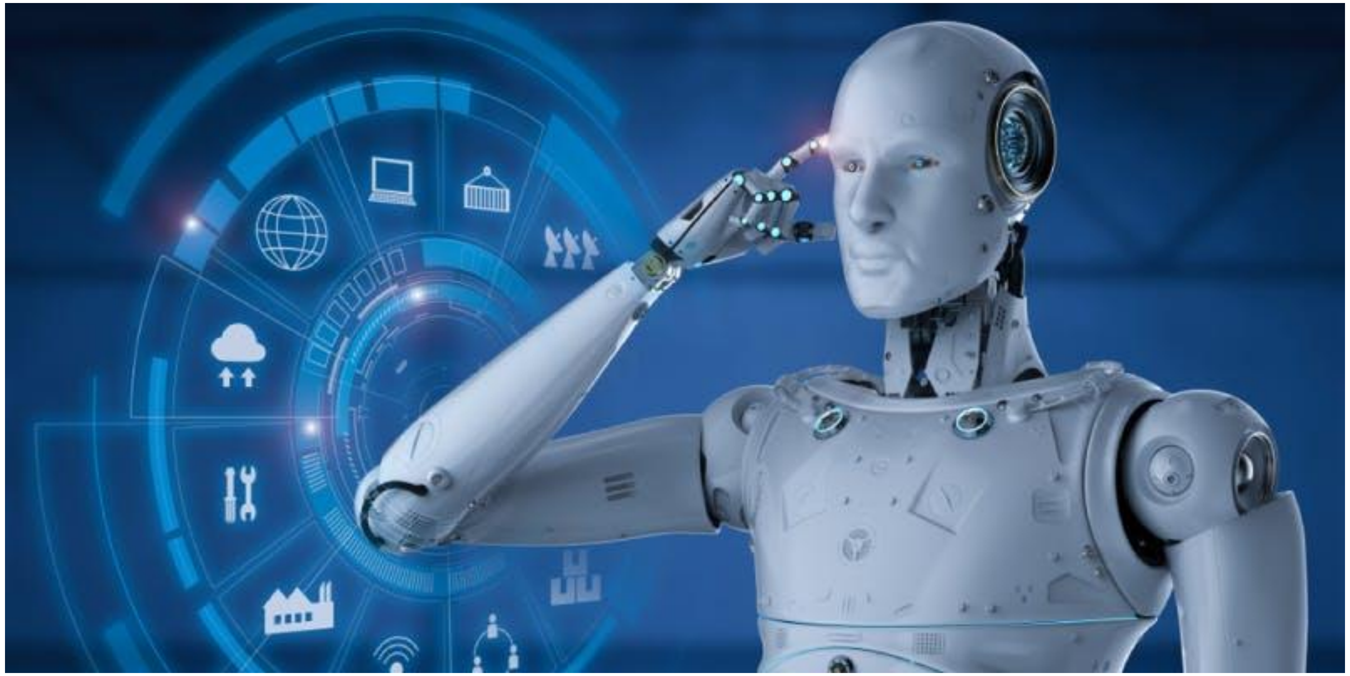
- How is a Machine Learning Model Created?



Identifies Features
(E.g., country of origination, time sent)
Learner - Algorithm
Parameters
(distilled learnings)
Input (E.g., Email data features as training data)
Output:
Model

AI & Machine Learning

- Emerging Issues
  - Algorithmic Discrimination
  - Privacy
  - Product Liability
  - Antitrust Algorithmic Collusion
  - Law Enforcement Access



AI & Machine Learning

- Product Liability
  - Example: Autonomous Vehicles – Would they save the lives of the drive and passengers while sacrificing pedestrians?
  - Trolley Stop Problem
  - Strict Liability
  - Design defect and duty to warn consumers

AI & Machine Learning

- Can a machine be negligent (or something more)?
  - What information was available to the computer for decision making?
  - What algorithm was used to assess risk of a given course of action?
  - Were the algorithms used to determine risk and take action reasonable?
  - Was the behavior of a third party or Plaintiff reasonably foreseeable?
  - What is the standard of care owed a Plaintiff by an algorithm?
  - The standard of care owed by the developer of the algorithm?

