State of Blockchain Laws and Regulations in 2019

Speakers:

Daniel B. Garrie, Esq., Co-Founder, Law & Forensics; Mediator, Arbitrator, e-Discovery Special Master, JAMS

Kari Larsen, Partner, Perkins Coie LLC

Robert Levin, CEO, Emerging Star Capital LLC

(c) Global Cyber Institute 2019. All Rights Reserved.

Speakers



Daniel Garrie
Co-Founder, Law & Forensics;
Mediator, Arbitrator, e-Discovery
Special Master, JAMS



Kari Larsen
Partner, Perkins Coie LLC



Robert Levin
CEO, Emerging Star Capital LLC

(c) Global Cyber Institute 2019. All Rights Reserved.

Disclaimer

- This is not legal advice nor should it be considered legal advice
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients
- This presentation is offered for educational and informational uses only

(c) Global Cyber Institute 2019. All Rights Reserved.

Agenda

1. Introduction to Blockchain and Its Uses
2. Regulatory and Legal Landscape of Blockchain
3. Regulatory and Legal Landscape of Smart Contracts
4. General Multinational Considerations
5. Intellectual Property Considerations
6. Case Law

(c) Global Cyber Institute 2019. All Rights Reserved.



Introduction to Blockchain and Its Uses

(c) Global Cyber Institute 2019. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-SA



This Photo by Unknown Author is licensed under CC BY-NC-ND

What is Blockchain?

- Blockchain was invented in 2009 by a person (or group) known as Satoshi Nakamoto, with the intent to support Bitcoin.
- Blockchain is a distributed ledger technology that has emerged as a potential global solution to Multinational enterprises looking for consistency and integrity in the execution of international transactions.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

Blockchain and the Financial Industry

- Businesses and regulators are increasingly using blockchain to conduct and provide oversight of cross-border banking and finance activities.
- The visibility offered through blockchain is currently being used to track provenance and document financial transactions in multinational arrangements, ranging from supply chain to trade finance.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Safer Payment

- The authentication necessary to execute and record a transaction, and the irreversibility of a transaction once it is recorded in the blockchain, provides a secure and auditable record of each transaction, reducing the time, labor, and costs traditionally associated with manually verifying, reconciling, and settling international payment or money transfers

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Multi-Jurisdictional Supply Chain

- Traceability and control aspects are driving blockchain usage to multinational businesses, where members in the supply chain are involved across multiple jurisdictions, because blockchains supply a digital passport for every transaction.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Smart Contracts and Blockchain

- A smart contract program irreversibly automates performance of the parties' obligations based on the fulfillment of a condition or set of conditions defined in the program.
- A legal contract can be made "smart" either entirely or in part, through use of smart contract programs using blockchain technology.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Example: Insurance Purchases Using Smart Contracts and Blockchain

- When purchasing insurance for global exposure there are various actions required at the global and local level before any policies can be validly issued, i.e. Cash before cover, anti-money laundering (AML), and mandatory reinsurance retentions.
- With blockchain, many of the steps can be automated through use of a smart contract that executes based on the terms of the parties' agreement(s)."

(c) Global Cyber Institute 2019. All Rights Reserved.



Regulatory and Legal Landscape of Blockchain

(c) Global Cyber Institute 2019. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-SA-NC


This Photo by Unknown Author is licensed under CC BY-ND

Blockchain in the U.S.

- The regulatory regime in place by the Federal government, is tied to the activity on or by the blockchain and that can be regulated by both state and federal agencies depending upon the activity.
- Various U.S. agencies have been active in addressing virtual currency and the potential regulatory ramifications. FinCEN issued guidance in 2013 clarifying that its money transmitter definition applies to transactions involving virtual currency, and recently issued supplemental guidance providing further information on the requirements of virtual currency business. The CFTC has approved exchanges, clearinghouses focused on virtual currency, and various exchanges have certified virtual currency products for trading.

(c) Global Cyber Institute 2019. All Rights Reserved.

