Scrutinizing Security: Auditing for Vulnerabilities in Blockchain and Cryptocurrency Markets

Michael Clements

Director, Financial Markets and Community Investment

US Government Accountability Office

Agenda

- What is blockchain and what are the use cases, especially in financial services?
- What are the benefits and risks of blockchain-related products and services?
- What's the regulatory and supervisory framework for blockchain-related products and services?
- What lessons does the FTX failure provide?
- What actions are needed to address regulatory gaps and weaknesses?

Blockchain

- Blockchain is a type of distributed ledger that allows users to conduct and record tamper-resistant transactions that multiple parties make without a central authority, such as a bank.

- Non-financial applications
  - Real estate records
  - Government operations (e.g., grants management)
  - Supply chains

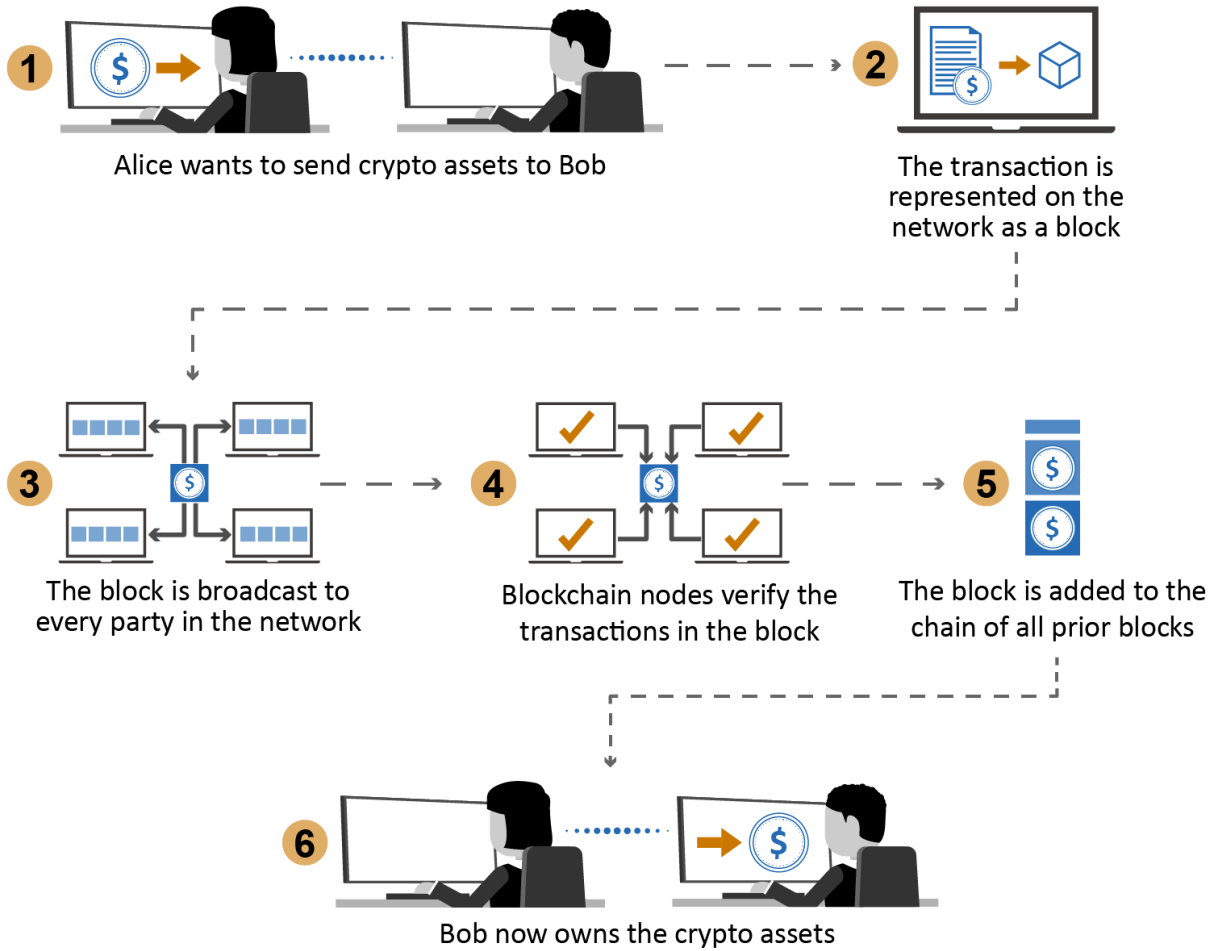
- Financial applications
  - Crypto assets

Crypto Assets

- A crypto asset is a type of private sector digital instrument that primarily depends on blockchain technology.
  - Cryptocurrencies, including Bitcoin and stablecoins
  - Security tokens
  - Crypto derivatives

- Crypto assets have related activities and finance-related use cases.
  - Custody
  - Borrowing and lending
  - Trading

Distributed Finance (DeFi)



Source: GAO. | GAO-23-105346

Centralized Finance (CeFi)

- While blockchain promises decentralized transactions, many retail investors engage with crypto assets through intermediaries.

