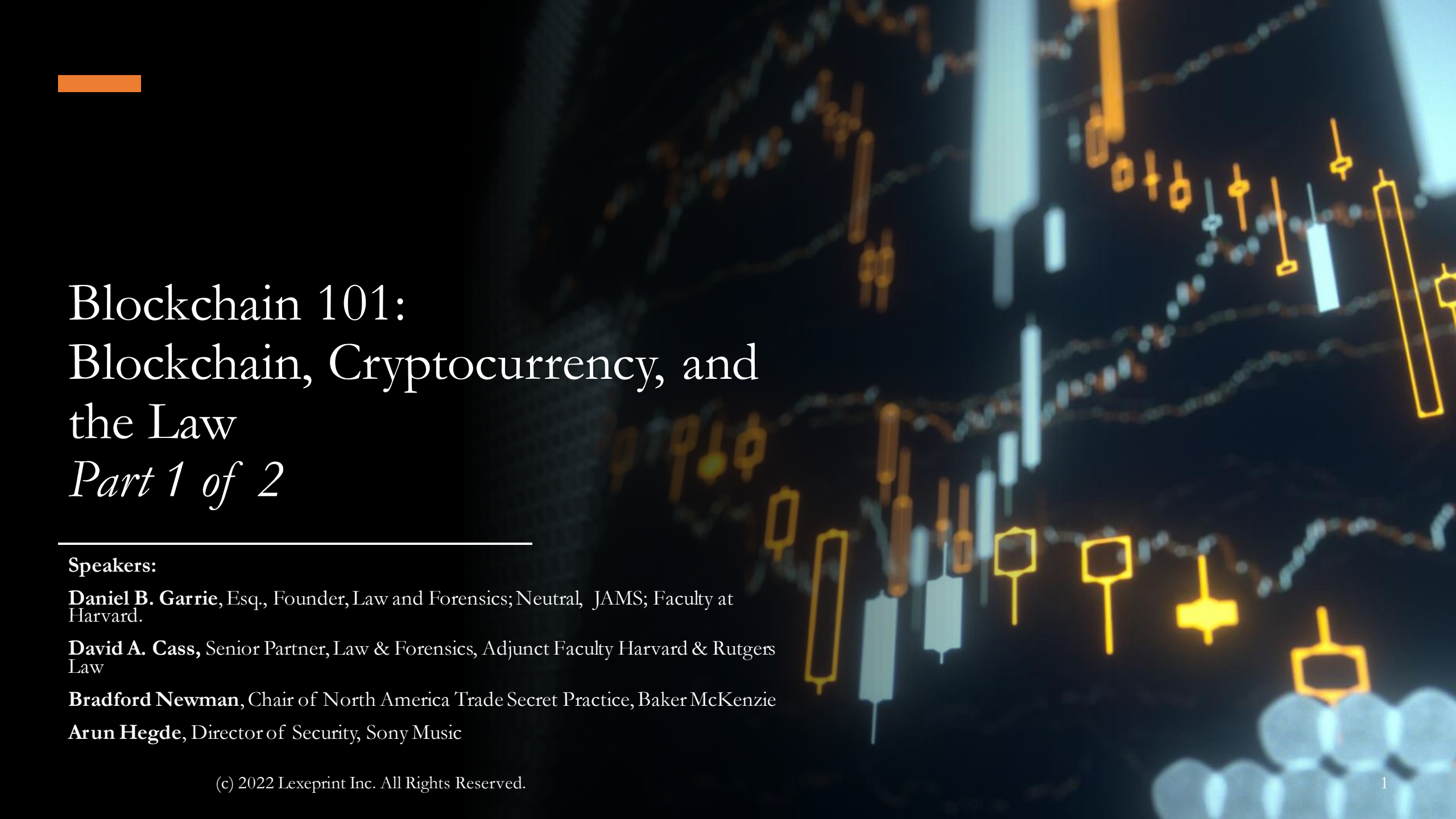


Blockchain 101: Blockchain, Cryptocurrency, and the Law

Part 1 of 2

Speakers:

Daniel B. Garrie, Esq., Founder, Law and Forensics; Neutral, JAMS; Faculty at Harvard.