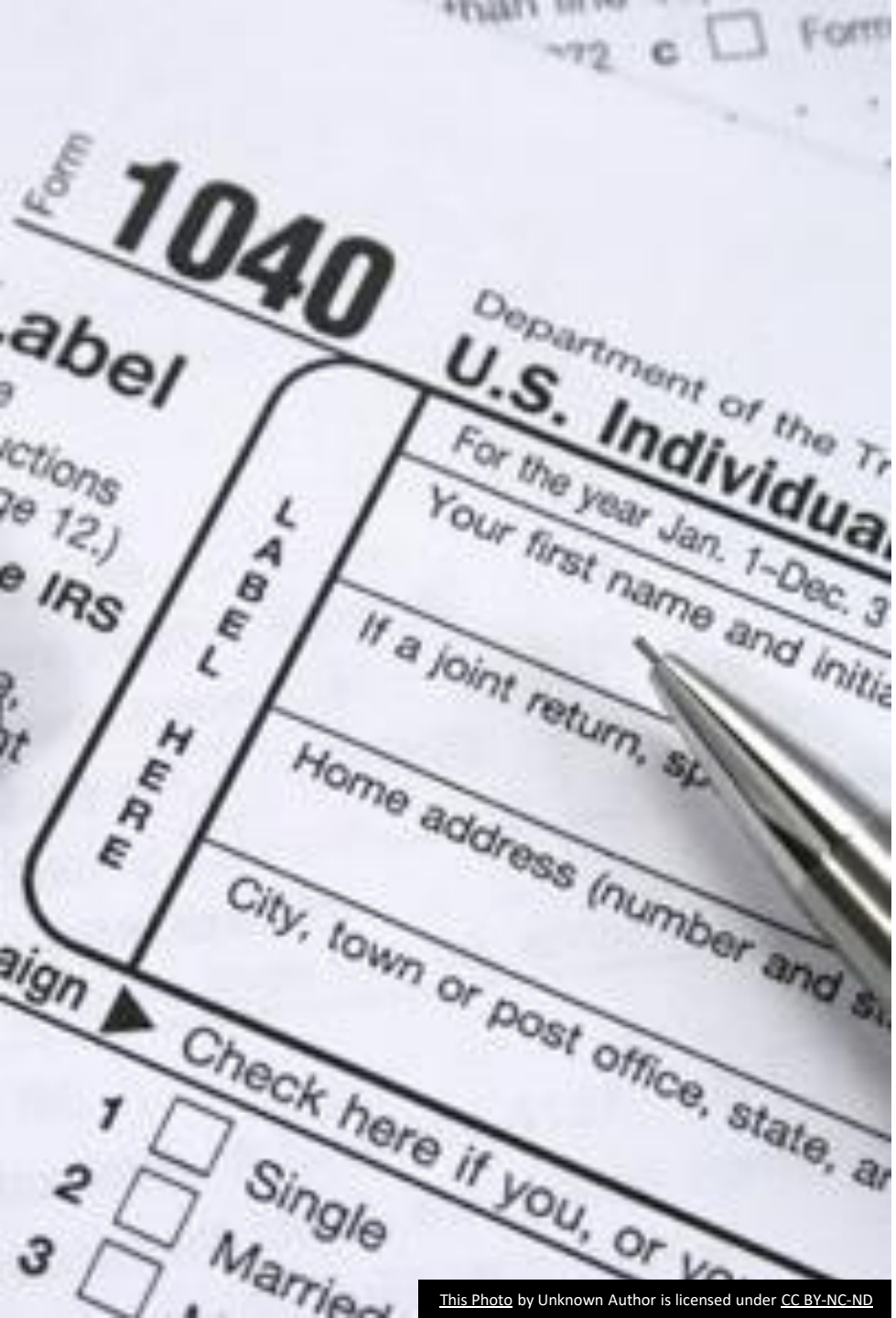


This Photo by Unknown Author is licensed under CC BY

Blockchain in the U.S.

- The ownership and sale of cryptocurrency and other digital assets are subject to a complex patchwork of federal and state laws. Some significant areas of the law include:
  - Taxation
  - Securities
  - Commodities
  - Anti-money laundering
  - State money transmitter regulation

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

Taxation

- Beware that federal income taxes are owed on any realized gains in the value of cryptocurrency on the following events:
  - The sale of cryptocurrency for cash
  - The purchase of goods and services with cryptocurrency
  - The exchange of one cryptocurrency for another cryptocurrency
- Ordinary income tax is also owed for the “fair market value” of any cryptocurrency that has been mined by the taxpayer.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Securities

- The Securities and Exchange Commission (SEC) has regulatory authority over the issuance or resale of any token or cryptocurrency that has the characteristics of an “investment contract.”
- An “investment contract” has been defined by the Supreme Court as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial of managerial effort of others.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Commodities

- On September 17, 2015, the U.S. Commodity Futures Trading Commission (CFTC) ruled that "virtual currencies" are commodities subject to CFTC regulation.
- The Commodity Exchange Act (CEA) provides the CFTC with civil enforcement authority to investigate and prosecute alleged violations of the Commodity Exchange Act and Commission regulations, including fraud and manipulation in both cryptocurrency derivatives markets as well as in cryptocurrency spot markets.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

Anti-Money Laundering

- Under the Bank Secrecy Act (BSA), a money services business (MSB) is subject to the federal anti-money laundering regulations of the Financial Crimes Enforcement Network (FinCEN).
- In 2013, FinCEN issued Guidance that an "administrator or exchanger of convertible virtual currency is a 'money transmitter' for BSA purposes, and thus is subject to MSB compliance and registration as well as oversight by FinCEN."
- In addition, the Internal Revenue Service has the authority to examine MSBs with respect to their compliance with FinCEN's anti-money laundering regulations. A "money transmitter" is a type of MSB that is regulated by FinCEN.

