

RSA®Conference2018

San Francisco | April 16–20 | Moscone Center



#RSAC

SESSION ID: TV-T04

INFOSEC 101 FOR ICO'S: HOW THE MOST "SECURE" TRANSACTION PROTOCOL FAILED

Ira Goldstein

SVP Global Tech Ops
Herjavec Group
@HerjavecGroup

Course Outline



The Most Lucrative, Fastest Executed and Least Traceable Hack

- Your primer on how \$500 million was lost through Initial Coin Offering hacks

Lack of Regulation and Problem of Attribution are *Features* of This System, not *Flaws*

- Explore how the feature set of Blockchain applications is anathema to security

The Rules of Engagement Start and End With Social Engineering

- Driven by FOMO to likely get scammed, fund crime or both



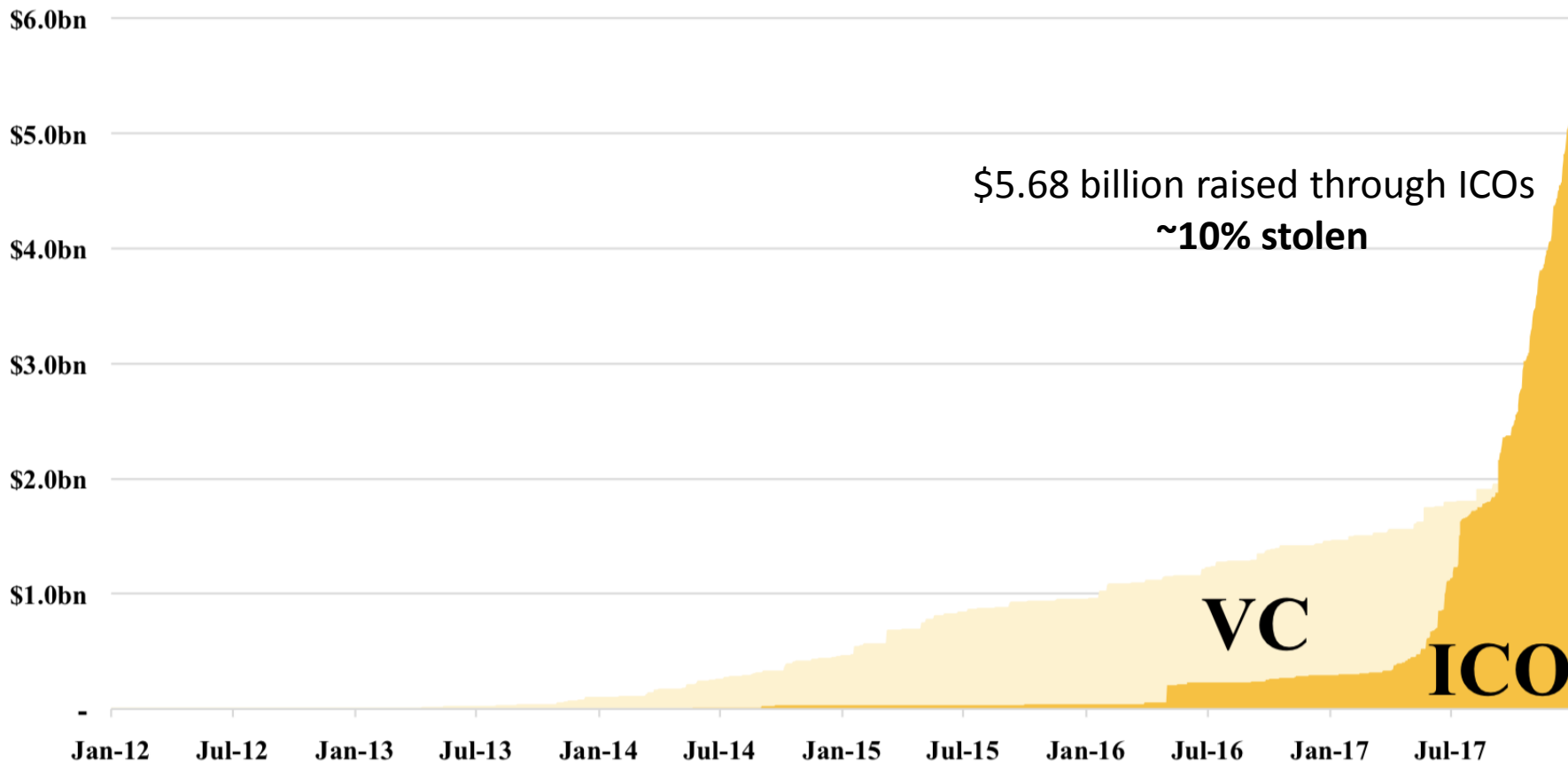
How the world thinks of Blockchain



How the world should think of Blockchain

All-Time Blockchain Funding

Cumulative VC Cumulative ICO



650 years ago...



