Emerging Threats in the Crypto Sector

Brian Trackman

Acting Director, LabCFTC

U.S. Commodities Futures Trading Commission

September 10, 2019

Disclaimer

CFTC DISCLAIMER: This presentation is being made by a representative of the U.S. Commodity Futures Trading Commission on behalf of the Commission for educational and informational purposes only. It does not constitute legal interpretation, guidance or advice of the Commission. Any opinions or views stated by the presenter are his/her own and may not represent the Commission's views.

Threat	Something that may cause injury or harm
Risk	(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; peril

Sources: https://www.merriam-webster.com; https://oed.com/

Risk in the Crypto Sector

Financial Marketplaces	• A number of risks are inherent to marketplaces. Abusive trading and market manipulation are familiar risks that undermine market integrity, and with it trust and confidence among participants.
Participant Victims	• Another familiar category of risk relates directly to participants. • Fraud, hacks, ransomware attacks, cyber theft, and other nefarious activity can victimize individual parties.
Digital Tokens	• The development of digital tokens has added a new layer of risks, which include operational, regulatory, security, and speculative. • Custody is one key area. How can virtual assets be safeguarded effectively? How can holdings be verified?
Crypto Trading Networks	• The structure and implementation of new crypto trading networks is a also a unique source of risk. Decentralization, governance and accountability are key focus areas.

BITFINEX

- Bitfinex was one of the largest digital currency exchanges. More than $60 million worth of bitcoin was stolen through a hack of the platform in 2016.
    - Largest theft since Mt. Gox in 2014.
    - The attack compromised “multi-sig” wallets, which divide keys among users and were thought to be more secure. The price of Bitcoin plunged after news of the theft broke.
    - To compensate for the hack losses in 2016, the exchange generalized the losses across all accounts and compensated its users with new BFX tokens, each valued at $1 USD. BFX token holders subsequently had their tokens fully redeemed or converted to shares of the company.
    - Most recently, two brothers have been arrested and charged with the 2016 theft.

- Bitfinex entered into an undisclosed arrangement with Tether whereby it effectively borrowed $850 million in value. The Tether tokens were not backed as described with actual dollar deposits. The DOJ and CFTC opened a criminal probe, resulting in a penalty.

The DAO

- Decentralized autonomous organizations are entities that utilize smart contracts to operate.
- In early 2016, one such organization calling itself The Decentralized Autonomous Organization or "The DAO" launched. It was to be a venture capital fund for crypto and blockchain projects.
- That summer, The DAO was hacked, and 3.6 million ether tokens then valued at about $70M USD were stolen. The attack essentially turned The DAO into a broken ATM machine by using a recursive call to transfer ether out multiple times before the smart contract could update its balance.
- Post Script: On July 25, 2017, US SEC published a ruling that:

  "Tokens offered and sold by a 'virtual' organization known as 'The DAO' were securities and therefore subject to the federal securities laws. The Report confirms that issuers of the distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. Those participating in unregistered offerings also may be liable for violations of the securities laws."

QUADRIGACX

- QuadrigaCX was Canada’s largest cryptocurrency exchange.
- In January 2019, QuadrigaCX’s Twitter page stated that its founder, 30-year-old Gerald William Cotten, died suddenly during a journey to India.
- QuadrigaCX stated that all the assets of the exchange were kept in a cold storage, and only Cotten knew the password. About $190M USD in value was lost.
- Firms such as CipherTrace have stated that QuadrigaCX had moved most of the crypto currency to other exchanges well before Cotton’s alleged death.
- Ernst & Young stated QuadrigaCX had no significant internal controls, which meant Cotton could move crypto currencies within, to, or from the platform at will.

