Private Crypto Assets & Central Bank Digital Currencies

International Monetary Fund
Law & Financial Stability Seminar

September 2018

Agenda

AML vulnerabilities inherent in blockchain technology

Cybersecurity risk considerations and limitations

Market manipulation, market integrity

Financial Connectors (“Gateways”)

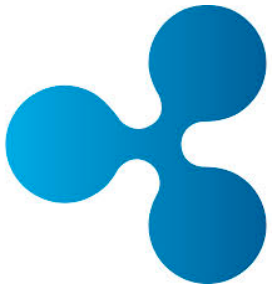
Financial Connectors (“Gateways”)

The Fundamentals

The Fundamentals

- Digital wallets relatively easy to establish

Digital Wallets



rkmLJN5D28dHuH8vZNUZpMC43pEHpocV

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity
- Thousands of cryptocurrency exchanges (‘gateways’) connected to blockchains

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity
- Thousands of cryptocurrency exchanges (‘gateways’) connected to blockchains
- Instant, irreversible transactions

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity
- Thousands of cryptocurrency exchanges ('gateways') connected to blockchains
- Instant, irreversible transactions
- Unlimited potential for structuring / layering funds through multiple wallets

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity
- Thousands of cryptocurrency exchanges ('gateways') connected to blockchains
- Instant, irreversible transactions
- Unlimited potential for structuring / layering funds through multiple wallets
- Use of mixers, tumblers, shufflers, privacy coins

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity
- Thousands of cryptocurrency exchanges ('gateways') connected to blockchains
- Instant, irreversible transactions
- Unlimited potential for structuring / layering funds through multiple wallets
- Use of mixers, tumblers, shufflers, privacy coins
- Issuances of digital "IOUs"

The Fundamentals

- Digital wallets relatively easy to establish
- Anonymity / pseudo-anonymity
- Thousands of cryptocurrency exchanges ('gateways') connected to blockchains
- Instant, irreversible transactions
- Unlimited potential for structuring / layering funds through multiple wallets
- Use of mixers, tumblers, shufflers, privacy coins
- Issuances of digital "IOUs"
- Hardware crypto wallets

Examples of Blockchain-based Activity

01 **LAYERING**

funds through multiple gateways, rapidly moving funds on/off the Blockchain

02 **STRUCTURING**

transactions to avoid known U.S. reporting thresholds

03 **REPORTS**

of hacking and cyber thefts from digital wallets

04 **FUNNELING**

Many-to-one, one-to-many transactions through digital wallets

05 **PHISHING**

Fraudulent emails
And/or websites designed to compromise digital wallets

06 **PYRAMID SCHEMES**

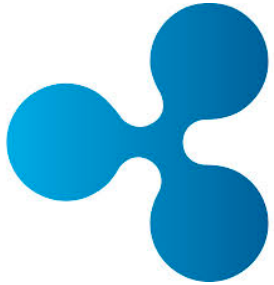
Third-party sales of crypto through illegal marketing schemes

Cybersecurity

Cybersecurity Challenges

- ‘Private Key’ controls access to the funds

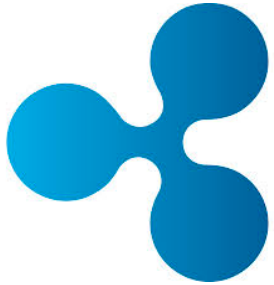
Digital Wallets



rkmLJN5D28dHuH8vZNUZpMC43pEHpocV

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Private Keys



rkmLJN5D28dHuH8vZNUZpMC43pEHpocV

sh8i9d2YRnEjJ3fpFkL8txQSCVo79

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

5KJvsngHeMpm884wtkJNzQGaGErckhHJBGFsvd3VyK5qMZXj3hS

Cybersecurity Challenges

- ‘Private Key’ controls access to the funds
- Security vulnerabilities rarely seen at the blockchain protocol level
  - typically caused by user error

Cybersecurity Challenges

- ‘Private Key’ controls access to the funds
- Security vulnerabilities rarely seen at the blockchain protocol level
  - typically caused by user error
- Target credentials to exchanges’ security protocols

Cybersecurity Challenges

- ‘Private Key’ controls access to the funds
- Security vulnerabilities rarely seen at the blockchain protocol level
  - typically caused by user error
- Target credentials to exchanges’ security protocols
- Custody solutions

Cybersecurity Challenges

- ‘Private Key’ controls access to the funds
- Security vulnerabilities rarely seen at the blockchain protocol level
  - typically caused by user error
- Target credentials to exchanges’ security protocols
- Custody solutions
- Effectiveness of cybersecurity regulation

Example

NYDFS 23 NYCRR Part 500, Section 500.01(d)

"A Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt ***or misuse an Information System or information stored on such Information System"***

"Information System means a discrete set of electronic information resources organized for the collection, ***processing,*** *maintenance,* ***use, sharing, dissemination or disposition of electronic information…. "***

Cybersecurity Challenges

- ‘Private Key’ controls access to the funds
- Security vulnerabilities rarely seen at the blockchain protocol level
  - typically caused by user error
- Target credentials to exchanges’ security protocols
- Custody solutions
- Effectiveness of cybersecurity regulation
- Cyber attacks on a global scale

Market Integrity

Market Integrity

- Off-ledger exchanges

Market Integrity

- Off-ledger exchanges
- Dark Pool trading

Market Integrity

- Off-ledger exchanges
- Dark Pool Trading
- Whale Trades

Market Integrity

- Off-ledger exchanges
- Dark Pool trading
- Whale trades
- Wash Trading

Market Integrity

- Off-ledger exchanges
- Dark Pool trading
- Whale trades
- Wash Trading
- Pump and Dumps

Market Integrity

- Off-ledger exchanges
- Dark Pool trading
- Whale trades
- Wash Trading
- Pump and Dumps
- Shilling

Closing Thoughts

- Systematic, global approach to cryptocurrency regulation
- New protocols for governance of blockchain tech
  - national variability but not tied to any specific geography
  - rooted in a multi-stakeholder model
  - emphasizing ethics and security as core values
- Collaborative cross-border regulatory and law enforcement partnerships
- Information sharing (trends, typologies, etc.) between industry and agencies
- More education
  - regulators
  - lawyers
  - bankers

Questions?

Antoinette O'Gorman
Crypto / Fintech Compliance Advisor