AI & Machine Learning

- Plaintiff Attorney: Kitt, why did you assume that it was safe to take that turn?
- Kitt (Defendant): 43 61 6e 20 79 6f 75 20 70 6c 65 61 73 65 20 61 73 6b 20 74 68 61 74 20 71 75 65 73 74 69 6f 6e 20 69 6e 20 53 51 4c 20 74 68 72 6f 75 67 68 20 6d 79 20 41 50 49 3f 3f
- Court Translator: Can you please ask that question in SQL via my API?
- Plaintiff expert enters a query into Kitt in Command Line mode.
- Kitt (via CLI): I don’t know. Why don’t you ask the guy who coded the algorithm?!

AI & Machine Learning; Privacy & Data

- Privacy
  - Do your public representations disclose how you will use data from Machine Learning?
  - Have you obtained consent?
  - Are you in compliance with regulatory requirements? (e.g. GDPR, PIPEDA, CCPA, Etc.)
- Data Rights
  - Ownership of AI & Machine Learning (and IoT) data is still uncharted legal territory. Many different data elements – Many different owners. Ownership varies by country (and by contract).
  - Design modular applications that work well in the absence of certain data elements, which may be restricted in certain countries.
  - Draft privacy policies and user agreements to grant necessary rights to use, host and manipulate the data.
  - Draft partnering and distributor agreements to ensure proper usage and access.

