CHRYSALIS

DIGITAL ASSET EXCHANGE

Thomson Reuters Conference

Manifest Destiny: Risk, Opportunity & Reward Around Digital Currencies

New York City April 14-15, 2022

Chrysalis: Deep domain knowledge

Paul McCarthy
CEO
Founder

Doug McCalmont
CCO
Co-Founder

Joseph Bognanno
COO
Co-Founder

Dr. Rula Sayaf
CTO
Co-Founder

Combined 75+ plus years of experience committed to venture

Combined Skills and Expertise			
Government & Law Enforcement Relationships	Forensic Technologies	Cyber Security	Cryptography
Financial Services & Insurance Relationships	Crypto Currency & Digital Assets	Confidential computing	AI & ML
Regulation & Compliance	Due Diligence	Data Protection & Privacy	Quantum Computing

Chrysalis

Bringing trust to digital assets by ensuring those **risks** are **minimized**, while **unlocking** liquidity for those who have fallen victim to a hack, theft or key loss.

Chrysalis – Research and Development

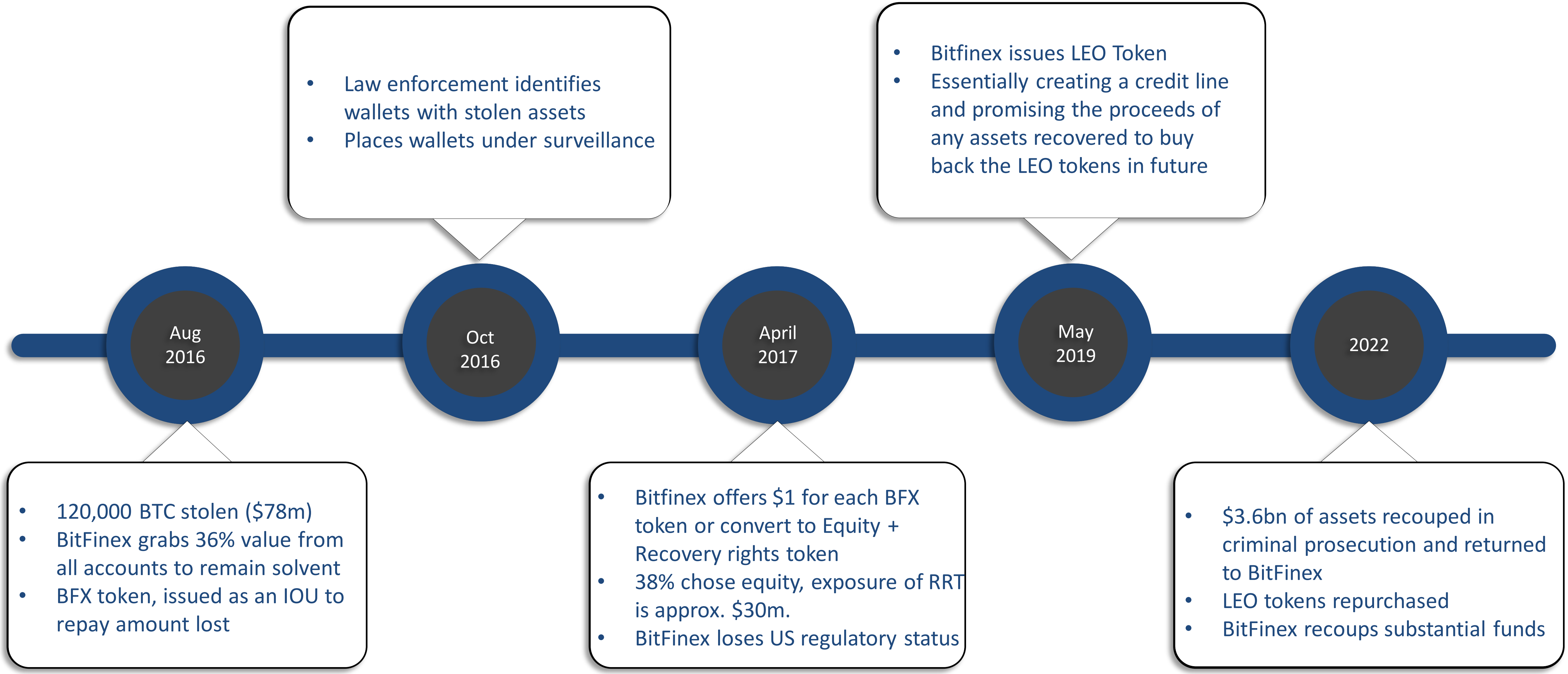
Focus Areas

- Understand threats posed by Post-Quantum Cryptography (PQC) to Blockchain and Digital Assets
- Monitor the advances of PQC to:
  - Understand application of PQC capability to redeem Distressed Digital assets
  - Protect Distressed assets and Chrysalis tokens

In collaboration with

- KULeuven PQC Team & Security Researchers:
  - Member of the National Institute of Standards and Technology (NIST) PQC developing team

BitFinex Hack



Aug 2016

- 120,000 BTC stolen ($78m)
- BitFinex grabs 36% value from all accounts to remain solvent
- BFX token, issued as an IOU to repay amount lost

Oct 2016

- Law enforcement identifies wallets with stolen assets
- Places wallets under surveillance

April 2017

- Bitfinex offers $1 for each BFX token or convert to Equity + Recovery rights token
- 38% chose equity, exposure of RRT is approx. $30m.
- BitFinex loses US regulatory status

May 2019

- Bitfinex issues LEO Token
- Essentially creating a credit line and promising the proceeds of any assets recovered to buy back the LEO tokens in future

2022

- $3.6bn of assets recouped in criminal prosecution and returned to BitFinex
- LEO tokens repurchased
- BitFinex recoups substantial funds

BitFinex: How Chrysalis could have helped

Customers

1. Not forced to take a 36% haircut
2. Retain visibility on their assets as information became available with investigation
3. Minimize legal costs for asset recovery
4. Option to sell assets rather than wait for recovery
5. Benefit from appreciation

BitFinex

Could have prevented:

1. Creation, maintenance and repurchase of RRTs
2. Client financial losses of $850 million
3. Regulatory & law enforcement scrutiny
4. Financial penalty of $18.5 million
5. Exile from the US market
6. Reputational damage

Law Enforcement

1. Provide transparency to those impacted in the process
2. Streamline the process of returning funds to customers impacted.

Ronan Network Hack (Bridge Vulnerability)

1. $600 million plus stolen in USDC and ETH
2. Ronan Bridge connects Ethereum to the Ronan Chain
3. The nine bridge validators were responsible for manually examining the assets on the bridge
4. It took six days for the hack to be discovered (due to manual operations)
5. Social engineering was used to manipulate the majority of validators (five)

Because security surrounding monolithic entities is growing in sophistication, links between those monolithic entities are now the "targets" of bad actors.

The Chrysalis DAE protocol can dramatically improve the results of the Ronan hack

- Retain visibility on "missing" assets
- Minimize legal costs
- Option for victims to sell rights to missing assets
- Victims receive full benefit of financial appreciation