(c) Global Cyber Institute 2019. All Rights Reserved.



State Money Transmitter Regulation

- State money transmission licenses, generally aimed at consumer protection for services like PayPal or Western Union, regulate: (i) transmitting money, (ii) issuing or selling payment instruments, and/or (iii) issuing or selling stored value. A number of states have extended these activities to encompass blockchain-based virtual currency.
- Acquiring money transmission licenses involves the following, depending on the state: (i) application fees up to $10k/state, (ii) net worth or capitalization requirements ranging from several thousand to a million or more, (iii) surety bond coverage ranging from $10k to several million, and (iv) ongoing reporting, examinations, and renewal fees associated with maintaining the license.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Blockchain in Commerce – U.S.

- Several U.S. states have enacted or proposed legislation validating the use of blockchain technology in commerce.
- States include:
  - Vermont - Blockchain to be considered a regularly conducted business activity establishing a presumption that the information in blockchain is correct.
  - Nevada – Recognizes blockchain as a form of electronic records satisfying the requirement for a written record in city and county government.
  - Delaware – Authorizing registration of shares of Delaware companies in blockchain form.
  - Wyoming – 13 laws total as of 2019 (see following slide)

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC

Wyoming

- With 13 laws total, Wyoming is the only US state to provide a comprehensive legal framework that enables blockchain technology to flourish, both for individuals and companies.
- Recognizes direct property rights for individual owners of digital assets of all types (virtual currencies, digital securities and utility tokens) and applies the super-negotiability rules of commercial law to virtual currencies—which foster their liquidity—by applying the very same rules that apply to money.
- Creates a fintech sandbox to provide regulatory relief to financial innovators from existing laws for up to 3 years. It's broadly reciprocal with fintech sandboxes both in the US and globally.
- Authorizes a new type of state-chartered depository institution to provide basic banking services to blockchain and other businesses. The bank is required to have 100% reserves, cannot lend, is for business depositors only, and FDIC insurance is optional. Such banks could be operating as soon as March 31, 2020.
- Authorizes the first "qualified custodian" regulatory model designed specifically with digital assets in mind by creating a special type of bank under state law. Wyoming banks can start such operations as soon as fall of 2019.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