David A. Cass, Senior Partner, Law & Forensics, Adjunct Faculty Harvard & Rutgers Law

Bradford Newman, Chair of North America Trade Secret Practice, Baker McKenzie

Arun Hegde, Director of Security, Sony Music

(c) 2022 Lexeprint Inc. 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) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Founder, Law and Forensics
Neutral, JAMS
Faculty, Harvard



David A. Cass
Senior Partner
Law & Forensics
Adjunct Faculty Harvard &
Rutgers Law

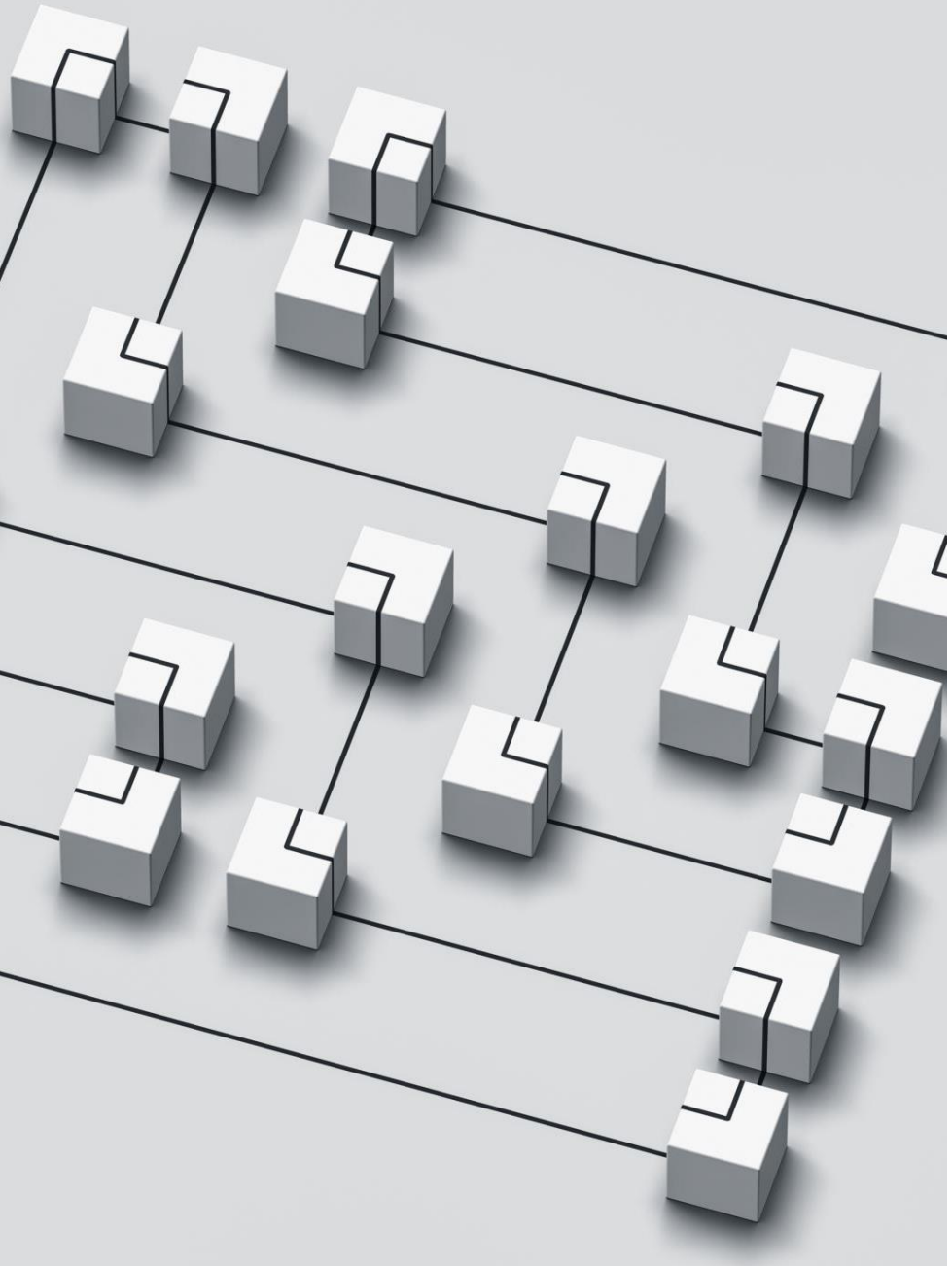


Bradford Newman
Chair of North America
Trade Secret Practice –
Baker McKenzie



Arun Hegde
Director of Security
Sony Music

(c) 2022 Lexeprint Inc. All Rights Reserved.



