

Crypto and Blockchain: Understanding the Technology and Challenges It Presents

Part 1 of 2

Speakers:

Daniel B. Garrie, Esq., Founder, Law & Forensics; Neutral, JAMS; Adjunct, Harvard

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

(c) 2022 Lexeprint Inc. All Rights Reserved

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

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 & Forensics
Neutral, JAMS
Adjunct, Harvard



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

(c) 2022 Lexeprint Inc. All Rights Reserved

Agenda

Part 1:

- Blockchain Basics
- Cryptography 101
- Append only ledgers

Part 2:

- Consensus
- Digital Signatures & Transactions
- Decentralized Networks, Incentives & Mining
- Governance, Forks, and Collective Action

(c) 2022 Lexeprint Inc. All Rights Reserved



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

Blockchain Technology

- 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



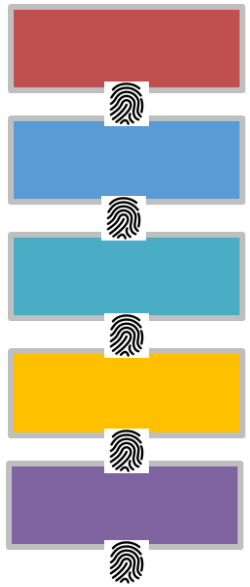
Blockchain Technology

- 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, Blockchain is a form of distributed ledger technology that enables data sharing across a network of individual computers.
- The main appeal of blockchain technology is twofold:
  - all data and transactions that are on the blockchain are nearly impossible to modify or hack; and
  - the data itself is transparent.

(c) 2022 Lexeprint Inc. All Rights Reserved

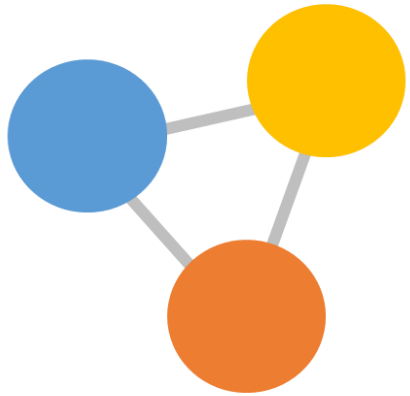
Blockchain Technology

Timestamped append-only ledger



Secured via cryptography
- Hash functions for **integrity**
- Digital signatures for **consent**

Multiple party consensus protocol



Addresses '**cost of trust**'
May use Native Token as incentive
- Permissioned
- Permissionless

Decentralized auditable database



Tamper resistant record of
- Transfers of **value**
- Running of **computer code**

(c) 2022 Lexeprint Inc. All Rights Reserved



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

Blockchain Technical Components

- Append-only Ledgers
  - Cryptographic Hash Functions
  - Block Headers & Merkle Trees
  - Timestamped Logs (Blocks)

(c) 2022 Lexeprint Inc. All Rights Reserved



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

Lexeprint PUBLISHING GROUP

Blockchain Technical Components

- Transactions, Code & Ledgers
  - Asymmetric Cryptography & Digital Signatures
  - Addresses
  - Transaction Inputs & Outputs or State Transitions
  - Unspent Transaction Output (UTXO) set or Account Based
  - Programming Code for Transactions (Bitcoin Script, Solidity, or other)

