RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M02

Cryptocurrency Attacks, Security challenges, and Management Tools

Diogo Monica (@diogomonica)

Bitcoin

FOX Business
@FoxBusiness
Follow

.@tylerwinklevoss: "Bitcoin is backed by cryptography, mathematics, and one of the largest computer networks in the world... It's also open source and can evolve and grow over time."

4:29 PM - 11 Dec 2017

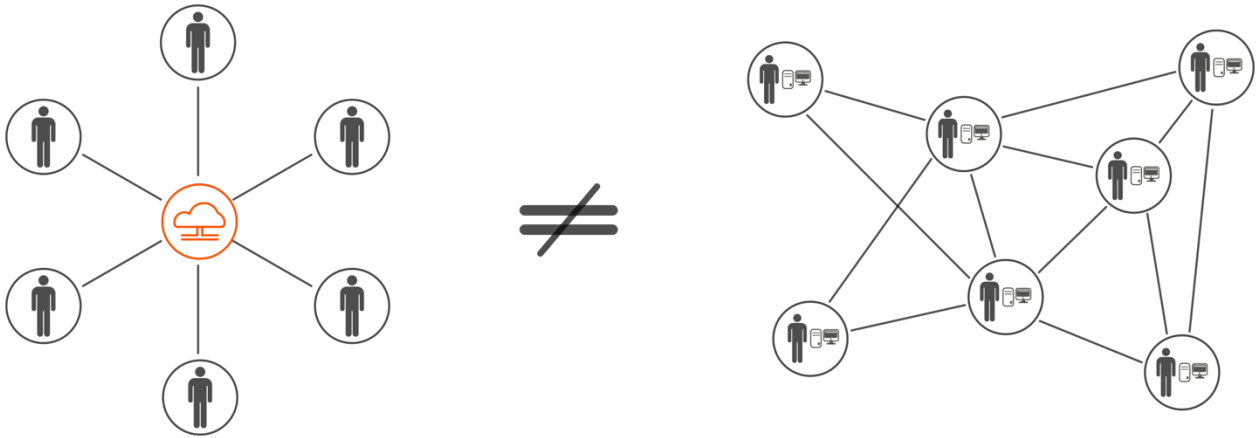
25 Retweets 61 Likes

13 25 61

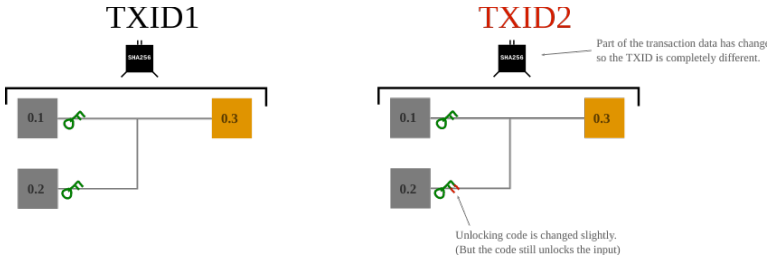
PKI

Public key infrastructure is **also** backed by cryptography.

The main difference



Attacks on bitcoin



Implementation bugs

VULNERABILITIES

CVE-2010-5141 Detail

Description

wxBitcoin and bitcoind before 0.3.5 do not properly handle script opcodes in Bitcoin transactions, which allows remote attackers to spend bitcoins owned by other users via unspecified vectors.

Protocol issues

$$s = k^{-1}(z + rd_S) \bmod n \;\Rightarrow\; d_S = r^{-1}(sk - z) \bmod n$$

VULNERABILITIES

CVE-2010-5139 Detail

Description

Integer overflow in wxBitcoin and bitcoind before 0.3.11 allows remote attackers to bypass intended economic restrictions and create many bitcoins via a crafted Bitcoin transaction.

CROWDFUND INSIDER

Hacked! Tether Claims Theft of $30M+ in Digital Currency

November 21, 2017 @ 6:19 pm By JD Alois

Crowdfund Insider
JD Alois
Hacked! Tether Claims Theft of $30M+ in Digital Currency
0m 0s
1m 36s
1 x
Rate SpeechKit

ROBERT MCMILLAN BUSINESS 03.03.14 06:30 AM

THE INSIDE STORY OF MT. GOX, BITCOIN'S $460 MILLION DISASTER

Mark Karpeles, the chief executive officer of bitcoin exchange Mt. Gox, center, is escorted as he leaves the Tokyo District Court this past Friday.