Agenda

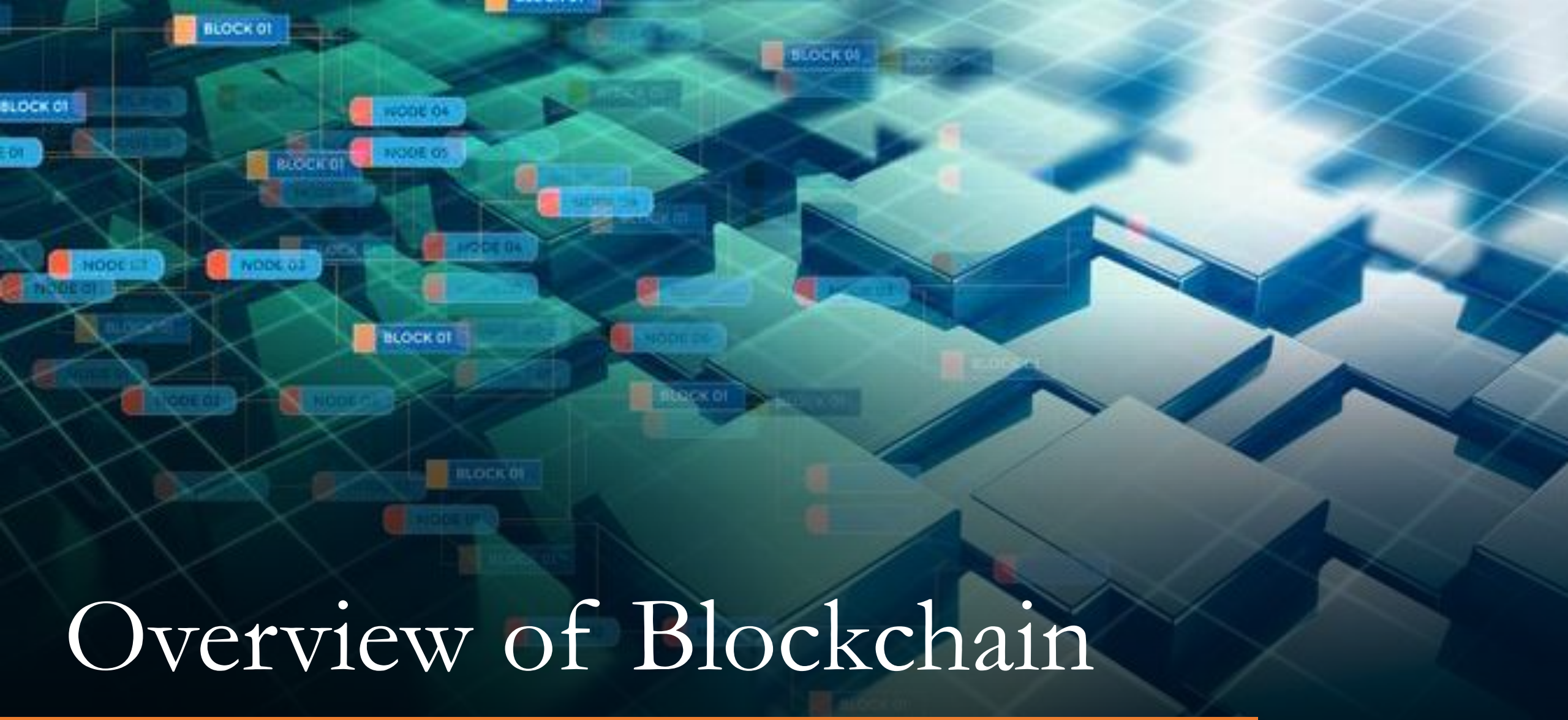
Part 1:

- Overview of Blockchain
- How Does Blockchain Work?
- What Makes Blockchain Unique?

Part 2:

- What is the Relationship Between Blockchain and Cryptocurrency?
- Current State of the Law and Regulations for Blockchain
- Recent Cases

(c) 2022 Lexeprint Inc. All Rights Reserved.



Overview of Blockchain

(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY



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

Introduction to Blockchain

- Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government).
- At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network, no transaction can be changed once published.

(c) 2022 Lexeprint Inc. All Rights Reserved.



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

What is Blockchain?

- In its simplest form, Blockchain is a data structure on which transactional data which are highly resistant to modification may be stored.
- As a data structure, a blockchain is a form of distributed ledger technology that enables data sharing across a network of individual computers.
- The main appeal to blockchain technology is twofold:
  - all data and transactions that are on the blockchain are nearly impossible to modify or hack
  - the data itself is transparent.

(c) 2022 Lexeprint Inc. All Rights Reserved.



History of Blockchain

- In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority.
- The first such blockchain based cryptocurrency was Bitcoin.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Real-World Uses

- Payment Processing and Money Transfers
- Monitor Supply Chains
- Retail Rewards Programs
- Digital IDs
- Data Sharing
- Copyright and Royalty Protection
- Digital Voting
- Immutable Data Backup
- Tax Regulation and Compliance
- Medical Record Keeping
- Weapons Tracking
- Equity Trading
- Managing IoT Networks
- Expediting Energy Futures Trading and Compliance
- Securing Access to Belongings
- Tracking Prescription Drugs

