

# LEGAL ISSUES IN CRYPTOGRAPHY AND CRYPTOCURRENCIES

**Instructor:** Dr. Giovanna Massarotto

## **Structure**

14 sessions

## **Description**

This course explores the intersection of cryptography and law, with a particular focus on cryptocurrencies. It begins by tracing the evolution of cryptography, from its role as a critical tool in World War II to its development through the work of mathematicians, philosophers, and activists who championed privacy as essential to human and economic freedom. This movement, known as the cypherpunk movement, ultimately led to the creation of Bitcoin—a groundbreaking digital payment system.

Students will critically examine cryptography and its applications, including cryptocurrencies like Bitcoin, to understand their impact on society and the complex legal challenges they present. The course will emphasize the evolving role of privacy in an increasingly digital world and its significance for economic freedom through payments.

Each class will be highly interactive, requiring active learning, active listening, and the ability to both respond to and formulate questions. Guest speakers, including Patrick Murck (co-founder and lawyer of the Bitcoin Foundation), the Deputy General Counsel and Vice President of Ripple Wansun Song and Prof. Brett Falk from the Penn Computer Science Department, will be invited to enrich class discussions.

## **Course Objectives**

By the end of the course, participants should expect to:

- Understand the foundations of cryptography and its legal foundations.
- Evaluate the role of cryptography in protecting privacy and free speech critically.
- Analyze different cryptographic applications via case studies.
- Gain a deeper understanding of cryptocurrency and the main legal issues involved.
- Recognize the impact that these technologies have on society, with a concentration on the financial sector.
- Examine the evolving role of cryptography and cryptocurrency in law and explore their future implications.

## **Evaluation Methods**

Attendance is required. Please do not come to class, if you are sick. Email me and we will speak about how you can keep up with the material and class discussion.

## Participation (30%).

Students will be expected to have read the assigned readings, and cases before each class. Class preparedness and participation are essential. If something in the assigned reading is not understandable, students are encouraged to ask for an explanation. Students will be provided with a PowerPoint handout. The participation grade will be based on students' preparation for each class and a team assignment that includes a presentation. For this assignment, students

will develop a case related to a cryptographic application (e.g., FTX and the crypto case involving Kim Kardashian) specified in the syllabus. Students are expected to investigate the main legal issues involved critically and be prepared to present and debate their findings with the class. Presentations will take place between Week 7 and Week 13.

### Writing Assignment (70%)

The written exam will consist of a paper (around 25 pages in length) that requires students to explain and critically analyze an ongoing debate in the field of cryptography and law by including a case study. Topics and cases will be suggested, although you may choose your own topic. You are encouraged to discuss your selected case and approach with your instructor. Students will be asked to reflect upon and include readings and discussions covered in class and demonstrate careful research of the relevant law and scholarly literature, including law journal articles.

**Artificial Intelligence Policy.** You may use AI tools to assist in the creation of your written work in this course subject to the general principle that **all work submitted by you must be your work product alone**. Specifically:

- You may use AI tools to help you brainstorm about topics or refine your topic ideas;
- You may use AI tools to assist you in your research;
- You may use AI tools to help you edit a draft that you have written for clarity or length;
- You may not use AI tools to create “first drafts” or other blocks of textual material.

**You must cite any use of a generative AI tool**, and include clear and specific details about the tool, its version, the developers or the organization responsible for it, and any pertinent parameters or settings that influenced the generation. Here's a sample format and an example:

### **Format:**

[AI tool name] ([Version, if available]). Developed by [Developers/Organization Name]. Retrieved [Date], from [URL or source if applicable]. [Specific parameters/settings if necessary].

### **Course Material**

Readings are specified for each week. There is no required textbook, but I am happy to recommend books or additional readings if you are interested in exploring specific topics from class in greater depth.