(c) 2022 Lexeprint Inc. All Rights Reserved

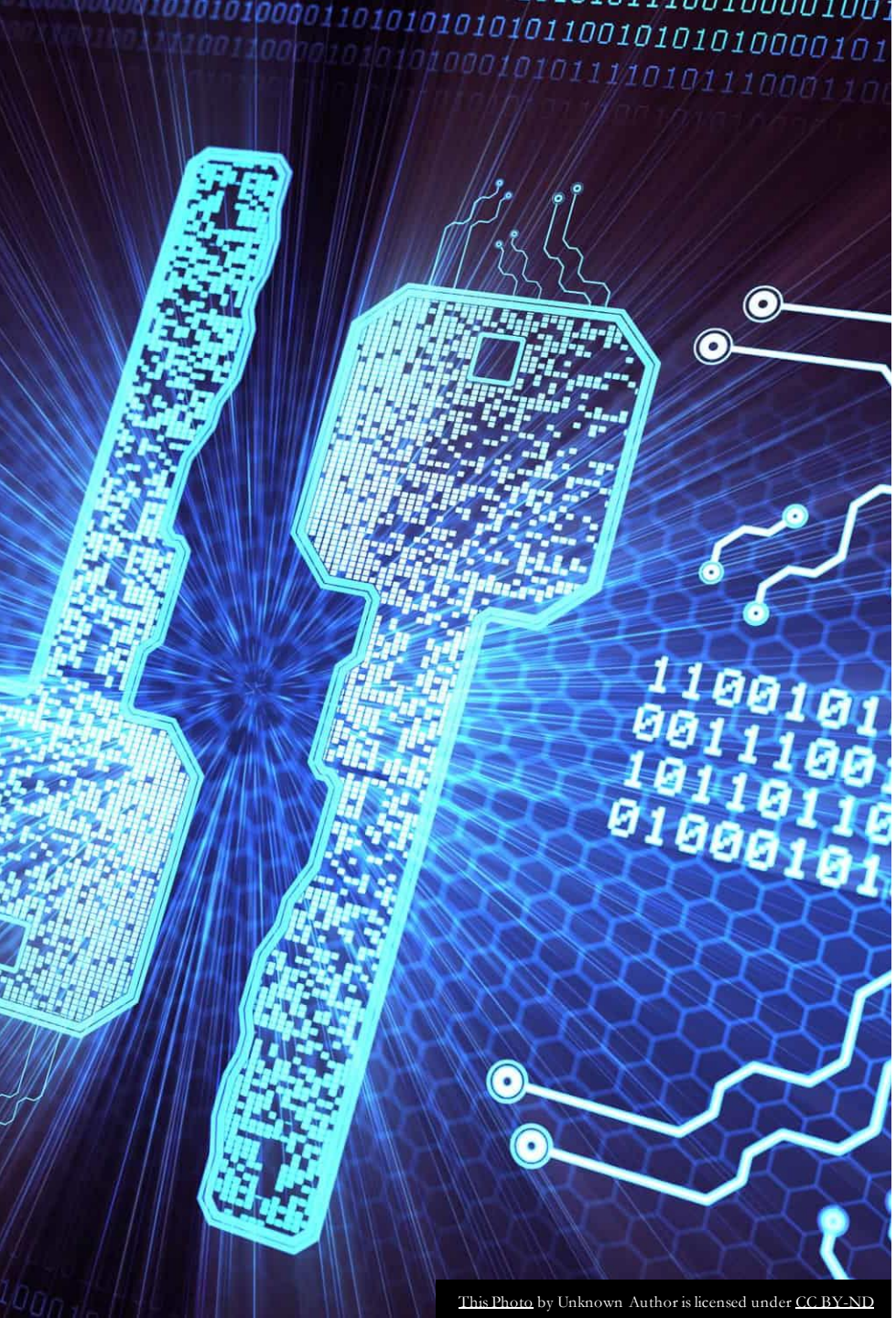

This Photo by Unknown Author is licensed under CC BY-SA

Lexeprint PUBLISHING GROUP

Blockchain Technical Components

- Decentralized Network Consensus
  - Consensus Protocol (Proof of Work, Proof of Stake, or other)
  - Native Token
  - Network

(c) 2022 Lexeprint Inc. All Rights Reserved



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

Lexeprint PUBLISHING GROUP

Cryptography 101

- The primary goal of cryptography is to secure important data on the hard disk or as it passes through a medium that may not be secure itself. Usually, that medium is a computer network.
- Services: Cryptography can provide the following services:
  •Confidentiality (secrecy)
  •Integrity (anti-tampering)
  •Authentication
    - Non-repudiation