Threats Beyond the Familiar…

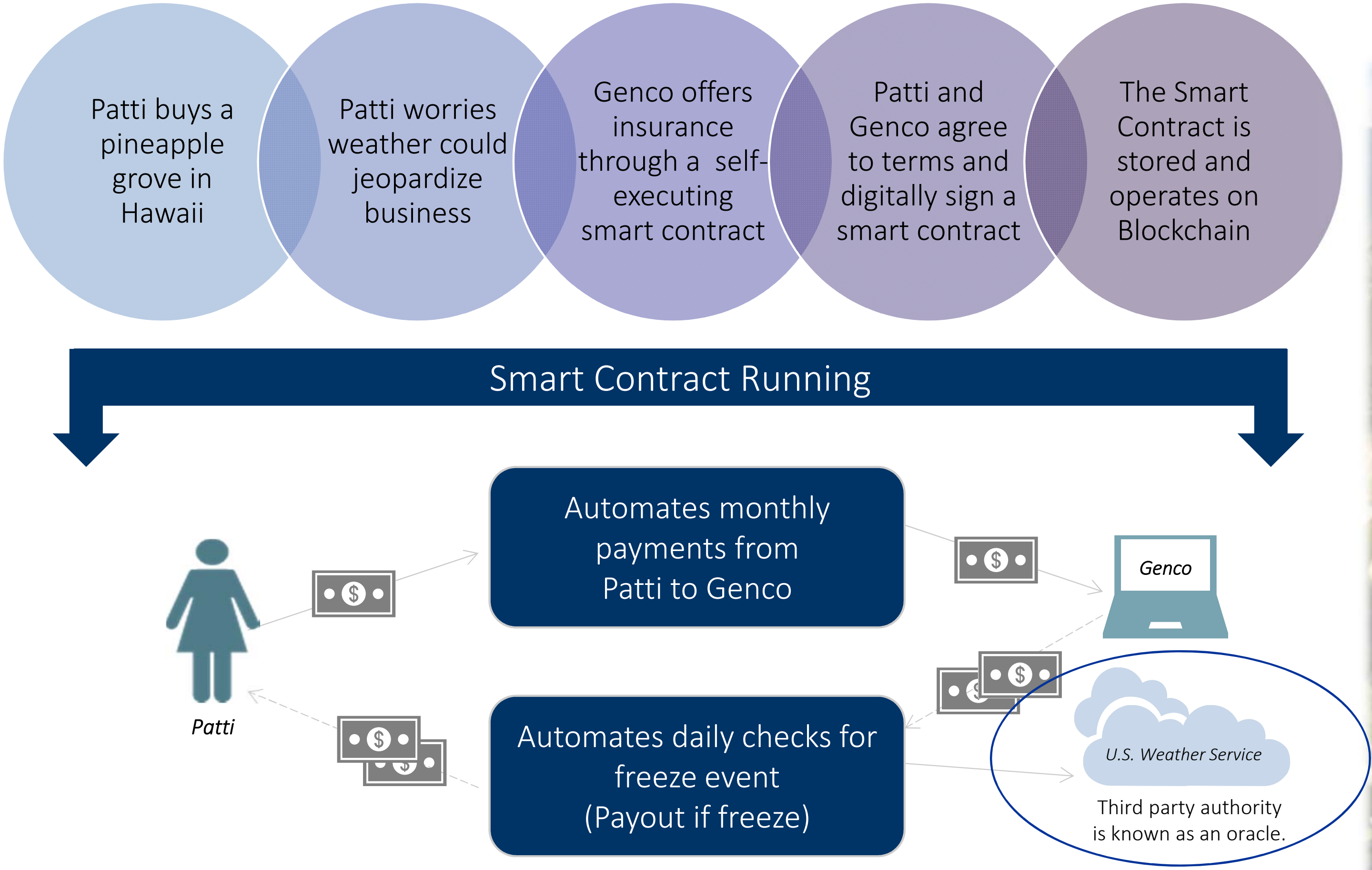
Forking

- Forking occurs when a new branch splits off an existing blockchain. Forking can be the result of a change in consensus algorithm or other software changes.
- Forks are said to be "soft" or "hard." Unlike a soft fork, a hard fork is not backwards compatible. In essence, a hard fork initiates a brand new blockchain.
- In 2016, following the DAO attack, the Ethereum network, led by its architect Vitalik Buterin, implemented a hard fork – essentially to "restart" the Ethereum blockchain to a point before the DAO attack. This resulted in two blockchains: (new) Ethereum and Ethereum Classic, which some participants continued to use.
- Strong feelings on both sides. Some favored the change; others did not.
- Forking can create arbitrage opportunities, and also may expose one or more branches of a blockchain to attack.
- Forking creates another issue: When a participant holds an option or contract for future delivery, which forked token do they receive?

Oracles

- Oracles are sources of data that smart contracts (blockchain-based code) can access. Oracles provide a link from virtual blockchains back to the real world. Proper execution of smart contracts often depends on oracles to verify conditions or facts.
- The Oracle Problem is defined as the security, authenticity, and trust conflict between third-party oracles and the trustless execution of smart contracts. Simply put, how do you ensure the integrity of oracles?
- Oracle Related Risks:
  - Hacking of the oracle.
  - The oracle breaks or shuts down or fails to respond as expected.
  - The oracle is abandoned.
  - The oracle is involved in fraud.
  - The "mainstream" oracle changes.
  - Connections to the oracle are compromised.

Re-Visiting Pineapples: The Role of Oracles



Patti buys a pineapple grove in Hawaii

Patti worries weather could jeopardize business

Genco offers insurance through a self-executing smart contract

Patti and Genco agree to terms and digitally sign a smart contract

The Smart Contract is stored and operates on Blockchain

Smart Contract Running

Automates monthly payments from Patti to Genco

Automates daily checks for freeze event (Payout if freeze)

Third party authority is known as an oracle.

Inflated Trade Volumes

- Global Bitcoin trading volumes are reported to be billions of dollars per day.
- But much of this volume may not be "real." Some allege that the "vast majority" of reported volume is fake and/or non-economic wash trading.
- One analysis alleges that up to 95% of reported volume is specious.

Additional Considerations

- Many transactions in cryptocurrencies may occur off-chain.
- Understand incentives to inflate trade volume (*e.g.*, token listing fees and driving additional volume to the exchange)

Impacts

- Market Transparency and Integrity
- Direct impact on pricing / "cash markets"
- Carry over impact on any derivative products.

Sources: https://coinmarketcap.com/currencies/bitcoin/ ; https://static.bitwiseinvestments.com/Research/Bitwise-Asset-Management-Analysis-of-Real-Bitcoin-Trade-Volume.pdf

Physical Reality

- A breakthrough in cryptography
  - Quantum computing?
- A local outage
  - California substation
- A downed network
  - AWS

Future Developments

***Reading Tea Leaves,* Harry Herman Roseland (1906)**
Source: https://commons.wikimedia.org

SOVEREIGN TOKENS

REGULATION

?

Takeaways

- Threats in the crypto sector are wide-ranging. They may originate in unexpected ways.
- Left unaddressed, threats can degrade confidence and trust.
- A proactive, comprehensive approach is important to mitigate threats in the crypto sector.
- Investors and users of cryptocurrencies should educate themselves before getting involved. Appropriate disclosure requirements play a vital role.

Questions/Comments?

Contact us: LabCFTC@cftc.gov

Stay Connected: www.cftc.gov/LabCFTC