PHOTO: TOMOHIRO OHSUMI/BLOOMBERG VIA GETTY IMAGES

BITCOIN

Cyberattack temporarily hits bitcoin exchange Bitfinex

- Major digital currency exchange Bitfinex reported a distributed denial-of-service attack that temporarily took the system offline Monday.
- Bitcoin dipped below $11,000, but within an hour, Bitfinex tweeted that operations were returning to normal.
- The latest technical difficulties followed several cyberattacks on digital currency exchanges in June, including Bitfinex.

Evelyn Cheng | @chengevelyn
Published 12:40 PM ET Mon, 4 Dec 2017 | Updated 3:01 PM ET Mon, 4 Dec 2017

CNBC

Dado Ruvic | Illustration | Reuters

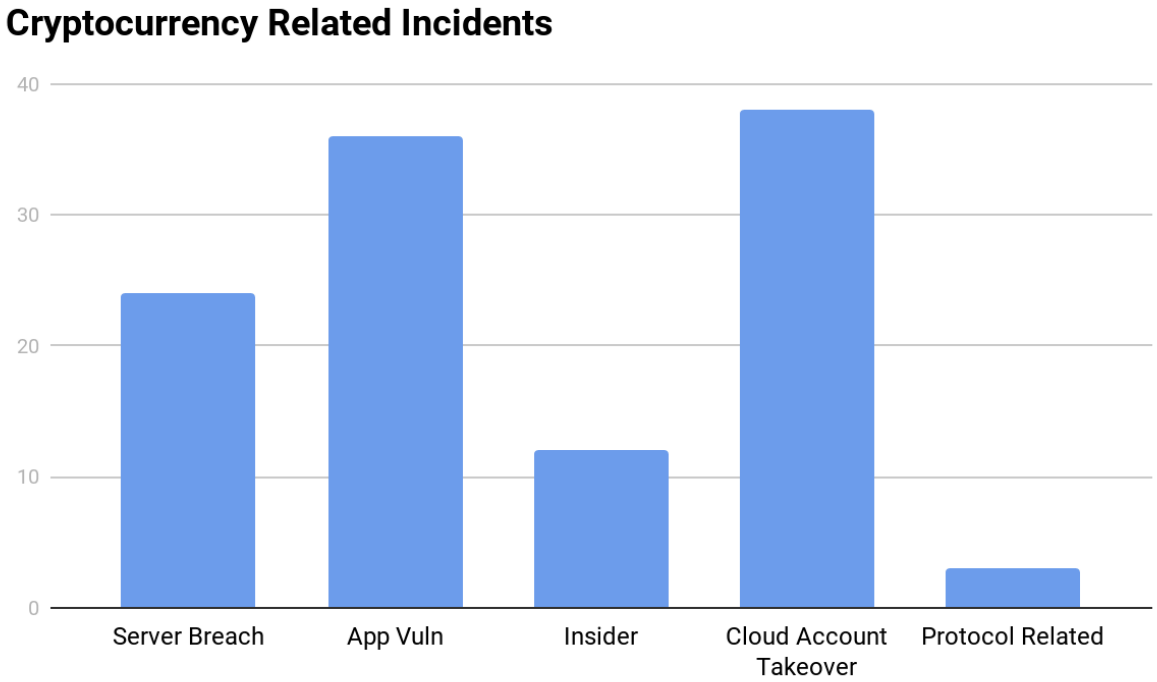
Photo illustration of Bitfinex cryptocurrency exchange website.