- Possible barriers to fully decentralized transactions.
  - Technical skills
  - Time and interest

- Crypto asset platforms have emerged to fill the void.
  - Custody services
  - Centralized exchanges (borrowing and lending, trading)

Blockchain in Finance – Possible Benefits

- Blockchain-based financial services could provide benefits.
  - **Cost savings** – potential to reduce costs for payments and other transactions by removing intermediaries
  - **Faster transactions** – transactions may execute more quickly than traditional financial services
  - **Transparency** – may provide greater transparency for some information than traditional financial services

Blockchain in Finance – Risks

- Blockchain-based financial services pose significant risks, many of which have occurred.
  - **Volatility risk** – prices of crypto assets typically have been more volatile than other financial assets
  - **Market and financial stability risk** – with greater integration, volatility could spread to traditional financial institutions and markets
  - **Intermediary risk** – some trading platforms have paused withdraws and transactions during market stress

Blockchain in Finance – Risks

- Blockchain-based financial services pose significant risks, many of which have occurred.
  - **Cybersecurity and theft risk** – consumers and investors have experienced significant losses from fraud and scams
  - **Information asymmetry risk** – crypto asset issuers and platforms may not fully disclose material information, including risks
  - **Illicit activity risk** – the perception of anonymity makes crypto assets a preferred tool for certain criminal enterprises

Blockchain in Finance – Regulatory Framework

- Federal financial regulators oversee regulated institutions' engagement with crypto assets. Regulatory jurisdiction for crypto assets varies based on the activity and intermediary.
  - Securities and Exchange Commission (SEC)
  - Commodity Futures Trading Commission (CFTC)
  - Banking regulators
  - Financial Crimes Enforcement Network (FinCEN)

- States may oversee crypto-assets and related activities, such as money transmission.

Blockchain in Finance – Regulatory Framework

- A key factor driving regulatory jurisdiction is whether the crypto asset is a commodity, security, or something else.

- For example, to determine whether a crypto asset is subject to its regulation, SEC assesses whether the asset meets the statutory definition of a "security" under the federal securities laws.
  - *Howey* test [*SEC v. W.J. Howey Co.*, 328 U.S. 293, 298-99 (1946)]
  - *Reves* test [*Reves v. Ernst & Young*, 494 U.S. 56 (1990)]

Blockchain in Finance – Regulatory Framework

- The federal regulatory regime applicable to crypto asset trading platforms depends on the crypto assets they trade.
  - SEC registration as a national securities exchange
  - CFTC registration as a commodity derivatives exchange (bitcoin futures)
  - FinCEN registration as a money transmitter

- The level of oversight varies greatly.
  - SEC and CFTC: Focused on investor protection and market integrity through listing requirements and prevention of fraud, deception, and trading manipulation. Also, BSA/AML compliance.
  - FinCEN: Focused on BSA/AML compliance.

Blockchain in Finance – Regulatory Framework

Registration status	**Listing requirements** (minimum financial and non-financial standards for the assets trading on an exchange)	**Market integrity** oversight (monitor for fraud, deception, and trading manipulation)	**Illicit finance** oversight (monitor for money laundering and Bank Secrecy Act compliance)
SEC registration as a national securities exchange	●	●	●
CFTC registration as a commodity derivatives exchange	●	●	●
FinCEN registration as a money transmitter			●

Blockchain in Finance – Regulatory Framework

- Trading platforms may be required to register as money transmitters under state law. State money transmitter regulation may not address market integrity issues and the potential for fraud, deception, or market manipulation.

- Some states may provide more comprehensive regulation, but such oversight would apply only to those trading platforms licensed and operating in that state.
  - For example, New York BitLicense

Blockchain in Finance – Regulatory Gaps

- Regulatory gaps for blockchain-based financial products pose risks to investors, consumers, and financial stability.

Regulatory Gaps – Spot Markets for Non-Security Crypto Assets

- Federal regulators have limited authority to regulate platforms that don't trade securities or commodity derivatives—known as spot markets for non-security crypto assets.
  - CFTC has determined that certain crypto assets, such as Bitcoin, are commodities.

- Spot markets are generally subject to registration and oversight by FinCEN as money transmitters for BSA/AML compliance and may be required to register as money transmitters with states.

- Several platforms without federal oversight have experienced fraud and trading manipulation.

Regulatory Gaps – Stablecoins

- Stablecoins purport to hold a stable value relative to a fiat currency, such as the U.S. dollar. To keep their value, issuers often state their stablecoins are backed by reserve assets.

- No uniform standards exist for reserves, including reserve levels, asset composition, audit requirements, or public disclosure. This increases the risk that a stablecoin may not be able to hold its value and honor user redemption requests.

- To the extent stablecoins become more integrated into the financial system, their failures could pose risks to financial stability.

FTX - Background

- FTX was established in 2019, primarily as a centralized cryptocurrency exchange platform. FTX allowed users to trade cryptocurrencies and crypto derivatives

- FTX grew rapidly across different business models
  - Alameda Research—A crypto hedge fund founded in 2017, later became affiliate to FTX.
  - LedgerX—A platform for cryptocurrency derivatives, acquired by FTX in October 2021.

FTX - Background

- Problems arose in summer 2022 when cryptocurrencies experienced significant volatility.

- FTX is alleged to have misused funds via Alameda Research.
  - FTX may have provided unlimited line of credit to Alameda.
  - Alameda received trading preference on FTX's trading platform.
  - Alameda used FTX funds, including customer funds.

FTX – Problems and Lessons

- Customers face significant financial risk.
  - Funds considered part of bankruptcy estate (e.g., Celsius)?

- The FTX experience provides several lessons.
  - Importance of internal controls
  - Mitigation of conflicts of interest
  - Segregation of customer and company assets
  - Clarity of regulatory authority and timeliness of regulatory action

Blockchain in Finance – What's Needed

- Congress should consider legislation that designates a federal regulator to provide for regulatory oversight of spot markets for non-security crypto assets.

- Congress should consider legislation providing for consistent and comprehensive oversight of stablecoin arrangements.

- Federal financial regulators should jointly establish a formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response.