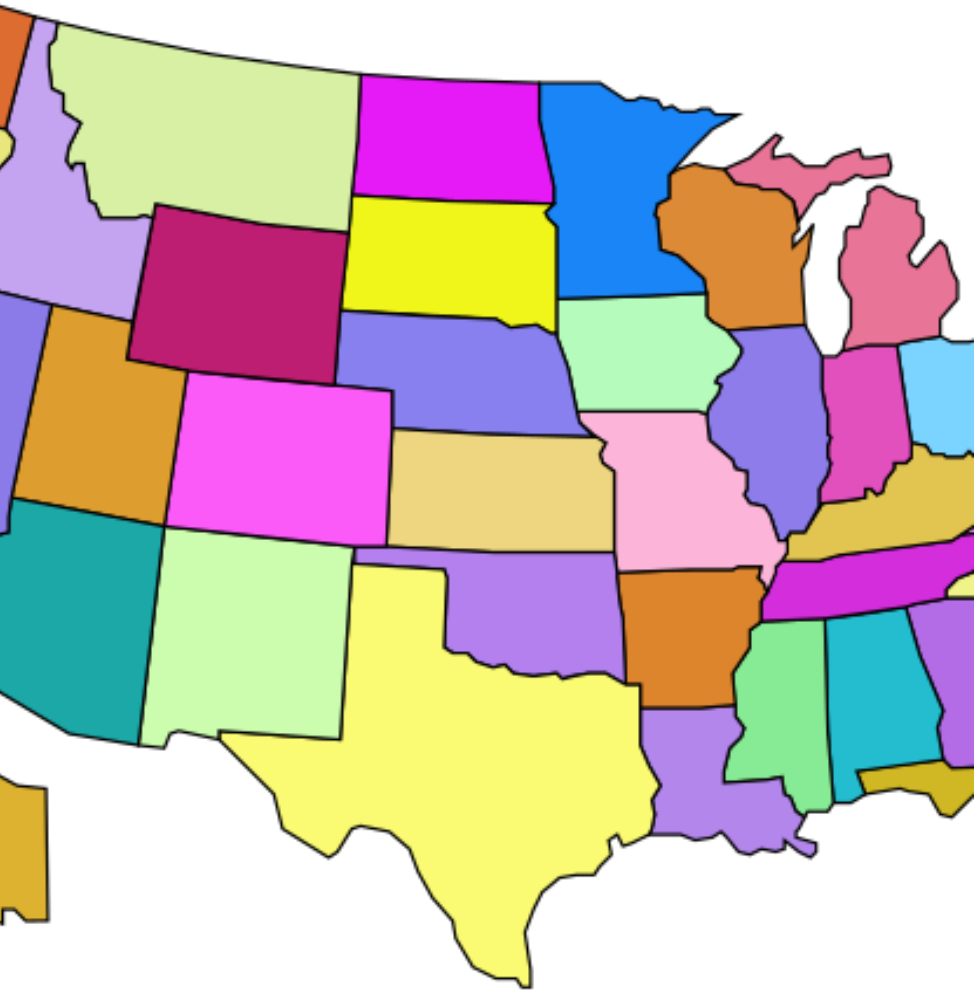
Blockchain in Commerce – Global

- Australia is currently implementing a blockchain-powered securities exchange.
- In 2017 Japan's Ministry of Internal Affairs and Communications announced a blockchain/smart contract solution that would allow companies to interact with the government.
- The Monetary Authority of Singapore, in collaboration with a consortium of banks launched "Project Ubin".
- The European Commission announced the launch of #BlockChain4EU in 2017.

(c) Global Cyber Institute 2019. All Rights Reserved.



Regulatory and Legal Landscape of Smart Contracts



Legal Enforceability – U.S

- There is a spectrum of architectural models through which the transactional aspects of legal contracts can be made “smart”.
- Ranging from replicating aspects of legally binding off-chain “natural language” transactions to coding legal transactions that fully exist as smart contract programs.
- Various commentators have surveyed existing law in numerous jurisdictions and concluded that it forms a basis for providing legal effect to smart contracts.

(c) Global Cyber Institute 2019. All Rights Reserved.



State Legislation

- Arizona passed legislation prohibiting denial of legal effect or enforceability of a contract solely because the contract contains a smart contract term.
  - The Arizona legislation specifically defines the terms "blockchain technology" and "smart contract" and recognizes that smart contracts may exist in commerce.
- Nebraska and Tennessee have proposed similar legislation.

(c) Global Cyber Institute 2019. All Rights Reserved.

Factors to Consider in Electronic Contracting



This Photo by Unknown Author is licensed under CC BY

- In an analysis done by Norton Rose and R3, it was observed in US law that considerations should be given to:
  - How the parties will give assent to the terms of the smart contract,
  - What steps should be followed to ensure the parties have proper notice of the contract terms, and
  - What must be done to bind the party to a contract that is executed electronically.
- If these factors are considered and addressed courts in the U.S. would be willing to support automatic contracting.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-ND

Legal Enforceability Abroad

- Most countries appear to be willing to enforce formation of contract by electronic means so long as the usual rules of contract formation apply.

(c) Global Cyber Institute 2019. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY

Choice of Law Questions

- Questions of which law will govern, and which jurisdiction will apply in multinational smart contracts that are silent on governing law and jurisdiction and where performance is replicated across a distributed ecosystem spanning multiple countries often need to be addressed.
- Will tort concepts apply to contract interpretation?
- What systems can be put into effect to remedy an irreversible result wrongfully or erroneously achieved?

(c) Global Cyber Institute 2019. All Rights Reserved.



General Multinational Considerations

al Cyber Institute 2019. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-NC



This Photo by Unknown Author is licensed under CC BY-SA-NC

Blockchain Globally

- With blockchain use cases and applications expanding in scope and number, regulators around the world, including the US, Canada, Switzerland, the UK, China, Japan, Singapore, and Australia, have expressed interest in regulating blockchain to protect consumer and the market from fraud and other illegal conduct.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Blockchain Technology and Smart Contracts

- As data is implicated in all blockchains and smart contracts, we should consider what information is being processed, how it is used, who is accessing it, and where it is being stored and transmitted.
- The privacy of personally identifiable information (PII)is a concern in all regions, particularly with respect to certain types of consumer data and sensitive information.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

What is Personally Identifiable Information?