FINANCE • CRYPTOCURRENCY

How to Steal $500 Million in Cryptocurrency

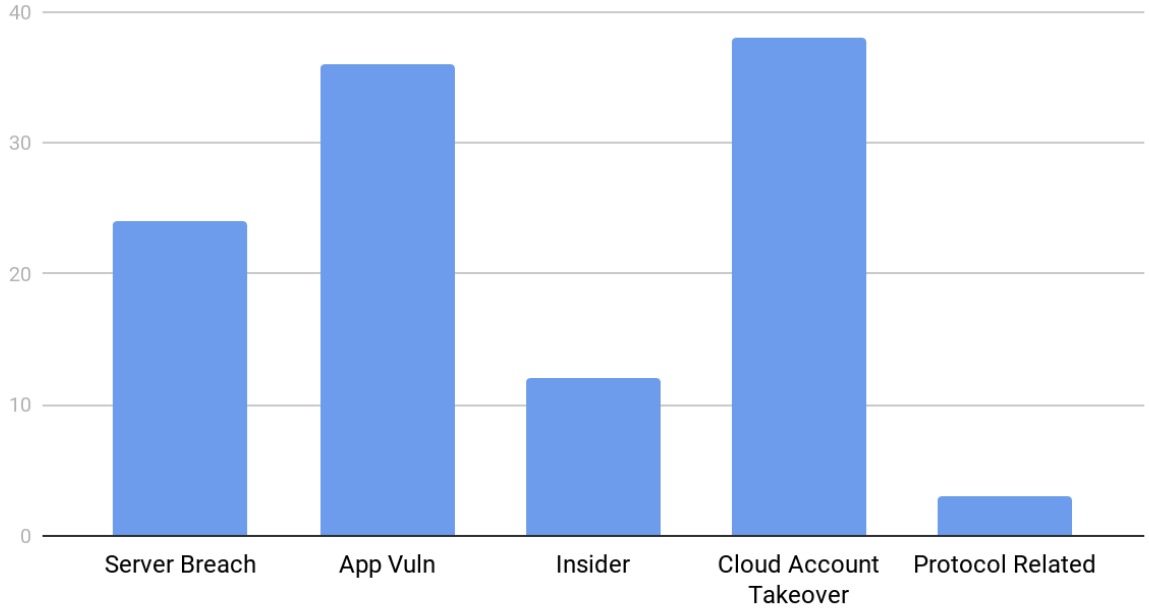

APRIL MAY JUN JULY AUGUST SEPTEMBER
DN
NB
SP

Cryptocurrency Related Incidents



magoo.github.io/Blockchain-Graveyard

Infosec Incidents?



Example 1: Blackwallet

1. Hacker(s) accessed the company's **hosting provider account**.
2. After gaining access, they **changed the DNS entry** to point to a malicious replica of the website.
3. Stole the funds of users that used the compromised website.

Example 2: Nicehash

1. Hacker(s) were able to *infiltrate our internal systems through a* ***compromised company computer***.
2. After VPN login, *learned and* ***simulated the workings of our payment system*****.**
3. Managed to steal funds from accounts.

Example 3: Bitpay

1. Hacker(s) were able to **spearphish the CFO** and acquired working credentials.
2. These credentials were used to **communicate to the CEO** and **request multiple large transfers** ($1.8M worth of BTC).
3. BTC moves to attacker's account.