#RSAC



Cash paid Sep: 23 rd 1848	14
Mr. Digley	1 5 "
Mr. Jarvis	" 14 6
Mr. W. Lee to Mr. C. W.	3 " "
Dr. for Self	1 " "
Parker	1 2 6
Mr. Parrott Eight Pound Candles	" "
Mr. Lachoual	15 8 "
Jas. Lord	4 2 6
Mr. Saunders	3 " "
Manue	1 " "
Childley as for Book	7 1 4
James	" 12 "
Mr. Richler	4 " "
Sep 27	
Mucking for week ending Sep 16 th	4 4 6
Dr. for Dr. Sep 23	4 4 3

Your DB Admin...

217

TECHNICAL
SUPPORT

SNL

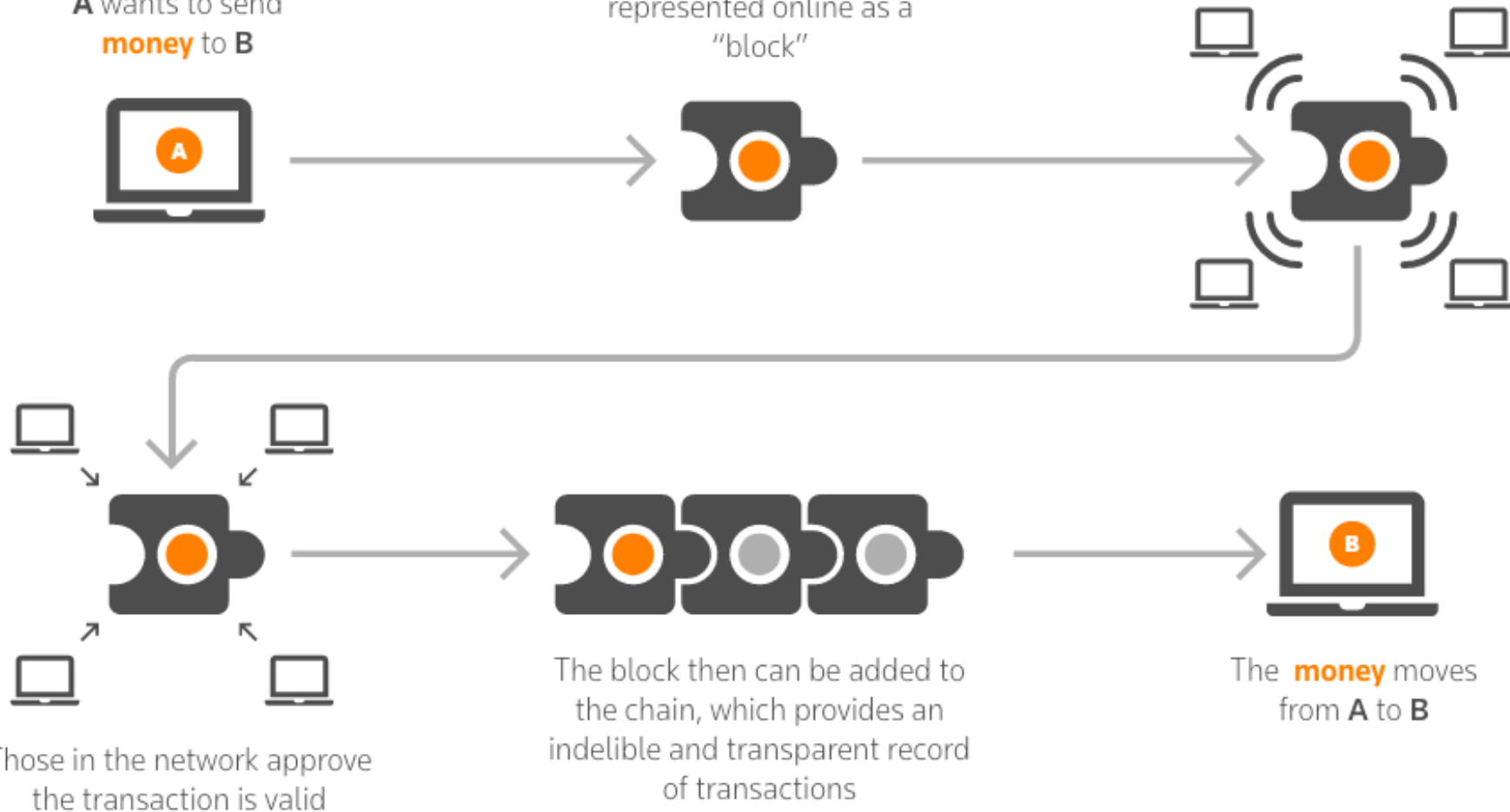


17 years later...