- PII generally consists of information that can be used to identify, or is information about, a natural person.
- Laws vary by jurisdiction.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Privacy Laws Governing Personally Identifiable Information

- Privacy laws govern
  - What can be collected
  - How the PII can be used
  - The security and integrity of the PII
  - If and how the PII can be transferred between entities and jurisdictions
  - When an individual's personal data must be deleted

(c) Global Cyber Institute 2019. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-ND

Personally Identifiable Information Globally

- In the United States laws governing PII generally focus on health and financial information.
- In the EU regulations treat race and ethnicity, political and religious beliefs, genetics and biometrics, health, and sexual orientation as special information.

(c) Global Cyber Institute 2019. All Rights Reserved.



Intellectual Property Considerations

(c) Global Cyber Institute 2019. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-SA



This Photo by Unknown Author is licensed under CC BY-SA

Ownership

- Ownership and licensing of both newly created and pre-existing materials should be addressed up front.
- The parties to the ecosystem should consider whether the newly created work should be solely owned (and if so by whom) or jointly owned, in which case the parties will need to determine how they act as joint owners.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

Indemnification

- The parties should also consider expressly stating what licenses and intellectual property infringement indemnification will be provided to each party, and whether there will be any periods of exclusivity or other competitive advantage.
- The intellectual property rights and protections should reflect the jurisdictions covered by the transactions encompassed by the ecosystem.

(c) Global Cyber Institute 2019. All Rights Reserved.

