RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-R11

How Bad Incentives Led to Crypto-Mining Malware, and What to Do about It

Sandy Carielli

Director of Security Technologies
Entrust Datacard
@sandycarielli

Agenda

- Incentives and “Side Effects”
- Blockchain and Incentives
- Cryptojacking
- Potential Solutions?
- Summary and Take Aways

RSAConference2019

Incentives and “Side Effects”

“Freakonomics” on Incentives…

Freakonomics The Movie (2010)

“Side Effects” … or Just “Effects”?

“SIDE EFFECTS ARE NOT A FEATURE OF REALITY BUT A SIGN THAT OUR UNDERSTANDING OF THE SYSTEM IS NARROW AND FLAWED.”

John D. Sterman, Business Dynamics

RSAConference2019

So, What Does This Have to Do With Blockchain?

Decentralization Drove Proof of Work

"…a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify…" (Bitcoin Wiki)

PROOF OF WORK

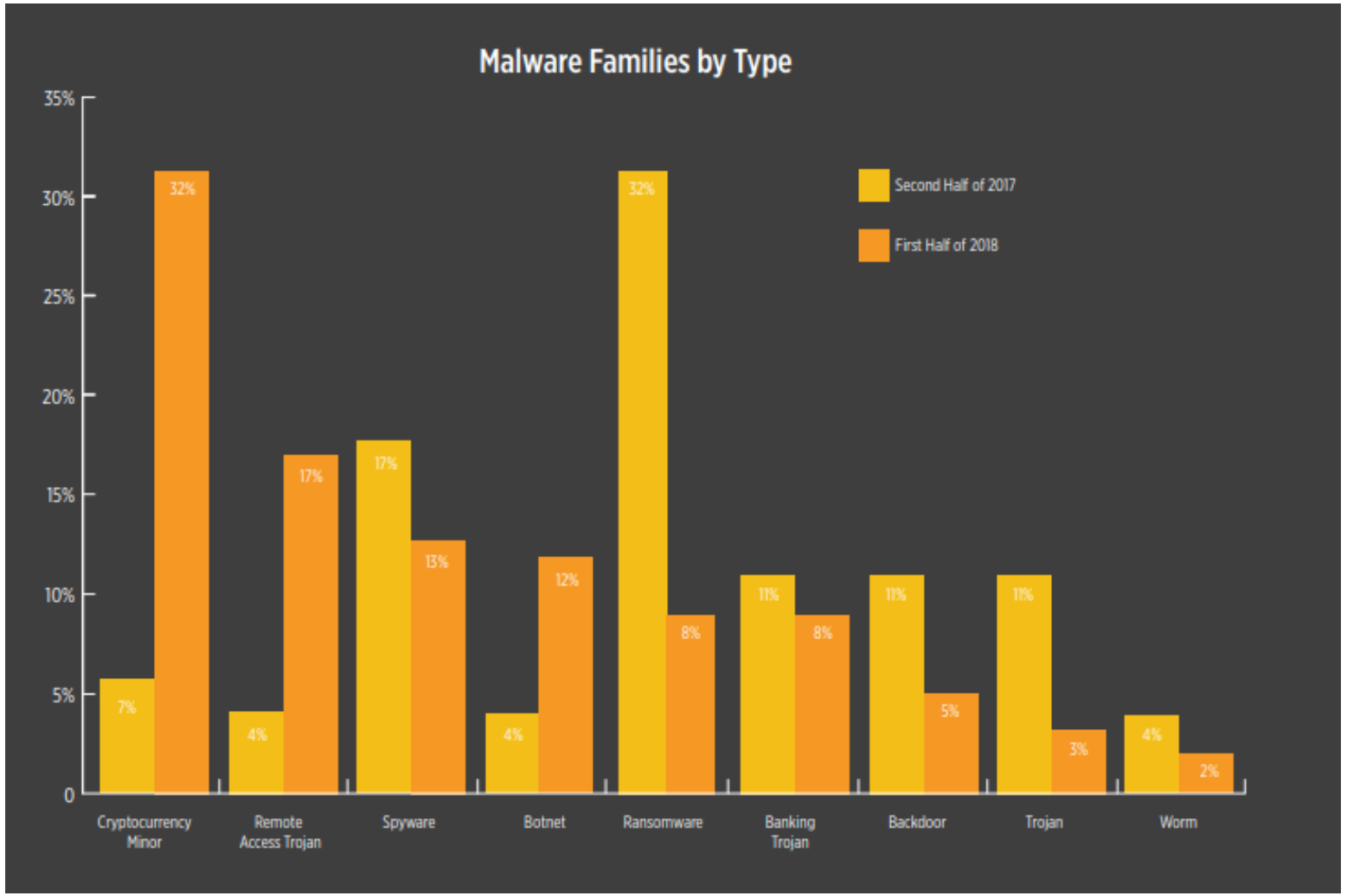
Proof of Work Incentive Schemes

Platform	Proof of Work Scheme	Incentive
Bitcoin	Hashcash	12.5 bitcoin per mined block (halves every 210,000 blocks)
Ethereum	Ethash	Five (5) ether per mined block
Zcash	Equihash	12.5 ZEC per mined block (halves every 840,000 blocks)

RSAConference2019

Welcome to Cryptojacking!

Cryptomining Malware Exploded in 2018



Skybox Security Vulnerability and Threat Trends Report 2018 Mid-Year Update (https://lp.skyboxsecurity.com/WICD-2018-07-Report-VT-Trends-MY_03Asset.html)

How Profitable Is Cryptojacking?

High Potential

"…a botnet of 100,000 bots carrying out browser-based mining, running continuously for 30 days, could make $30,000, or a file-based miner could make $750,000. The potential is there for big results in cryptojacking, but scale is a key part of the equation."

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-cryptojacking-modern-cash-cow-en.pdf

Lower in Reality?

"With a hash rate of 80 H/s and CoinHive's payout ratio8 , a miner earns about 5.8 USD per day and website on average, which supports our observation that web-based cryptojacking currently provides only limited profit."