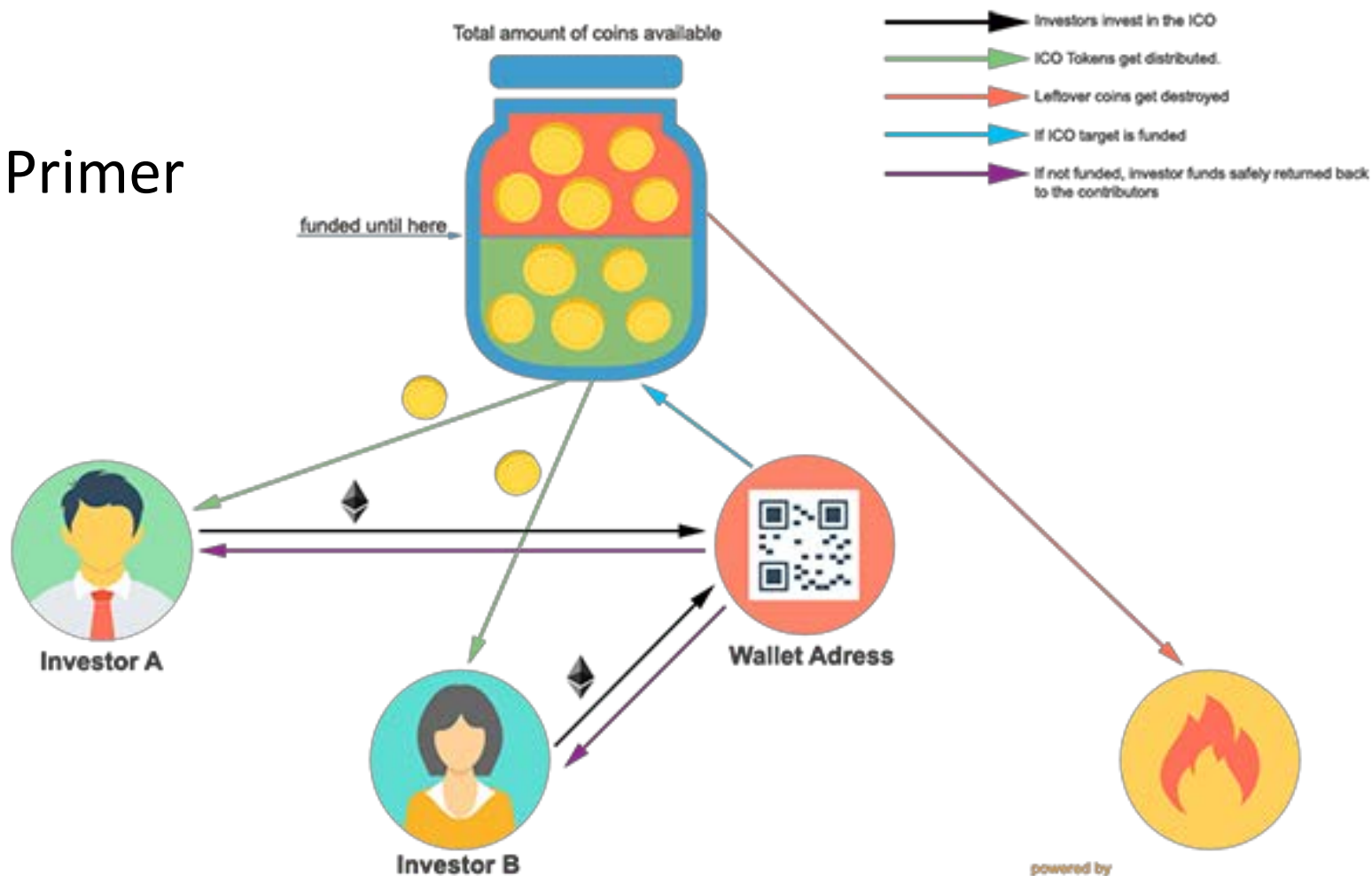
The block is broadcast to every party in the network

A wants to send **money** to B

The transaction is represented online as a "block"



ICO Primer



What has all that progress delivered?



- Anonymity!
- No regulation!
- No central authority!