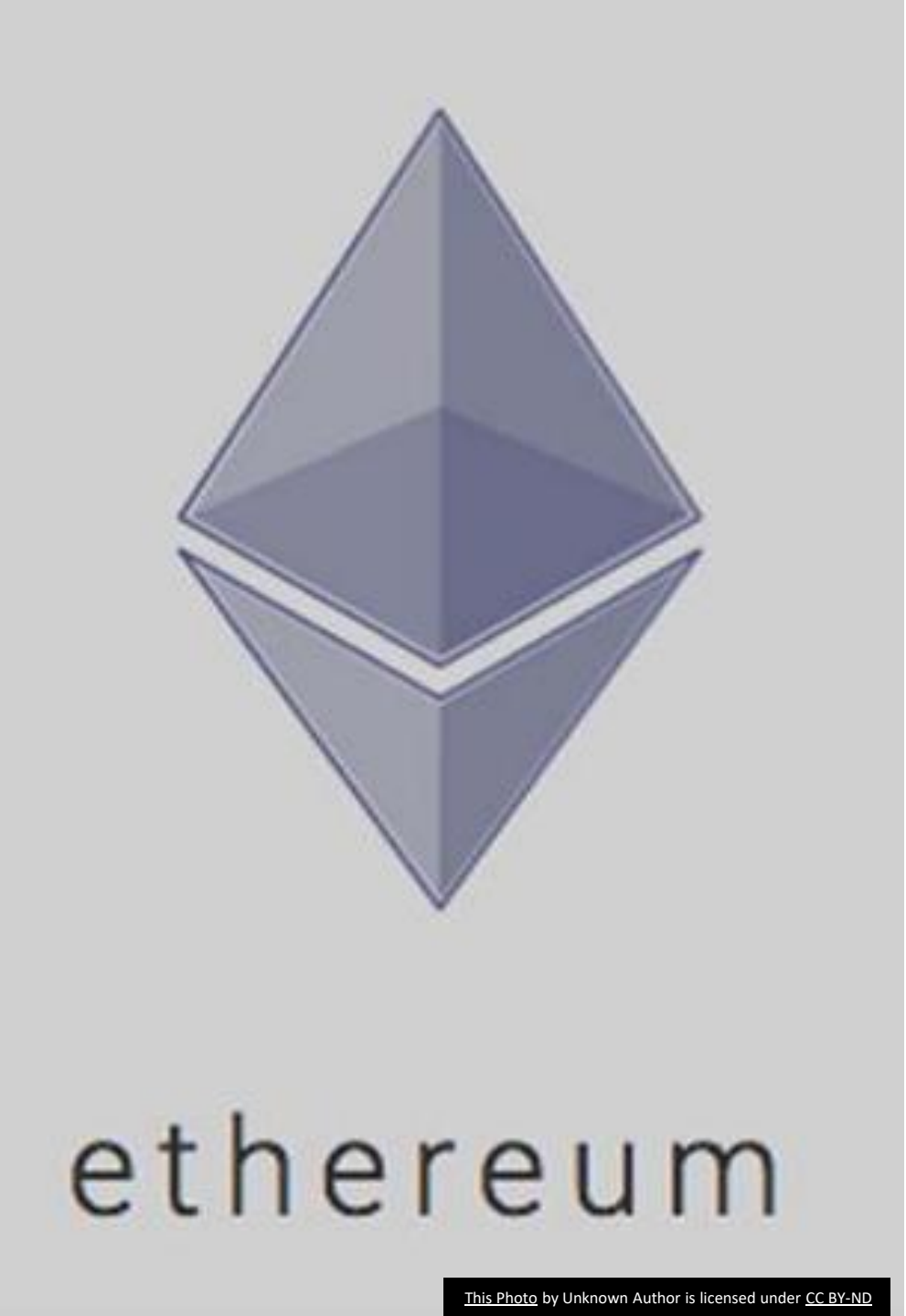


This Photo by Unknown Author is licensed under CC BY-SA

Beta Testing

- Parties who participate in beta testing of blockchain products may be asked to provide the consortium or vendor developing the product with ownership or a broad license to any feedback or suggestions provided by the testing participant.
- The testing participant may wish to consider whether retaining ownership of its feedback and suggestions is necessary in this context and carefully monitor what information it provides to ensure protection of any trade secret or other confidential information.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-ND

Copyleft Licenses

- Since most blockchain technologies are open source, certain technologies including applications in Ethereum, are subject to “viral” or so-called “copyleft” licenses.
- When software may be used by, modified, or distributed freely on condition that anything derived from it is bound by the same condition
- An example is the General Public License (GNU), where code linked to the copy-lefted code is then made subject to the copyleft license.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC

Blockchain Intellectual Property Council

- The Chamber of Digital Commerce created the Blockchain Intellectual Property Council to promote innovation in blockchain by addressing intellectual property rights issues, including combating the proliferation of patent troll in this space.
- The council has provided blockchain-specific patent information and is focused on implementing various intellectual property protection models.

(c) Global Cyber Institute 2019. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA-NC

Intellectual Property Protection Models

- Non-aggression agreements
  - where industry players agree not to assert patents against each other
- Developing patent pools
  - Where cross-licensing options are available to all pool participants
- Reducing inventory approach
  - Under which subscribing groups require members to agree not to sell patents without first granting a license to all group members

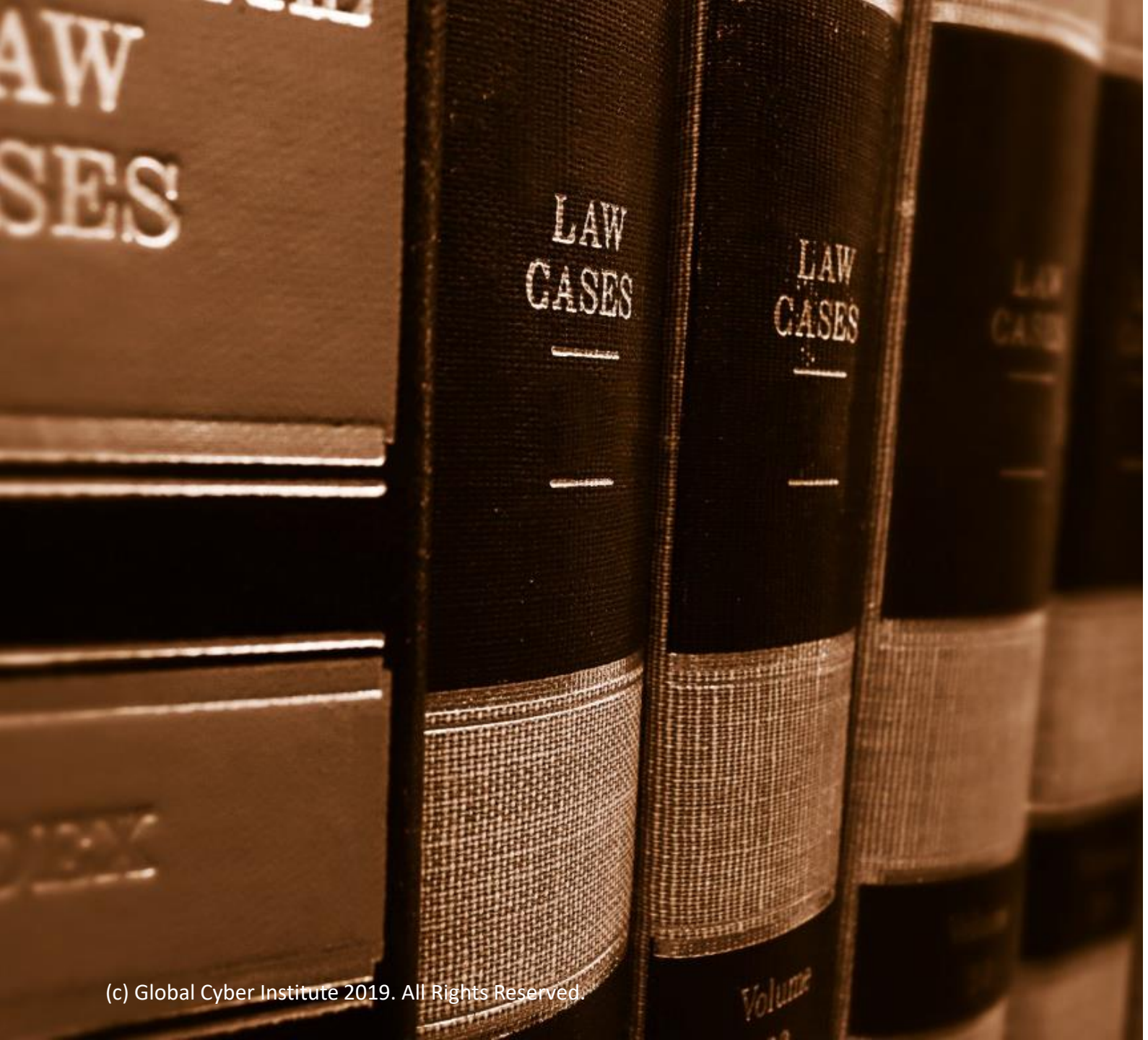
(c) Global Cyber Institute 2019. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-ND