https://arxiv.org/pdf/1808.09474.pdf

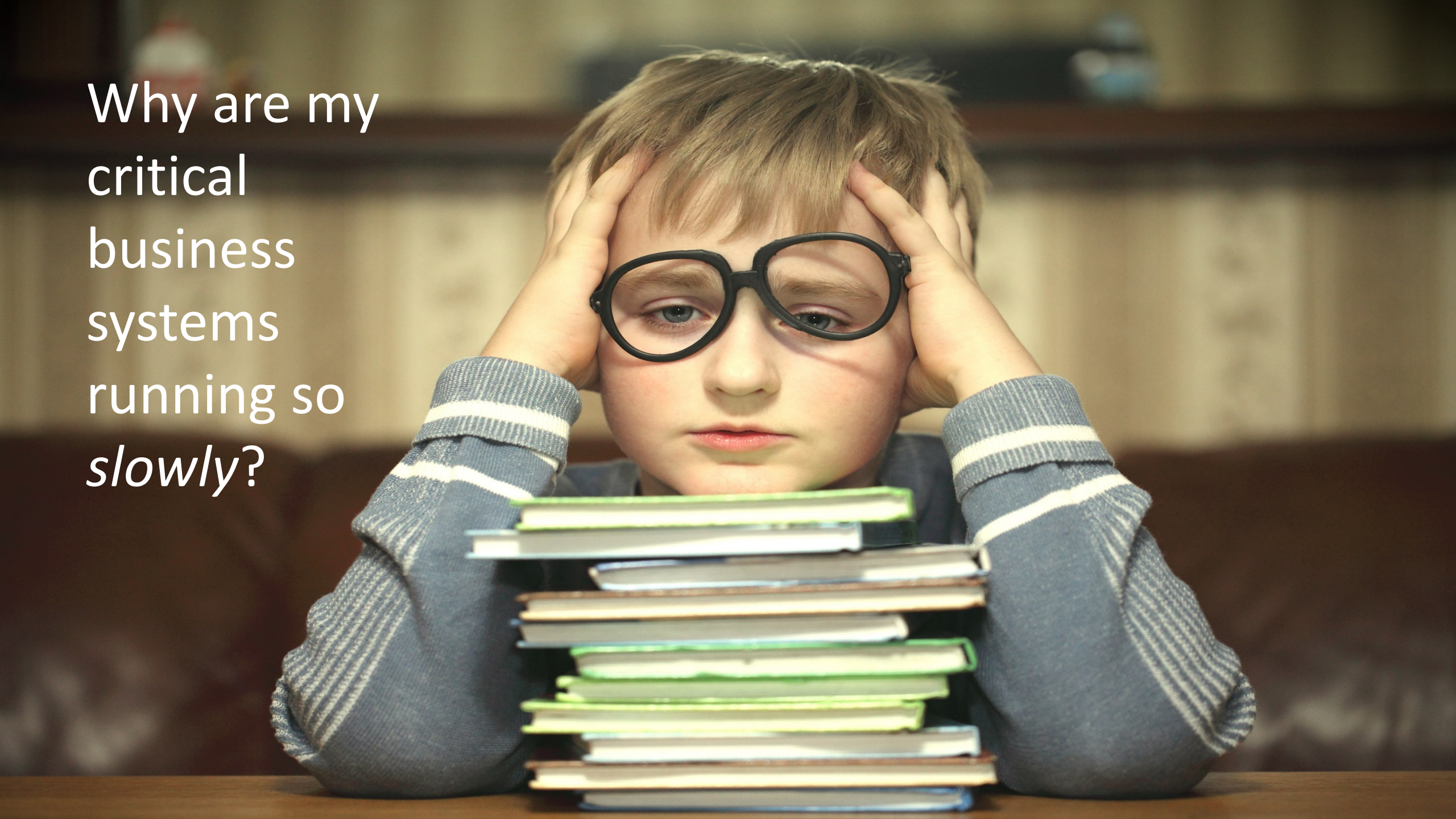
Crypto Mining Malware vs. Ransomware

Crypto Mining Malware

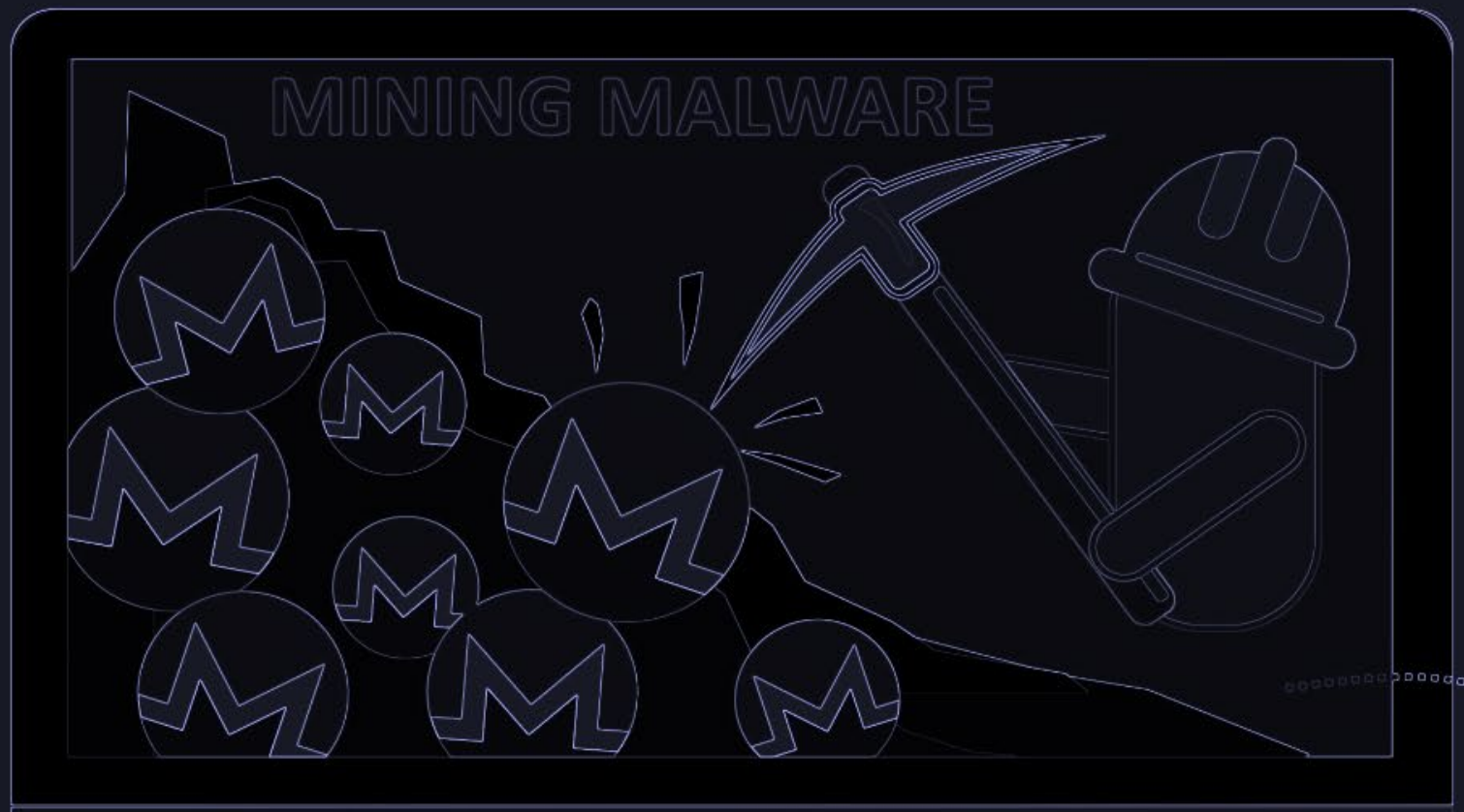
- Low visibility - could sit on a system for months
- Low to moderately disruptive
- Victim does not pay directly … but will bear costs of resource misuse