∴ information security nightmare


Notable ICO Hack #1





- Enigma: September 2017
 - The Dream: Quantitative Trading Platform on Cryptocurrency Markets
 - Equivalent of 1492 ETH stolen
 - Converted to USD: ~\$500k lost (calculated at time of loss)
 - The ICO led by “MIT graduates and researchers”
 - Slack account to communicate ICO updates was compromised
 - Website, mailing list and Slack leveraged for social engineering

'Bullseye' on your back








Sign in

Get started



Enigma Project

Follow

Our protocol is focused on fixing privacy and scalability for blockchains. We build Catalyst, a platform for data-driven crypto investing and trading. \$ENG

Jul 17, 2017 · 4 min read

Don't Get CoinDashed — How to Secure Your Token Sale

In the past year, token sales have time and again proven their merit as an effective method to secure funding and bootstrap a community surrounding an open source project. But like anything new and exciting (that involves large sums of money), token sales suffer from severe growing pains. Earlier today, the anticipated CoinDash token sale suffered an unfortunate [hack that led to the theft of \\$7m](#) (about half of the proceedings raised).

While token sales are an amazing new tool to democratize funding, they also put a tremendous amount of pressure on the organizations initiating them to properly manage the process. After all, raising tens of millions of dollars publicly paints a fairly big 'bullseye' on your back.

Blockchain etches hacks in indelible history



Warning! The Enigma.co webpage at <https://www.enigma.co/presale/> (*now taken down*) was compromised (August 21, 2017) and this address was used in the hack. Do not send your funds here!

Overview | Fake_EnigmaPhish



ETH Balance: 0.11028042628856924 Ether

ETH USD Value: \$90.48 (@ \$820.48/ETH)

No Of Transactions: 216 txns

Misc



More Options



Address Watch

Add To Watch List

Token Tracker

View Tokens (\$33.65)

13

Notable ICO Hack #2



- Veritaseum: July 2017
 - The Dream: Software and Network to Facilitate Decentralized Banking
 - 36,000 tokens stolen, representing 0.07% of offering
 - \$8 mil. Worth of VERI token traded to ETH (worth ~\$18 million at peak)
 - Third-party Supplier with access to token wallets had credentials compromised
 - Stolen tokens sold at discount to interested parties

Breach Disclosure in the world of ICOs



#RSAC

#1917

Reggie Middleton

Full Member



Online

Activity: 131

Merit: 100

UltraCoin "Smart" Derivatives:
The Future of Money



Re: VERITASEUM DISCUSSION THREAD

July 24, 2017, 01:05:34 PM

We were hacked, possibly by a group. The hack seemed to be very sophisticated, but there is at least one corporate partner that may have dropped the ball and be liable. We'll let the lawyers sort that out, if it goes that far.

Although I hate to see assets stolen, and I hate thieves, the incident proved both the resilient demand for our tokens and the utility of the decentralized exchange EtherDelta.

The hacker(s) made away with \$8.4M worth of tokens, and dumped all of them within a few hours into a heavy cacophony of demand. This is without the public knowing anything about our last traction.

I would like to make it known that we had the option to fork VERI, but chose not to. At the end of the day, the amount stolen was miniscule (less than 00.07%) although the dollar amount was quite material.

Another point that I would like to make clear is that Veritaseum tokens are software that represent our knowledge, advisory and consulting skills, products and capabilities. Without the Veritaseum team, the tokens are literally worthless! If someone were to someone confiscate 100% of the available tokens, all we need to do is refuse to stand behind them and recreate the token under a new contract. Again, we aren't selling currencies, we aren't selling securities. We are selling capabilities, and ability for those capabilities to connect parties P2P for the autonomous transfer of value. You can get away with a large securiteis heist, or a large currency heist. The Veritaseum team is what powers the value behind the Veritas token. A large theft of those tokens after a fork is as valuable as stealing 90M empty plastic cups.

The "marketcap" as the media likes to refer to, may seem high to those who don't understand how we employ platform economics, but those who understand should see that number as drastically undervalued. We have a roadshow for the NYC & Connecticut hedge funds next week. The Sr. partner of distressed credit of one of the world's largest funds specifically took the meeting after hearing about what we are doing. "This is big, very big" (that is an exact quote from the person who arranged the meeting, who is a 40 yr veteran of Wall Street, a literal brand name know by nearly every experienced professional - someone who had aggressively jumped on board team Veritaseum to assist in business development), for we are simultamesouly lining up private and sovereign credits to Veritize. This is in addition to what may be our final meeting with one of the world's top ten securities exchanges to use our product. That is in addition to our Veritizing a medical practice as a showcase for doctors and healthcare biz pros around the world to emulate (using Veritas, of course). Think of us just capturing 50 basis points of all of the medical practices and related healthcare businesses in the world
<https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-2017-health-care-outlook-infographic.pdf>
Which will actually scale exponentially with out financial industry dealings (assuming we can capture .02% of that
<http://www.investopedia.com/ask/answers/030515/what-percentage-global-economy-comprised-financial-services-sector.asp>
We have already landed the Jamaican Stock Exchange as VERI client just 30 days after the initial token offering. Actually, quite amazing...