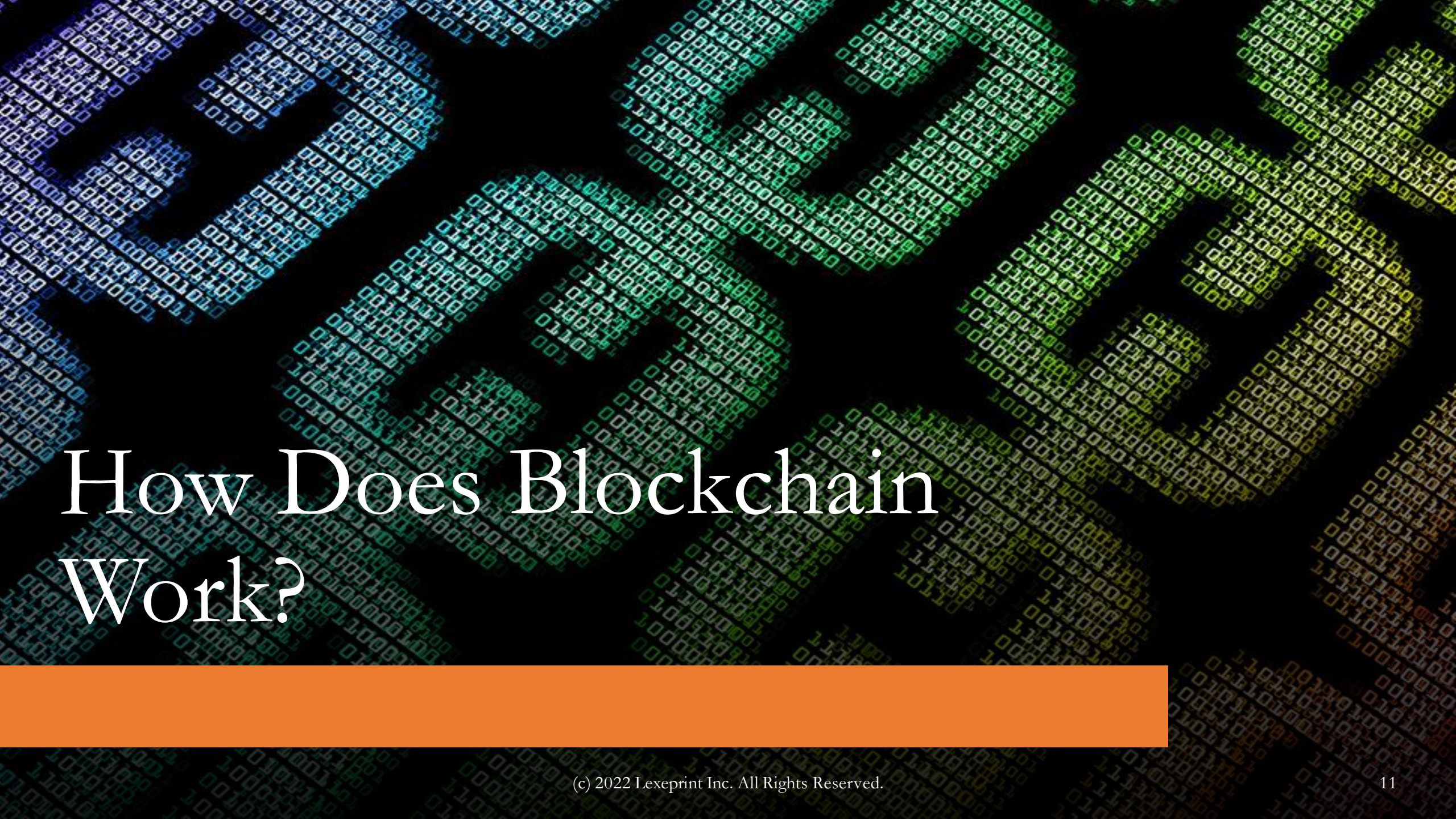
(c) 2022 Lexeprint Inc. All Rights Reserved.



Examples of Blockchain uses in the Legal Industry

- Smart contracts
- Chain of custody
- Intellectual property
- Litigation and settlements

(c) 2022 Lexeprint Inc. All Rights Reserved.



How Does Blockchain Work?

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

How Blockchain Works

- A Blockchain is a type of diary or spreadsheet containing information about transactions.
- An individual block in a blockchain contains the following elements:
  - Block number
  - Data stored in the block
  - Hash of the previous block
  - Hash of the current block

(c) 2022 Lexeprint Inc. All Rights Reserved.

How Blockchain Works

Blockchain Process Steps



P2P Network ⇨ **Communication** ⇨ **Validation** ⇨ **Verification** ⇨ **Confirmation**

1

Someone in the Peer to Peer network requests a transaction.

2

The requested transaction is broadcast to the P2P network consisting of computers, known as nodes.

3

The network of nodes validates the transaction and the users status using algorithms.