Ransomware

- Highly visible almost immediately
- Highly disruptive
- Victim pays the ransom (or not) – financial impact apparent


Why are my critical business systems running so *slowly*?


“Why did our power and cloud usage bills go up 40% last month, when our revenues were flat?!?”

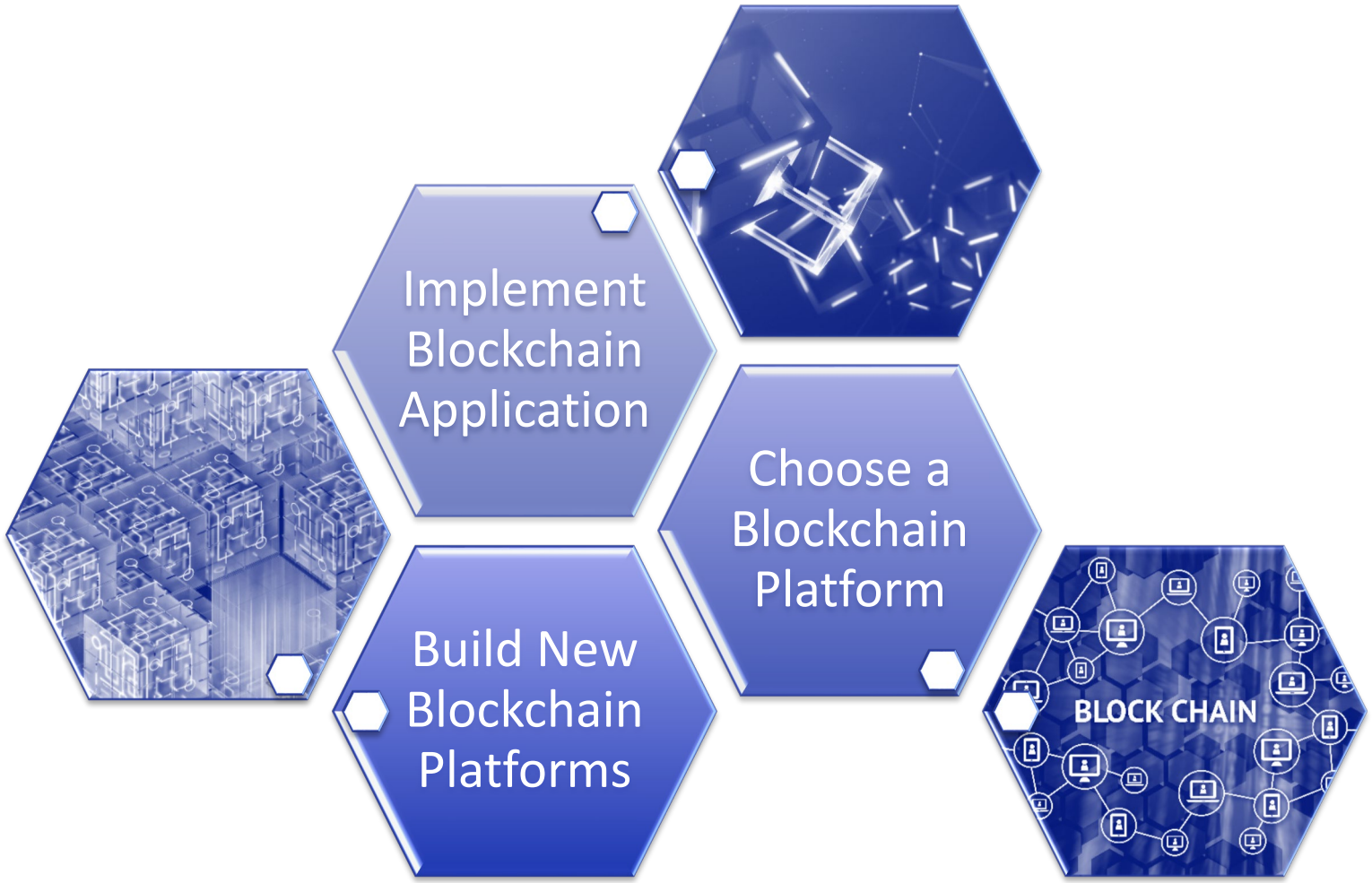


Some may call crypto mining malware an unintended side effect of public blockchain … but it’s just an effect that illustrates our lack of understanding of the system.

RSAConference2019

So, What Can You Do?

Our Role in The Ecosystem: What Choices Can We Make?



Private/Consortium Blockchain

PARTICIPATION *IS* THE INCENTIVE

Node work is the cost of doing business
Private and consortium chains typically permissioned, so bad actors can't join