Now, you can see how inconsequential the mere hack of a few million dollars

Disclosure Highlights



- “We were hacked”
- “The hacker(s) made away with \$8.4M”
- “The amount stolen was miniscule...although the dollar amount was quite material”
- “Now, you can see how inconsequential the mere hack of a few million dollars”

Notable ICO Hack #3



- CoinDash: July 2017
 - 28 day sale with a \$12 mil. cap for a utility token on a crypto trading network
 - 3 minutes after launch, 43,500 tokens lost to hackers
 - Worth \$7.4 mil. USD at the time – hack and hold – worth \$43 mil. USD at peak
 - Fraudulent Ether wallet address maliciously placed on Wordpress site
 - No visibility into what was stolen from whom
 - All subscribers received tokens as paid
 - Dilution not reported in public media
 - UPDATE: 30,000 tokens returned toCoinDash as of February 2018

"WE ARE HACKED"



#RSAC

mplus 1:59 PM
@channel It's time. Good luck! www.coindash.io only trusted source!
👍 10 🙄 11 🤔 4 🤔 3 🤔 3 🤔 4 🤔 3 🤔 7 🤔 4 🤔 2

jf4nathan 2:00 PM
joined #announcements. Also, @coindash_admin joined, @geoff joined.

mplus 2:03 PM
@channel WEBSITE HACKED
🤔 74 🙄 16 🤔 25 🤔 34 🤔 29 🤔 16 🤔 9 TM 5 🤔 25 🤔 6 🤔 12 🤔 8 🤔 8 🤔 7 🤔 8 🤔 4 🤔 7 🤔 4 🤔 6 🤔 4 🤔 9 🤔 5 🤔 5 🤔 3 🤔 2 🤔 2 🤔 1 🤔 1
don't believe the website.

hahack26 2:05 PM
joined #announcements. Also, @hnam31190 joined.

ram 2:07 PM
DONT SEND ETH TO THE SITE ADDRESS!!! WE ARE HACKED
🤔 62 🙄 47 🤔 18 🤔 18 🤔 20 🤔 48 🤔 14 🤔 13 🤔 10 🤔 9 🤔 25 🤔 11 🤔 11 🤔 12 🤔 10 🤔 12 🤔 7 !? 14 X 14 🤔 10 🤔 14 🤔 7 🤔 10 🤔 4 🤔 4 🤔 3 🤔 3 🤔 5 🤔 2
❤️ 3 🤔 3 🤔 3 🤔 1 🤔 2 🤔 1 🤔 1 🤔 1 🤔 3 🤔 2 🤔 1 🤔 1 🤔 1

mplus 3:35 PM
Needless to say the token sale is done... The official announcement is coming.
🤔 8 🤔 18 🤔 13 🤔 6 🤔 4 🤔 8 🤔 10 🤔 13 🤔 12 🤔 9 🤔 6 🤔 8 🤔 7 🤔 4 🤔 5 🤔 5 🤔 3 🤔 6 🤔 7 🤔 6 🤔 4 🤔 3 🤔 3 🤔 5 🤔 3 🤔 5 ? 1 🤔 2

The Downside of Anonymity



Secure | https://docs.google.com/forms/d/13S2gbsO2eHcqk7MmAwLF9Ky1k4E7EUE9jnry79GR50U/viewform?ts=596cfbdf&edit_requested=true

CoinDash Token Sale Follow Up

Please help us to investigate the status and solve the issues from the token sale by providing following information.

请帮助我们持续调查并解决此次代币发售的现状与问题。在下方问卷中提供你参与发售的相关信息。

* Required

Email | 邮件地址 *

Your answer

Your wallet address | 你的钱包地址 *

Your answer

Amount of ETH sent | 发送的ETH数量 *

Your answer

Your TX number (Proven transaction number) | 你的交易ID (请提供TXID) *

Your answer

The Upside of a Resilient Ecosystem?



TTPs (the “what and how”): Best Guesses



- **CoinDash**

- Wordpress vulnerability; targeted early ICO investors

- **Veritaseum**

- Third-party supplier credential compromise
- Leveraged frothy resale market

- **Enigma**

- Executive email compromise, possibly through phishing
- Admin access to platforms with no MFA drove compromise

Way Forward: “Crypto Ice Age”