A verified transaction can involve cryptocurrency, contracts, records or other information.

4

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

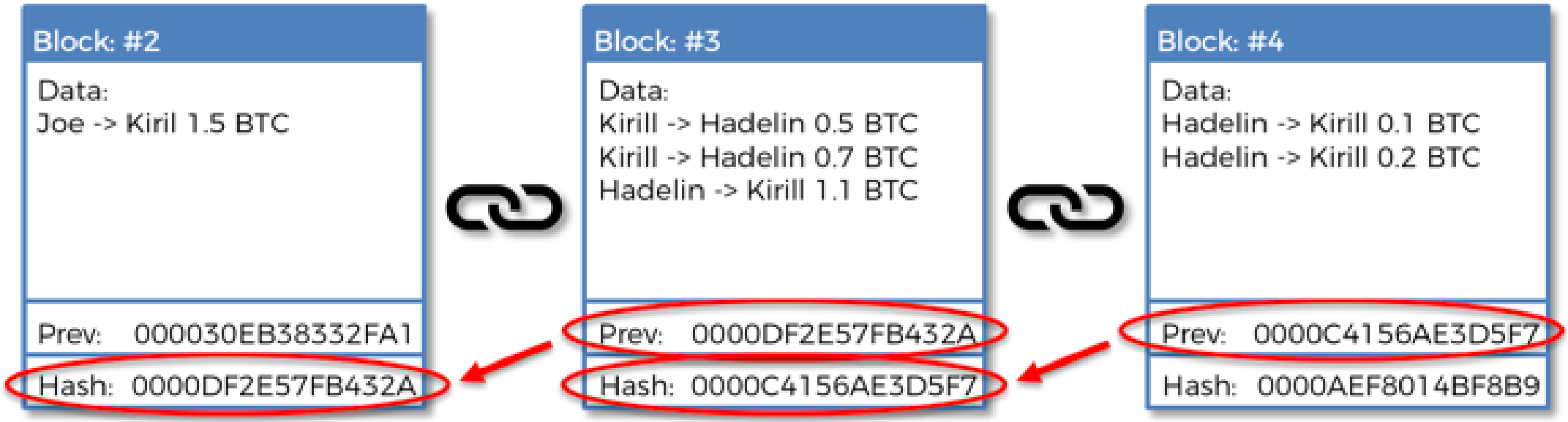
5

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

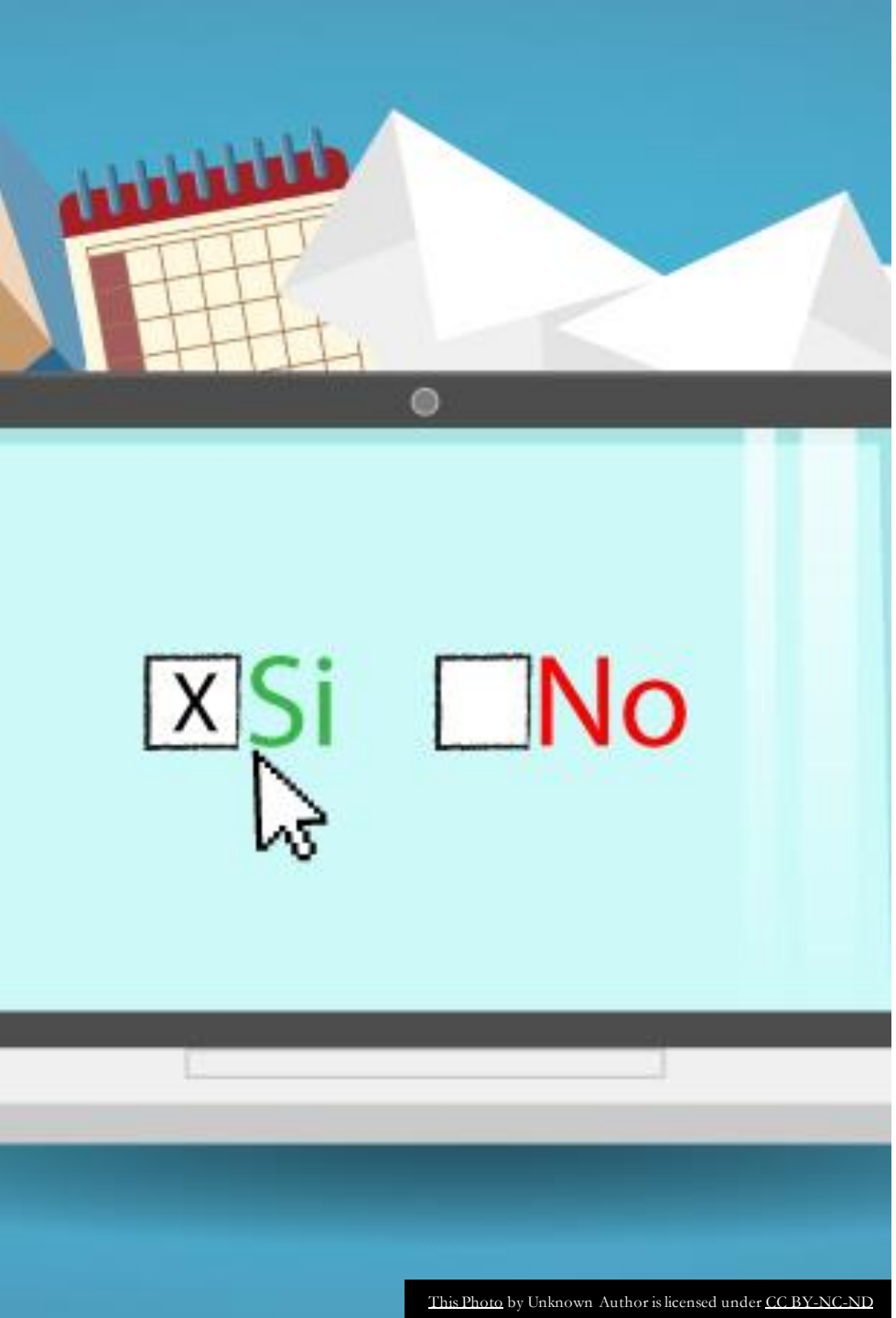
The transaction is complete.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Implementation – Individual Blocks