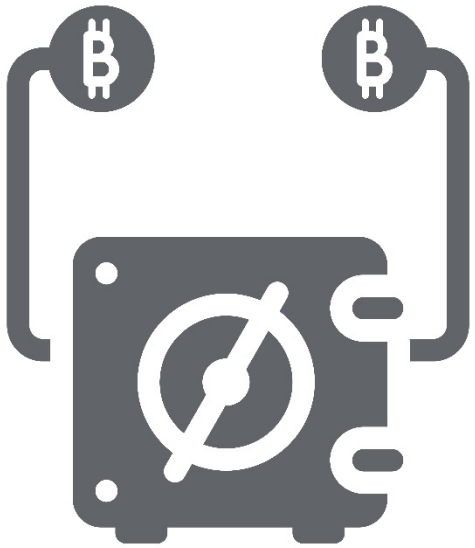
Change The Incentives?

No Incentive	Back to the original problem: how to get nodes to participate?
Limit How Much An Account Can Mine in a Given Time Period	Miners will just create multiple accounts…
Product Discounts / Transaction Fee Discounts	Miners more likely to care about the product or service Discounts must be compelling enough to incent your users Ensure discounts can't be misused (e.g., stacked)
Incentives to find and report weaknesses	Encourages good community behavior; can finding weaknesses be more profitable than exploiting them?

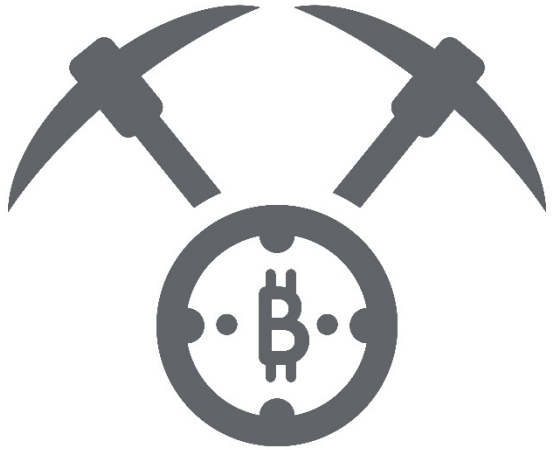
Remember: Human Beings Are *Still* Terrible at Creating Incentives

Freakonomics The Movie (2010)

What If We Don’t Use Proof of Work?