Global Blockchain Initiative

- The Association of Corporate Counsel has launched a global Blockchain Initiative, which will offer programming and tools to assist in-house practitioners with the wide variety of legal issues arising from the use of blockchain and smart contracts

(c) Global Cyber Institute 2019. All Rights Reserved.



Case Law

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

In the Matter of Tomahawk Exploration LLC and David Thompson Laurance, Securities

- Facts: On August 14, 2018, the U.S. Securities and Exchange Commission (SEC) issued an order against Tomahawk Exploration LLC (Tomahawk) and its principal, David Thompson Laurance, regarding an ICO for Tomahawkcoins that Tomahawk engaged in during mid-2017.
  - An initial coin offering (ICO) is a type of funding using cryptocurrencies. Mostly the process is done by crowdfunding but private ICOs are becoming more common.
- The SEC accepted Tomahawk's settlement offer, and in the Order, the SEC found that the virtual tokens being offered by Tomahawk were securities under the *Howey* test. While the part of the Order discussing unregistered sale of securities, fraud and misrepresentations to investors is rather obvious, the Order also discussed additional issues that significantly affect token sales worldwide. According to the SEC:
  - ICO bounty programs involve the sale of securities; and
  - Tokens can be treated as equity securities and considered "penny stock.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

Commodity Futures Trading Commission v. Gelfman Blueprint, Inc., and Nicolas Gelfman

- Facts: In September 2017, the CFTC filed a complaint against Gelfman Blueprint, Inc. and its CEO Nicholas Gelfman for operating a bitcoin Ponzi scheme. According to the Complaint, the Defendants used falsified performance reports and promises of significant payouts to solicit more than $600,000 from 80 customers between 2014 and 2016.
- Penalty: In October 2018, a judge order Gelfman and Gelfman Blueprint, Inc. to pay a combined total of over $2.5 million in fines and restitution. In addition an injunction was placed on Gelfman that permanently bars him from trading.

(c) Global Cyber Institute 2019. All Rights Reserved.



Questions?

(c) Global Cyber Institute 2019. All Rights Reserved.

Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
Phone: 855-529-2466
URL: www.lawandforensics.com



Kari Larsen
Email: KLarsen@perkinscoie.com
Phone: (212) 261-6866
URL: https://www.perkinscoie.com



Robert Levin
Email: robert@emergingstarcapital.com
URL: http://www.emergingstarcapital.com/

(c) Global Cyber Institute 2019. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Executive Managing Partner
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529-2466
M: (206) 228-5457
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
Computer Forensics, E-Discovery, Cyber Security

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States. In particular, Daniel recently located and recovered deleted files in both private and public cloud computing environments using his patented software, Forensic Scan. This investigation took less than forty-eight hours to clean and recover the data from the servers of a cloud-hosting provider that was compromised by a malicious cyber-attack. Thanks to the Forensic Scan technology, that Daniel co-invented and patented (US9990498B2 and US9990497B2), and his own expertise, Daniel and his team was able to identify the source of the breach and remediate the problem in record time.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases, including one involving the embezzlement of millions of dollars from a large non-profit. Daniel was able to perform a thorough analysis of the alleged embezzlers' phone and computer, despite the embezzlers' attempts to wipe them, and identify concrete evidence of the embezzlement to a jury. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes. Some of the major cases for which he has served as an e-discovery special master, or forensic neutral include: *Hougan vs. City of Newport Beach, No. 30-2012-00582855* (Super. Ct. Cal. 2014)*; Small v. University Medical Center of Southern Nevada, 2014 WL 4079507*(D. Nev. 2014)*; C.D.S. Inc. v. Zelter and Amazon Web Services, Inc.*, (S.D.N.Y. 2016); *Jawbone, Inc. v. Fitbit Inc.* et al (Super. Cal., S.F. County 2018). In addition to his vast litigious experience, Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) Global Cyber Institute 2019. All Rights Reserved.