### **Office hours**

Office hours, whether virtual or in person, are by appointment. Please email to schedule a meeting. You can reach me at [gmassa@law.upenn.edu](mailto:gmassa@law.upenn.edu)

Sessions
<p><b>Week 1. Introduction to Cryptography and Its Legal Foundations</b></p> <p><b>Description.</b> Week 1 lays the foundation of cryptography from both technical and legal perspectives: from the right to privacy to cryptography and security. It covers Alan Turing’s groundbreaking work in breaking the ENIGMA code, which played a vital role in ending World War II, and explains why cryptography was classified as a munition.</p>

**Readings:** 1) Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193-199 (1890); 2) *What is Cryptography?* [ISO](#); 3) *The Enigma of Alan Turing*, [CIA](#) (Apr. 10, 2015); 4) *A History of Government Attempts to Compromise Encryption and Privacy*, [Reflare](#) (Oct. 11, 2024).

## **Week 2. Cryptography: From Free Speech to National Security**

**Description.** Week 2 investigates the intersection between free speech, security, and law enforcement through case studies—most notably, the Zimmermann case and the Apple v. FBI dispute.

**Readings:** 1) Ronald J. Stay, *Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann*, 13 [GEORGIA STATE UNIV. L. REV.](#) 581 (2012); 2) Bruce Schneir, *Why Cryptography is Harder than it Looks*, [INFORMATION SECURITY BULLETIN](#) (1997); 3) Ruth Micheal, *FBI-Apple Encryption Dispute*, [EBSCO](#) (2023); 4) Bruce Schneir, *Why you Should Side with Apple, not the FBI, in the San Bernardino iPhone Case*, [THE WASHINGTON POST](#) (Feb. 18, 2016).

## **Week 3. Cryptography and Patents**

**Description.** Week 3 examines whether cryptographic systems can be patented, using case studies, including the patent for the RSA cryptosystem.

**Readings:** 1) Greg Vetter, *Patenting Cryptographic Technology*, 84 [CHI. KENT L. REV.](#) 757 (2010); 2) Cryptographic Communications System and Method, [GOOGLE PATENTS](#) (1983).

## **Week 4. The Cypherpunk Movement: Cryptography and The Big Brother**

**Description.** Week 4 covers the rise of the cypherpunk movement, which emerged from cryptoanarchy and high-tech Hayekian movements that developed with the introduction of the Internet. The cypherpunk dream was to enable human and economic freedom through cryptography and decentralized technologies like the Internet.

**Readings:** 1) Timothy C. May, *The Cryptoanarchy [Manifesto](#)* (1988); 2) Eric Hughes, *A Cypherpunk's [Manifesto](#)* (1993); 3) Peter H. Lewis, *Forget Big Brother*, N.Y. [TIMES](#) (Mar. 19, 1998).

## **Week 5. Bitcoin is the Cypherpunks' Dream**

**Description.** Week 5 proceeds with a discussion about the Cypherpunk dream of enabling economic freedom through private digital money. It introduces the concept of what money is and explores the history of private digital money from eCash to Bitcoin. The lecture will also cover the revolutionary public key cryptography and blockchain technology underlying Bitcoin.

**Guest Speaker:** Patrick [Murck](#) (Co-founder of the Bitcoin Foundation, fellow at Berkman Center for Internet & Society at Harvard University).

**Readings:** 1) David Chaum, *Achieving Electronic [Privacy](#)* (1992); 2) Aaron Van Wirdum, *The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream*, [BITCOIN](#)

[MAGAZINE](#) (Apr. 24, 2018); 3) Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).

## Week 6. Cryptography, Cryptocurrencies, and Privacy

**Description.** Week 6 explores advancements in cryptographic protocols and privacy, focusing on cryptocurrency applications, including Zero-Knowledge Proofs, Zcash, and Multiparty Computation.

**Guest Speaker:** Prof. Brett Falk ([Penn CS](#))

**Readings:** 1) Hiroaki Oguro, *What is Zero-Knowledge Proof - a Hot Technology Bringing Trustworthiness to Web3 Privacy?* NTT [Data](#); 2) Cryptopedia, *Zcash Leads the Way on Zero-Knowledge Proofs With zk-SNARKs*, [GEMINI](#) (Oct. 2, 2023); 3) *What Is Multiparty Computation?* IEEE DIGITAL [PRIVACY](#).