PROOF OF STAKE



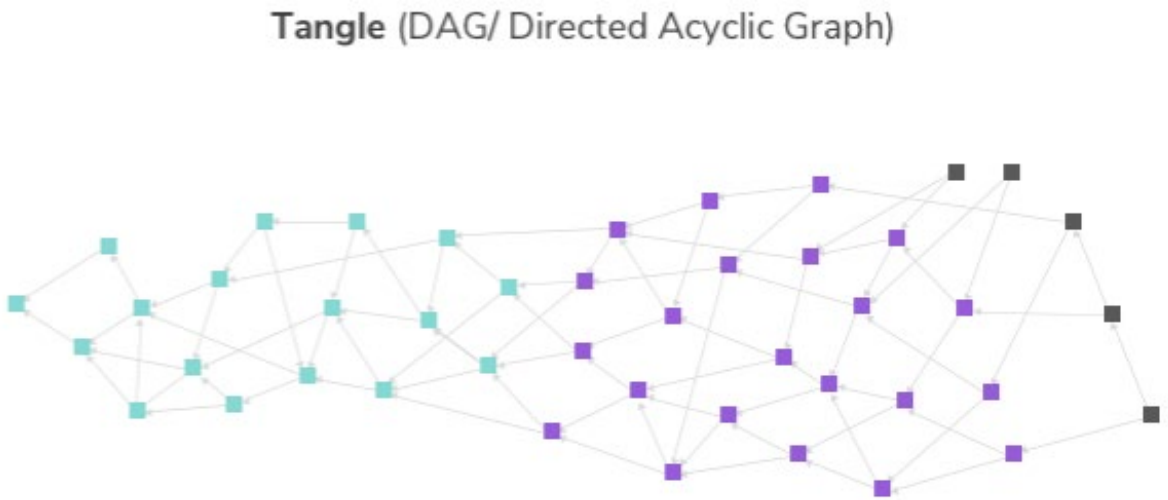
PROOF OF CAPACITY

What If We Don't Use Proof of Work?

	Proof of Stake	Proof of Capacity / Proof of Space
What is it?	• New block creator chosen based on wealth/stake • "Miners" (called forgers) take transaction fees • Prospective forgers join validator pool to be selected • Variants: Randomized, Age-Based, Delegated	• Allocate disk or memory space rather than computing cycles
Pros	• Forgers don't use computing power • Environmental impact reduced • Forgers must already own currency	• Environmental impact reduced
Cons	• Lack of computing power requirements may enable other attacks • The "Nothing-At-Stake" problem	• Modified malware could take over memory space

Other Options

- Ripple
  - Primarily for banking, reducing settlement time
  - No mining
- IOTA
  - Tangle, not blockchain
  - Designed for scalability
  - Reward for validating transaction is to have your transaction validated