Example 4: Poloniex

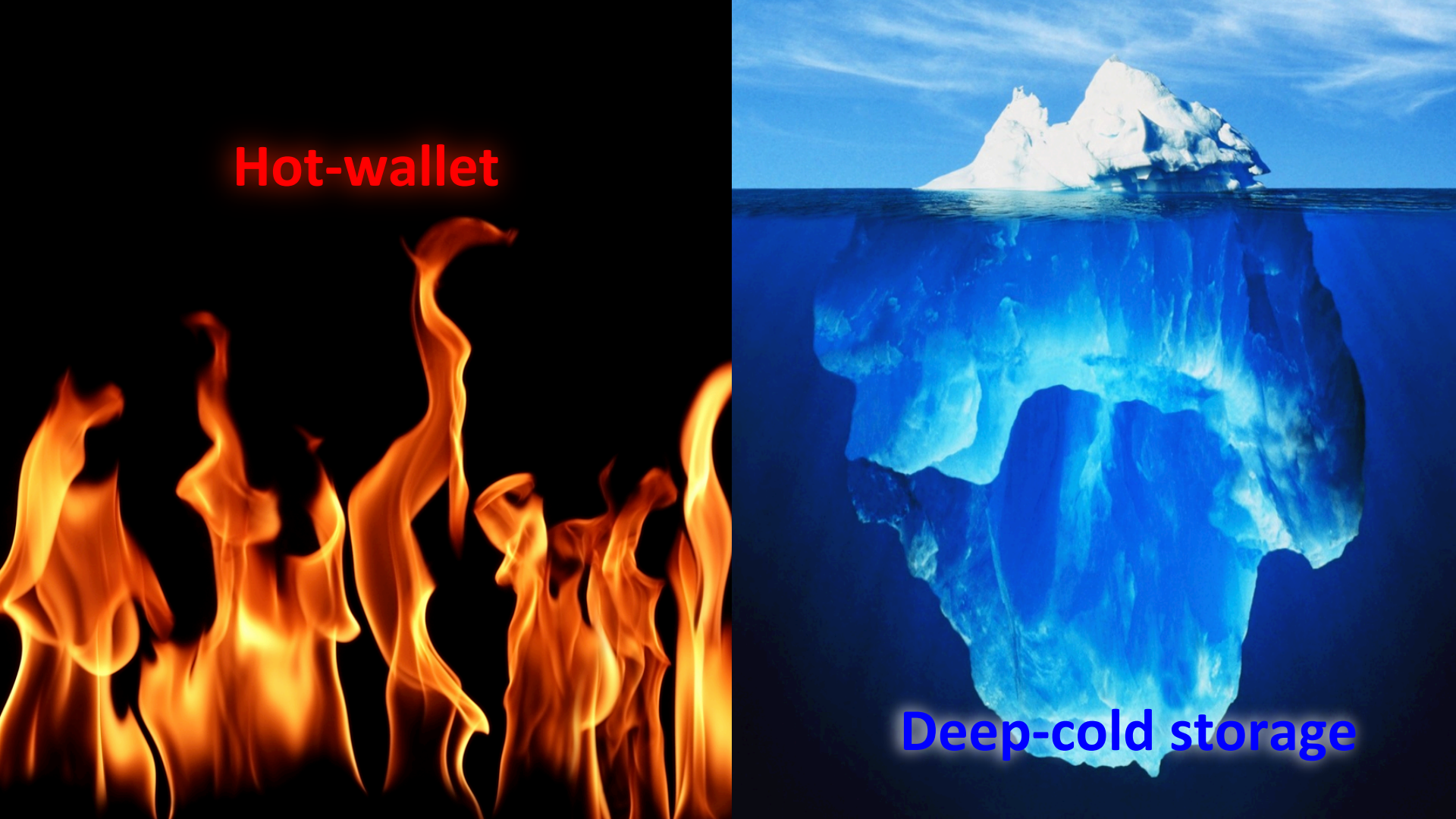
1. Hacker(s) discovered a **race-condition** on the withdrawal operation.
2. This race condition was exploited by **generating multiple simultaneous withdrawals** that got processed simultaneously.
3. While this resulted in negative balances, it still got valid insertions into the database and withdrawals would go through.