Kari Larsen
Perkins Coie LLP – Partner
Contact:
W: (212) 261-6866
E: KLarsen@perkinscoie.com
URL: https://www.perkinscoie.com

PERKINSCOIE
COUNSEL TO GREAT COMPANIES

Kari Larsen represents clients in U.S. and EU regulatory, legislative, risk management, compliance and internal control matters related to innovative technologies, such as digital assets and cryptocurrencies, and exchange-traded and over-the-counter commodities and derivatives markets.

Kari has direct experience working at the first U.S. based, banked and regulated digital currency derivatives exchange and clearing organization in the role of general counsel and regulatory advisor, where she managed all aspects of the legal, regulatory, governmental affairs, risk management and compliance functions of the exchange. She also served as general counsel at the world's second largest environmental futures exchange.
As part of her blockchain practice, Kari counsels clients on business and usage strategies, drafts and negotiates third party agreements, advises on potential regulatory requirements and liaises with government agencies. Her blockchain clients range from platforms that are in the funds, payments and money transmitters, trading, investments and exchange spaces. She also advises fintech and digital business clients on federal and state regulatory and compliance matters, including privacy, data security and cybersecurity, information governance, anti-money laundering, Bank Secrecy Act and Know-Your-Customer matters, vendor management and consumer protection.

Drawing on her two decades of experience, Kari advises clients on domestic and cross-border finance, commodity and derivatives trading regulatory and compliance requirements, and commodity trading compliance programs, with specific experience on the potential application of governmental requirements to innovative financial instruments. She assists clients in their interactions with the U.S. Commodity Futures Trading Commission (CFTC) and has a thorough understanding of the Commodity Exchange Act (CEA).

(c) Global Cyber Institute 2019. All Rights Reserved.



Robert Levin
Emerging Star Capital, LLC – CEO
Contact:
E: robert@emergingstarcapital.com
URL: http://www.emergingstarcapital.com/

Robert is an inventor, mobile & digital health expert, serial entrepreneur, and author. He is currently the CEO of Transclick, a real-time translation service with over 14 million digital client downloads. He has over 25 years of senior level Wall Street & Technology experience, and has raised $150 million for funds and technology companies.

Robert has expertise in applying innovation in machine learning (AI) to finance and other enterprise verticals, macro-economics applied to global asset allocation, alternative beta strategies, hedging portfolio risk, as well as private equity/VC in emerging technologies including cybersecurity, Blockchain and artificial intelligence.

He is an inventor, best-selling author, public speaker and holds one issued US patent. He is also a strategist in global macro, emerging markets and technology investments. He was trained at Salomon Brothers and was a top strategist for 2 hedge funds, reporting to Paul Tudor Jones at Tudor and Louis Bacon at Moore Global.

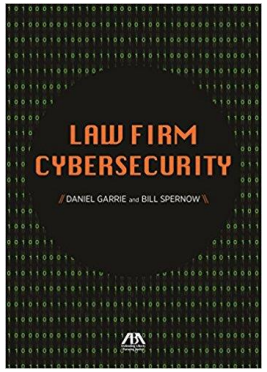
Robert is a Tech Laureate of the Tech Museum of Innovation and has won the Gold Edison Award for Innovation in mobile apps, is a member of the AlwaysOn Mobile 100 (top 100 mobile companies) and the AlwaysOn Global 250.

He is a thought leader in global innovation, and the author of the first biography of President Bill Clinton, Bill Clinton: The Inside Story, and Democratic Blueprints: National Leaders Chart America's Future.

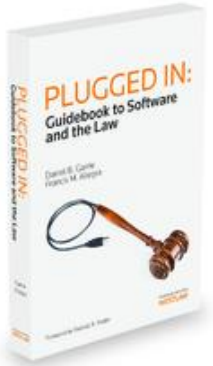
(c) Global Cyber Institute 2019. All Rights Reserved.

Additional Reading

Books



Law Firm Cybersecurity



Plugged In: Guidebook to Software and the Law



Software and the Law: Digital Forensic Investigations and E-Discovery



Dispute Resolution and e-Discovery

Articles



The Wider Implications of the California Consumer Privacy Act



'Act Of War' Questions In Cyberattack Insurance Case



Arbitrating Cyber Coverage Disputes

(c) Global Cyber Institute 2019. All Rights Reserved.