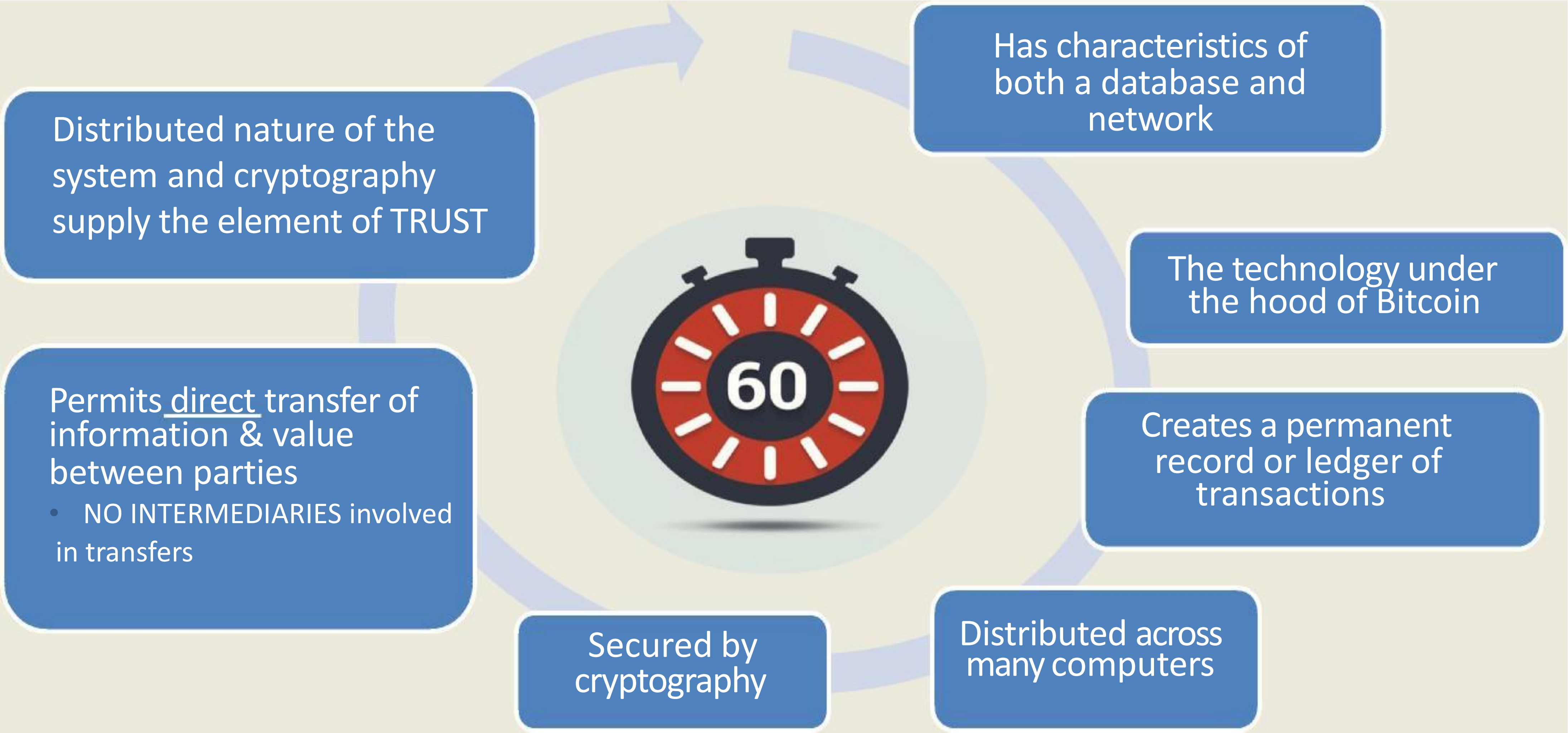
AI & Machine Learning; Privacy & Data

- Companies should analyze whether use of consumer data is compliant with regulatory requirements.
- FTC – Companies should consider whether they are violating any material promises to consumers or whether they have failed to discuss material information. All consumer data should be reasonably secured.
- HIPAA (by example) – Aggregation of PHI w/o patient authorization allowed for purpose of the covered entity improving healthcare operations.

AI & Machine Learning; FTC

- FTC Guidance (“Big Data: A Tool for Inclusion or Exclusion?” 2016)
  - Are the data sets missing information from particular populations and, if they are, take steps to address the problem.
  - Review the data sets to ensure that hidden biases are not having an unintended impact on certain populations.
  - Human oversight of data and algorithms when big data used to make important decisions (e.g. health, credit, employment)
  - Consider if fairness and ethical considerations advise against using big data.
  - Can you use big data in ways that advance opportunities for previously underrepresented populations.