(c) 2022 Lexeprint Inc. All Rights Reserved.



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

Permission vs. Permissionless

- Require permission to join and participate in consensus
- No permission required to join and interact
- Governance Structure
- Decentralized
- Private Transactions
- Transparent network
- Authentication process
- Immutability
- Scalable Network
- Harder to scale

(c) 2022 Lexeprint Inc. All Rights Reserved.



Validation Methods

- All blockchain networks require a consensus mechanism to validate every new block added to the chain.
- Consensus mechanisms allow nodes on the blockchain to agree upon the accuracy of each block of transactions before it is added to the chain.
- Proof of Work and Proof of Stake are two of the most used consensus mechanisms in the blockchain industry.

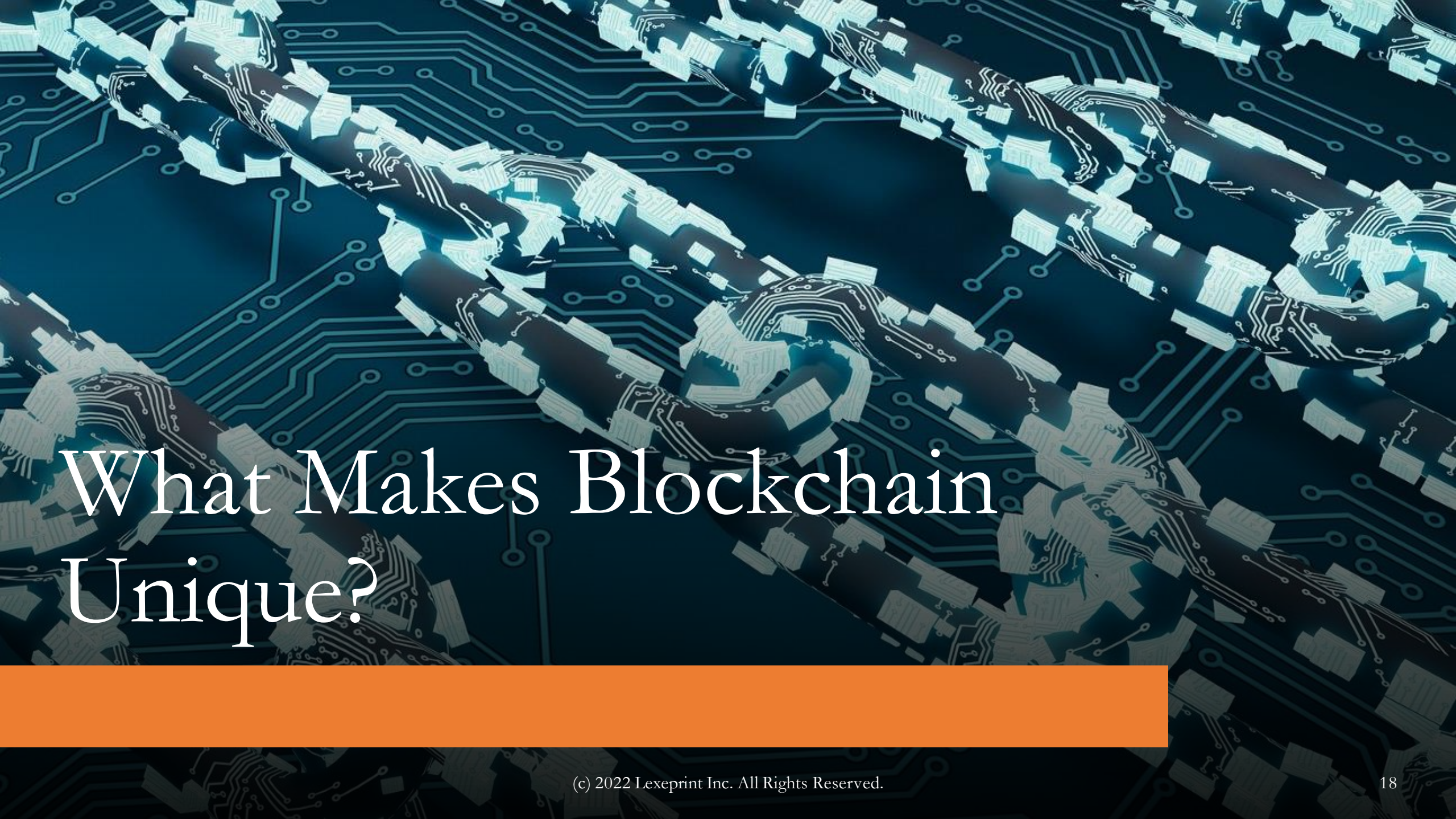
(c) 2022 Lexeprint Inc. All Rights Reserved.