## Week 7. Cryptocurrencies and Crimes

Student Presentation [FTX]

**Description.** Week 7 investigates major crimes concerning cryptocurrencies, from money laundering to scams, through case studies (e.g., Silk Road and Tornado Cash).

**Readings:** 1) The Chainalysis 2025 Crypto Crime [Report](#); 2) Press Release, *Tornado Cash Founders Charged With Money Laundering And Sanctions Violations*, [DOJ](#) (Aug. 23, 2023).

## Week 8. Cryptocurrencies: From Commodity to Security Regulation in the United States

Student Presentation [Kim Kardashian]

**Description.** Week 8 focuses on the debate over whether cryptocurrencies should be classified as commodities or securities, with an emphasis on the U.S. regulatory landscape and the impact of securities laws on cryptocurrencies.

**Guest Speaker:** a fireside chat with Ripple's Vice President, Deputy General Counsel Wansun Song

**Readings:** 1) Robert Stevens, *Securities vs. Commodities: Why It Matters For Crypto*, [COINDESK](#) (Mar. 8, 2024); 2) SEC, *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. SECURITIES AND EXCHANGE [COMMISSION](#) 3) Edward Lee, *The Original Public Meaning of Investment Contract*, HARVARD LAW SCHOOL FORUM ON CORPORATE [GOVERNANCE](#) (Jun. 1, 2024).

## Week 9. Cryptocurrencies and Regulation in Europe and U.K.

Student Presentation [Binance]

**Description.** Week 9 is devoted to exploring cryptocurrency regulation outside of the United States, with a focus on Europe and the U.K. The European Markets in Crypto-Assets (MiCA) regulation will be explored and debated.

**Readings:** 1) *What is MiCA (Markets in Crypto Assets Regulation)?* [COINBASE](#) ; 2) Press Release, *New Cryptoasset Rules to Drive Growth and Protect Consumers*, GOV.UK (Apr. 29, 2025).

### **Week 10. Stablecoin**

Student Presentation [Tether]

**Description.** Week 10 focuses on stablecoins and their regulation, examining the current legislation in the United States and exploring case studies such as Tether.

**Readings:** 1) *Will a New Law Make Cryptocurrency Safer?*, HARVARD LAW [TODAY](#) (Jul. 30, 2025); 2) Sandra Waliczek & Herry Yeung, *The GENIUS Act is designed to regulate stablecoins in the US, but How Will it Work?*, WORLD ECONOMIC [FORUM](#) (July 29, 2025).

### **Week 11. DeFi and Smart Contracts**

Student presentation [Consensys]

**Description.** Week 11 discusses decentralized finance (DeFi), including Decentralized Exchanges (DEX), such as Uniswap, and smart contracts underlying DeFi applications.

**Readings:** 1) Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, FEDERAL RESERVE BANK OF ST. [LOUIS](#) (Apr. 15, 2021); 2) What is Decentralized Finance (DeFi)? [KRAKEN](#) (Mar. 17, 2025).

### **Week 12. Smart Contracts and DAO**

Student presentation [Samuels v. Lido DAO]

**Description.** Smart contracts are software programs that automatically execute a set of predefined instructions. Week 12 explores the ongoing debate surrounding the enforceability of smart contracts and Decentralized Autonomous Organizations (DAOs).

**Readings:** 1) Stuart D. Levi and Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARVARD LAW SCHOOL FORUM ON CORPORATE [GOVERNANCE](#) (May 26, 2018); 2) Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, 21 STAN. TECH. L. [REV.](#) 198 (2018).

### **Week 13. Cryptocurrencies and Antitrust**

Student Presentation [Tether antitrust case]

**Description.** Week 13 discusses the main antitrust issues related to cryptocurrencies, including collusion and decentralization.

**Readings:** 1) Cheyenne Ligon, *Plaintiffs File New, Slimmed Down Complaint in Class Action Lawsuit Against Tether*, [COINDESK](#) (Jul. 15, 2024); 2) Giovanna Massarotto, *Can Antitrust Trust Blockchain?*, ALGORITHMIC [ANTITRUST](#) (Springer, 2022).

**Week 14. Course Review and The Future of Cryptography and Law**

**THIS SYLLABUS IS SUBJECT TO CHANGE**