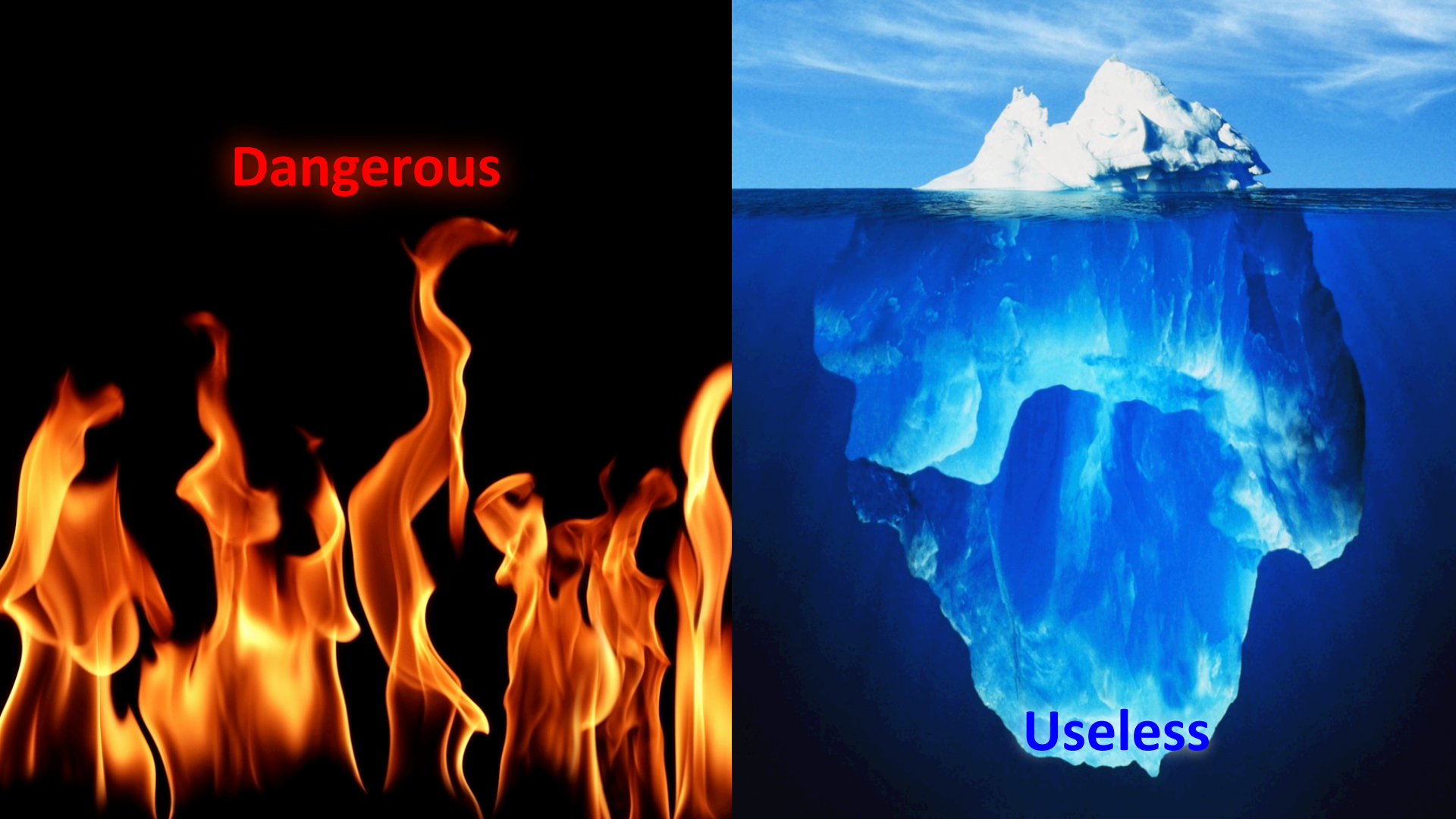
Example 5: Shapeshift

1. Hacker(s) **buys information from previous employee** (username/ passwords, valid SSH keys).
2. After accessing company's servers attackers **installed a rootkit**.
3. With unfettered access to the infrastructure, attackers were able to steal 315 BTC.

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.

Gene Spafford


Hot-wallet
Deep-cold storage


Dangerous
Useless


457
507
557
458
509

What is different?

- Attacker model must be **embargoed nation states**.
- Compromise of keys can't be solved with key-rotation.
- No such thing as revocation/transaction reversal.
- System must remain safe even when attackers have administrative control of every single host.
- No single individual can have the ability to authorize any sensitive operations.

What is different?

- A lot easier to estimate monetary impact of a breach :)

How can we do this?

- Native multi-signature support.
- Time-locks.
- Blockchain-specific properties.

Same fundamentals

- HSMs
- SDLC Security
- Minimize attack surface
- Reverse uptime

The protocols should help too

- Key splitting
- Implementations in low level languages (C, C++)
- Audited signing code
- Support for external signing oracles

Summary

- Cryptocurrencies can operate in adversarial environments.
- Attacks are targeted at the points of centralization: exchanges.
- No new techniques being used: same attacker playbook.
- Deep-cold storage is not a realistic solution for the problem.
- Attacker model should be embargoed nation states: root on every server.

Conclusion

- We've known how to secure digital assets for a long time, but we finally have a real, measurable, incentive to do so.