Proof of Work vs Proof of Stake

Proof of work	**Proof of Stake**
Participating nodes are called miners.	Participating nodes are called validators or forgers.
Mining Produced new coins.	No new coins are formed.
Miners receive block rewards.	Validators receive transaction fees.
Huge energy consumption.	Low to moderate energy consumption.
Computational power determines the mining capacity.	The stake in the network depends on the validating capacity.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What Makes Blockchain Unique?

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

Decentralizing the System

- Blockchain focuses on decentralizing an entire network. Decentralizing a system refers to an arrangement where there is no single owner of the network.
- Everybody on the network stores a copy of the ledgers and of every block. Using blockchain, the need for middlemen and trust authorities have been eliminated.
- Completing transactions have become easier as this technology allows people to trust each other rather than having them to prove their identities before making any transaction.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Transparency

- As blockchain decentralizes the system and enables everybody to arrive on the same network, the ability for people to view transactions becomes easier.
- Blockchain is a technology that increases transparency of transactions, as everybody on the network has a copy of the ledger. This makes the blockchain ledgers tamper-proof.
- Using blockchain technology, people can make transactions from any part of the globe. All they need to do is register themselves on these ledgers. Once registered, they can order anything from any part of the world pay on the blockchain.

(c) 2022 Lexeprint Inc. All Rights Reserved.



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

Privacy

- Privacy on blockchain is another feature of blockchain that makes it so special. Privacy in blockchain can be maintained as you publish the required data, and still rest assured that your information will not be misused.
- For people to keep their transactions and identity private, they can create private networks where access is limited, and people can choose from a list of entities to be added onto that blockchain network.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Security

- A feature that makes blockchain stand out of the crowd and showcases it as one of the prime-time technologies is its security.
- While making a transaction, your public key is converted into a private key and sent to the person who you want to make a transfer to.
- The private key sent to the user is a hashed version of the crypto-currency that is to be sent to the receiver. During this transaction, your private key is secure and is not being exchanged with anyone.

(c) 2022 Lexeprint Inc. All Rights Reserved.


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

Bitcoin Governance Model

- Bitcoin follows a governance model of collaboration of a tradition of open-source software.
- Bitcoin updates its software using the process from the Request for Comments format which was created in 1969.
- Bitcoin utilizes Off-chain Governance. This type of governance operates when all stakeholders agree and make all relevant updates and implementations in unison.
- If a consensus is not reached, the network is split into two chains that run different versions of the software. The successor to the original chain is the chain with the most transactional hashing power.

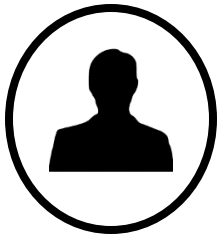
(c) 2022 Lexeprint Inc. All Rights Reserved.



Questions?

(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
URL: www.lawandforensics.com



David Cass
Email: david@lawandforensics.com
URL: www.lawandforensics.com



Bradford Newman
Email: bradford.newman@bakermckenzie.com
URL: https://www.bakermckenzie.com/en



Arun Hegde
Email: arun_hegde@g.harvard.edu

(c) 2022 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Founder
JAMS – Neutral
Harvard - Adjunct
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

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.

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. 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.

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) 2022 Lexeprint Inc. All Rights Reserved.