(c) 2022 Lexeprint Inc. All Rights Reserved

Cryptography: Communications in the presence of adversaries



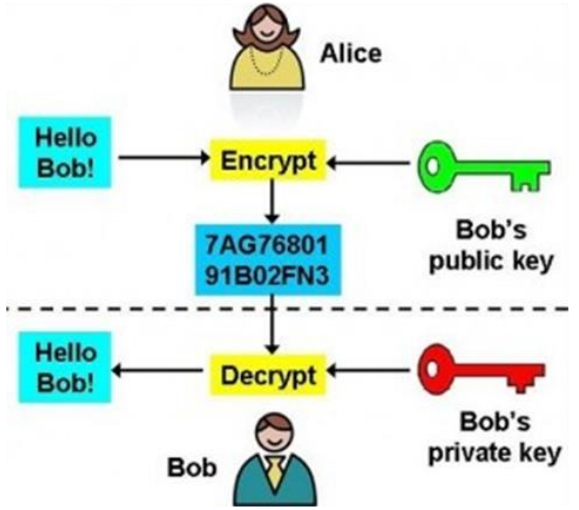
Hieroglyphics



Scytale Cipher
Ancient Times



Enigma Machine
1920s - WWII

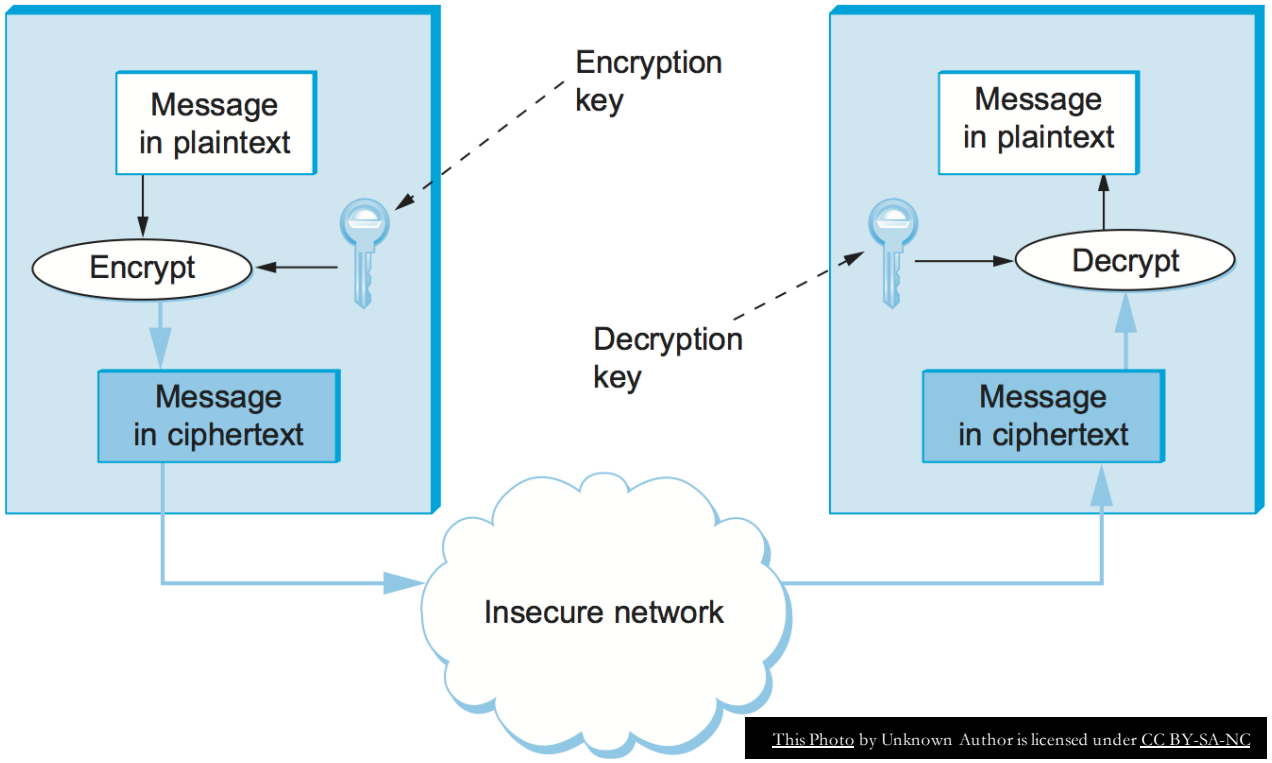


Asymmetric Cryptography
1976 to today

(c) 2022 Lexeprint Inc. All Rights Reserved

Cryptographic Hash Function

- One way - it cannot be used to obtain the original data, only to check that the data that generated the hash matches the original data
- A hash function is a unique identifier for any given piece of content. It's also a process that takes plaintext data of any size and converts it into a unique ciphertext of a specific length.



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

(c) 2022 Lexeprint Inc. All Rights Reserved

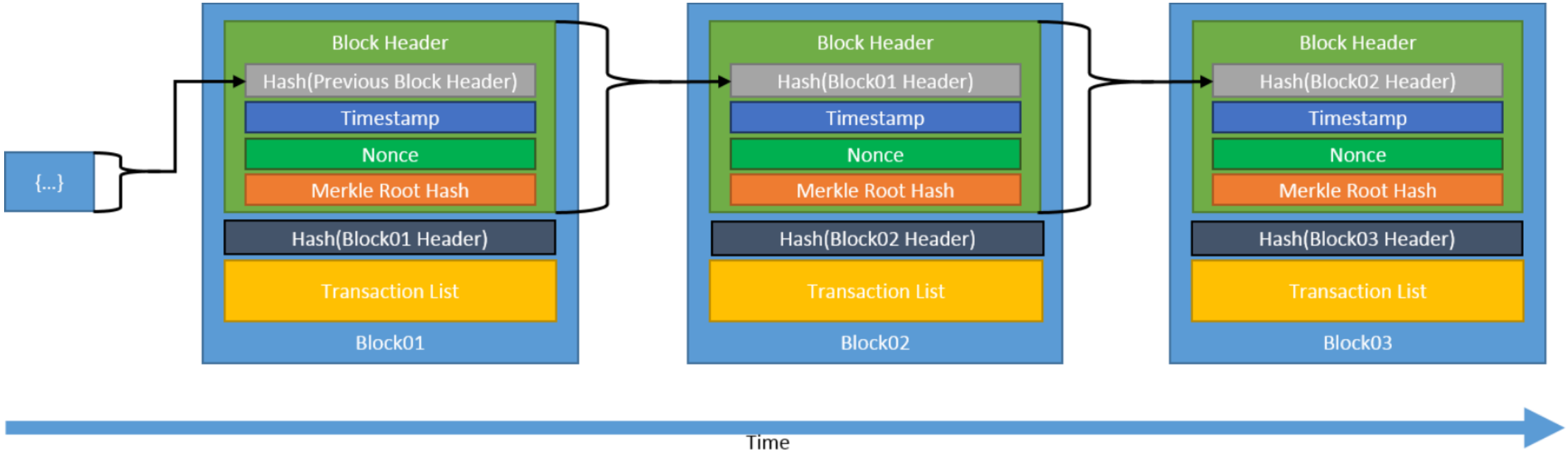
Timestamped Append only ledger





- The First Blockchain or How to Time-Stamp a Digital Document

(c) 2022 Lexeprint Inc. All Rights Reserved



(c) 2022 Lexeprint Inc. All Rights Reserved

Contact Us



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



David Cass
Email: davidcassciso@gmail.com
URL: https://www.lawandforensics.com/

(c) 2022 Lexeprint Inc. All Rights Reserved



Daniel B. Garrie, Esq.
Law & Forensics LLC – Founder
JAMS – Neutral
Harvard - Faculty
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://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, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, 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. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and 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 – Senior Partner
Contact:
E: davidcassciso@gmail.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.