Blockchains in Sixty Seconds



Distributed nature of the system and cryptography supply the element of TRUST

Has characteristics of both a database and network

The technology under the hood of Bitcoin

Creates a permanent record or ledger of transactions

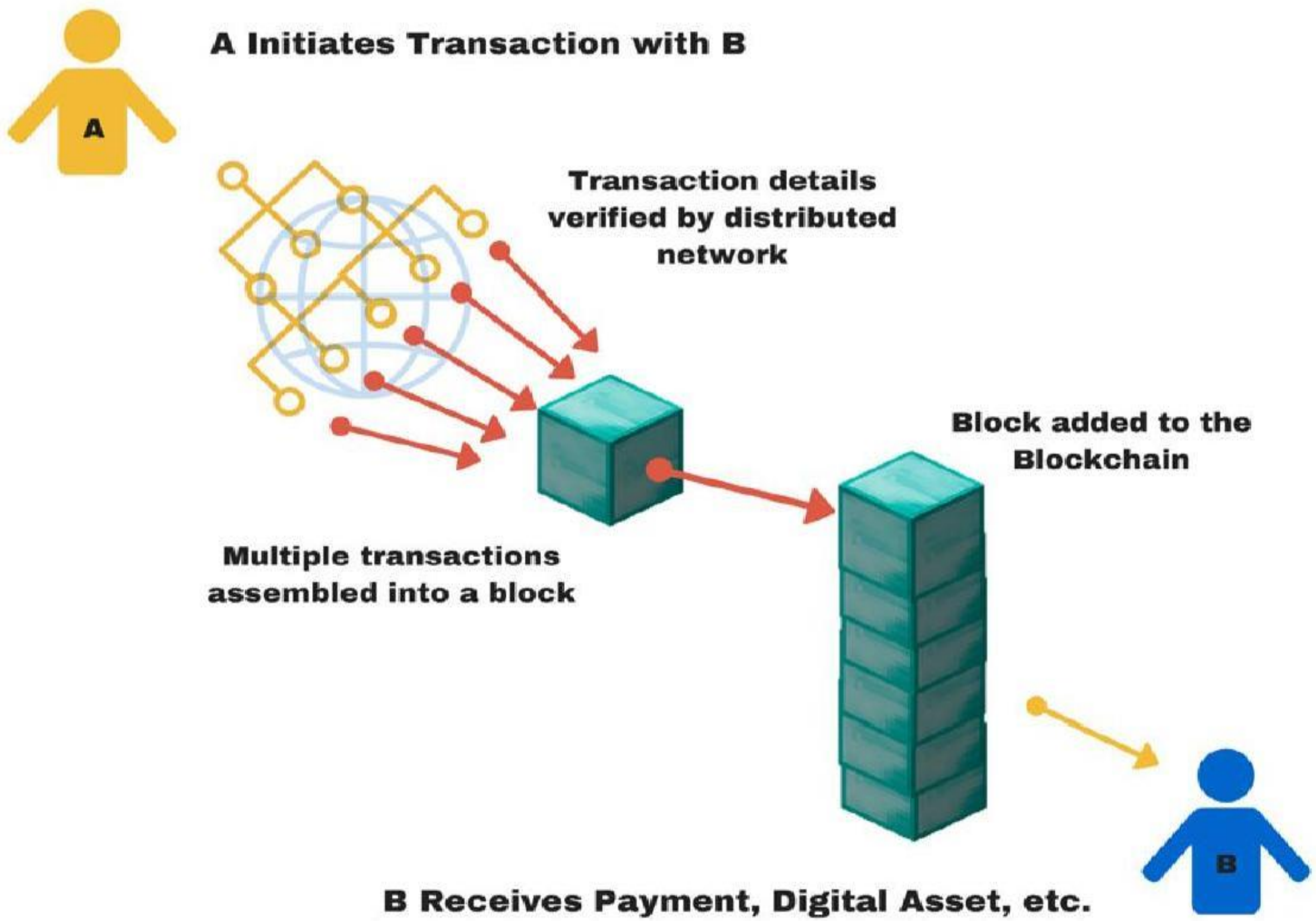
Distributed across many computers

Secured by cryptography

Permits direct transfer of information & value between parties

- NO INTERMEDIARIES involved in transfers

A Brief Peek at How a Blockchain Works



A Initiates Transaction with B

Transaction details verified by distributed network

Multiple transactions assembled into a block

Block added to the Blockchain

B Receives Payment, Digital Asset, etc.

Blockchain

Bitcoin has received the greatest media attention, HOWEVER, the underlying blockchain technology has the potential to revolutionize the way transactions are accomplished across industries. Examples include:

  - Logistics
  - Trading energy futures
  - Managing billing at electric vehicle charging stations
  - Social media by giving users ability to own and control their images and content

- Growing number of blockchain adopters experimenting with ways to increase scalability and scope. (Gartner projects that blockchain's business value-add will be $176B by 2025).