www.iota.org

RSAConference2019

Conclusion

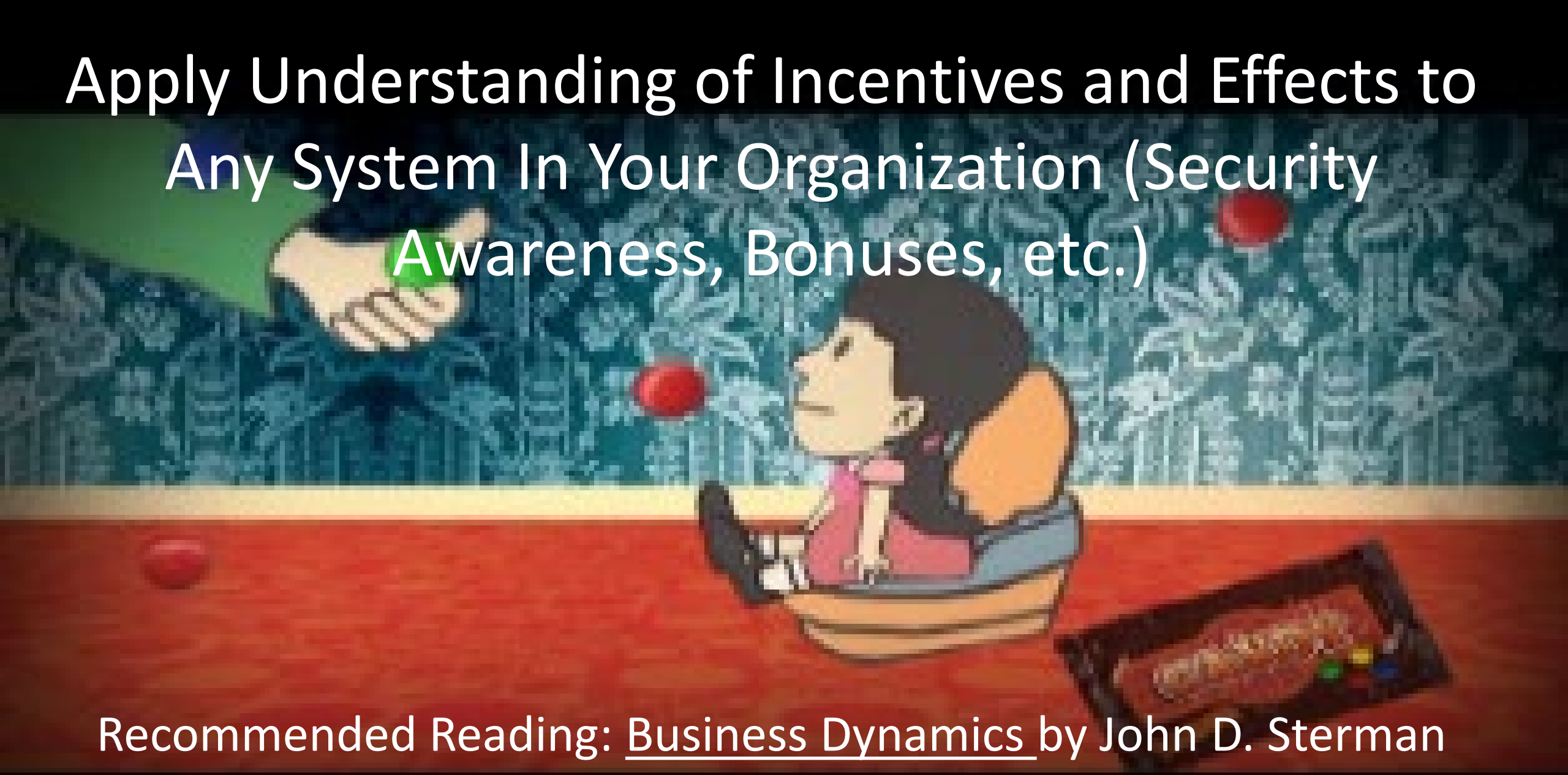
Summary

- Incentives are hard
- There's no such thing as "side effects"
- Crypto mining malware is an effect of blockchain incentive design
- There are other options for incentives that might reduce cryptojacking
- But everything has an effect … study the system carefully

Apply What You Have Learned Today

- Next week you should:
  - Look at platform and incentive options for current blockchain projects, consider effects and determine whether different approaches needed to reduce cryptojacking risk
- In the first three months following this presentation you should:
  - Learn more about system dynamics, incentives, effects and policy resistance
  - Evaluate incentive options when selecting blockchain platforms for future projects
- Within six months you should:
  - Watch for new incentive options and platforms, analyze potential effects and determine how they address your business case and risk model
  - Consider effects of any incentive program in your organization (blockchain or otherwise)

Apply Understanding of Incentives and Effects to Any System In Your Organization (Security Awareness, Bonuses, etc.)



Recommended Reading: Business Dynamics by John D. Sterman

Freakonomics The Movie (2010)

RSAConference2019

Questions?

RSAConference2019

Thank You!

@sandycarielli