David Cass
Law & Forensics LLC – Senior Partner
Contact:
E: david@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

David Cass is a senior partner at Law & Forensics LLC where he leads the Cryptocurrency and Digital Banking Practice and is a member of the Cyber Security and Forensics Practice. He has extensive experience in financial services regulation, cryptocurrency, digital assets, blockchain, cloud, and digital banking.

He most recently served as a lead regulator for the Federal Reserve Bank of New York where he was a member of the Large Institution Supervision Committee (LISCC). Prior to this appointment, David was the CISO & Global Partner of IBM's Cloud Security Service Unit where he was responsible for its security practices, processes, and policies.

He has been an active contributor of the FS-ISAC and the European Banking Federation on Cloud Compliance and Security for financial services firms and has worked closely with US and international regulators. He was part of the team that introduced the first financial services blockchain initiative utilizing public cloud supported by 10 major international banks.

Previously, he served as SVP & CISO for Elsevier where he led an organization of experienced legal, risk, and security professionals who provided data protection, privacy, security, and risk management guidance on a global basis. He also served as Elsevier's HIPAA officer.

David has an MSE from the University of Pennsylvania, and an MBA from MIT. He is a frequent speaker at high-profile conferences and served on a public corporation's Board of Directors. He also is an editorial board member for The Journal of Law & Cyber Warfare and serves as a board member for the UCLA Extension Silicon Beach Innovation Lab. He is a faculty member for the non-profit Global Cyber Institute, and an adjunct faculty member for Harvard and at the Rutgers Law School. He is a member of the New York City Cyber Critical Services & Infrastructure team organized by the NYPD and the office of the NY District Attorney.

In his free time, David is a volunteer firefighter & Swiftwater Rescue Technician.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Bradford Newman
Chair of North America Trade Secret Practice – Baker McKenzie
Contact:
E: bradford.newman@bakermckenzie.com
URL: https://www.bakermckenzie.com/en

Baker McKenzie.

Bradford Newman is a litigation partner resident in Baker McKenzie's Palo Alto Office and Chair of the North America Trade Secrets Practice. According to Chambers USA, Brad is a "recognized authority on trade secrets cases" who "is valued for his tenacious, intelligent and thoughtful approach to trade secrets matters." Bradford regularly serves as lead trial counsel in cases with potential eight and nine-figure liability, and has successfully litigated (both prosecuting and defending) a broad spectrum of trade secrets cases in state and federal courts throughout the country. He routinely advises and represents the world's leading technology, banking, professional service, manufacturing and commerce companies in connection with their most significant data protection and trade secret matters. Bradford is the author of Protecting Intellectual Property in the Age of Employee Mobility: Forms and Analysis, a comprehensive treatise published by ALM that offers authoritative guidance on legal risks and practical steps companies can take to protect their IP and remedy IP theft.

Bradford specializes in matters related to trade secrets, Artificial Intelligence, Decentralized Finance (DeFi), Smart Contracts, Blockchain and Cryptocurrency. He is the Chair of the AI Subcommittee of the ABA. Recognized by the Daily Journal in 2019 as one of the Top 20 AI attorneys in California, Bradford has been instrumental in proposing federal AI workplace and IP legislation that in 2018 was turned into a United States House of Representatives Discussion Draft bill. He has also developed AI oversight and corporate governance best practices designed to ensure algorithmic fairness. Brad also serves as outside general counsel to one of the world's leading DeFi projects.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Arun Hegde
Sony Music - Director of Security
Contact:
E: arun_hegde@g.harvard.edu

Arun Hegde is a seasoned information security professional and trusted advisor with over 16 years of multi-domain leadership experience in the field. Arun is Director of Security at Sony Music, a global entertainment conglomerate where he leads and manages security practices operating in over 50 countries. He has a solid record in providing Cybersecurity leadership to organizations ranging from startups to Fortune 20 companies including Sony Music, Microsoft, BNP Paribas, TD Ameritrade, and Citigroup. Recognized for building world-class teams that deliver exceptional performance in risk management, threat intelligence, forensics & digital evidence collection, enterprise/cloud security, regulatory and incident management. He has been developing and delivering customer-centric security solutions on site and in the cloud to mitigate risk and data breaches that diminish organizational integrity and value.

His entrepreneurial journey includes two international start-ups which provided services to Fortune 20 companies and world-renowned nonprofits.

Arun is a blockchain and crypto enthusiast who researches and invests in blockchain projects. Over the years, he has spoken at numerous crypto & blockchain security summits in the New York area. He also is a contributor at CryptoNewsBytes.com, one of crypto news media startup. Currently he is a Guest Associate Faculty at Harvard for 'Blockchain and Cryptocurrency' course for this semester.

(c) 2022 Lexeprint Inc. All Rights Reserved.