Blockchain

- Multiple issues have emerged that may inhibit the growth of blockchain initiatives.
  - No technical or process standards yet in place.
  - Market segmentation limits many companies from either adopting blockchain or collaborating with partners to promote widespread adoption.
- Expect to see more organizations adopt differing approaches to embrace blockchain:
  - Focus development resources on *use cases* with a clear path to commercialization.
  - Push for *standardization* in technology, business processes, and talent skillsets.
  - Work to *integrate and coordinate multiple blockchains* within a value chain

Legal Issues in Blockchain

- Regulation of bitcoin and other cryptocurrencies (securities, money, transfer laws, UCC, etc.).
- Ownership of digital assets.
- Cross-border implications.
- Legal effectiveness of smart contracts.
  - Application of existing law to new corporate forms
  - Liability/insurance for automated behavior
- Privacy and security issues

Regulatory Issues in Blockchain

- U.S. regulators monitoring the development of Blockchains
  - SEC - exploring potential applications in the public securities market.
  - Commodity Futures Trading Commission (CFTC) - is examining use of Blockchain and distributed ledger technology in the derivatives market.
  - Financial Crimes Enforcement Network (FinCEN) –
    - Administrative rulings and interpretive guidance regarding virtual currencies and blockchains
    - Issued a ruling that an online precious metals brokerage using Blockchain technology was subject to the regulator's money transmission regulations.
- Regulators will pay attention to the development and use of Blockchain technology in the regulated sector.

Regulatory Issues in Blockchain

- Effective governance is the key to the successful implementation of distributed ledger technology
  - Protect participants, investors and stakeholders while ensuring the system works despite systemic risk, privacy concerns and cybersecurity threats.
- Industry leaders should monitor applications to which blockchains are applied, particularly products and processes which may be abusive or may lead to unnecessary risk.
- Lower self-monitoring will lead to greater government regulation that may limit the application of Blockchain to future industries and markets.

Smart Contracts

- How do we define “smart contract”?
    - Complex transactional instructions built into code?
    - Legally enforceable contractual terms expressed in code?
    - New forms of automated transactions/value exchanges between parties (enforcement by code)?
- All of the above?

Smart Contracts

- Smart Code - Essentially just computer programs, but we use term “contract” because the programs can move value.
- When they reside on a Blockchain, they have these unique characteristics:
  - Transactional parameters that can be arranged by arms-length parties (i.e., across trust boundaries).
  - Program itself is stored on Blockchain, can control assets.
  - Once programmed, neither party can back-track – the code controls enforcement.
- BUT: Question as to whether enforceable under the law when something goes wrong (in many cases, value is long gone).
  - Fall back to typical contract law principles: Consideration, Offer, Acceptance, Mutual Assent?
  - If the terms are just the code itself, how do you even determine whether “something has gone wrong”?

Smart Contracts

- Code-based Legal Contracts
  - Essentially these are just contracts, but have these additional characteristics:
    - Code supplements the parties’ agreement (“call out” to specific code).
    - In some cases, code might supplant the underlying contract.
    - Ledger Labs would call this “smart legal contracts”.
  - Attorneys tend to mean these types of agreements when they talk about “smart contracts”.
  - Likely enforceable, so long as the underlying agreement demonstrates standard contract law principles.

Smart Contracts in Commerce & What’s Next

- Autonomous machine to machine transactions.
- May not matter if there is legal enforcement.
  - Code itself enforces compliance.
  - Parallel system to current legal systems.
- But what happens if something goes wrong? – The DAO is an example.
- What’s Next (at least in theory):
  - Attorneys will have to become much more comfortable with code.
  - Routine contract terms will become standardized so that they can be coded.
  - As more standardization occurs, some types of contract drafting now done by human lawyers may not be needed.

Emerging Technologies in the Financial Services Sector

- IoT generates Big Data YIELDING greater insights into consumers
    - Tailored experiences on demand
    - Treasure of data supports varied products
- AI used to develop/improve customer interface (e.g., chatbots, voice interfaces)
    - Risks of human error reduced
- Blockchain – tech-based transaction fuel efficiency and provide greater flexibility
- Smart Contracts reduce transaction processing times

Questions?

Geof Vickers, Partner

geof.vickers@nelsonmullins.com

Tori M. Silas, Partner

tori.silas@nelsonmullins.com