Cryptocurrency Myths:

Public perception and understanding in the Bitcoin era

Ben C. Roose

CS 898AT: Bitcoins and Cryptocurrencies

Instructor: Dr. Murtuza Jadliwala

What are we talking about?

We will look at:

- How Bitcoin has been portrayed in the public media
- How ransomware attacks have increased in the era of Bitcoins
- How there is a lack of understanding within the general public
- How we can give better understanding by finding different ways to explain technology!

Portrayal of Bitcoin by the media

- Bitcoin associated with hackers and ransomware:
  - **“Hackers Have Stolen Millions Of Dollars In Bitcoin -- Using Only Phone Numbers”** - Shin, L. Forbes. Dec. 20, 2016
  - **“What you need to know about bitcoin after the WannaCry ransomware attack”** - Fung, B. The Washington Post. May 15, 2017
  - **“Hackers have cashed out on $143,000 of bitcoin from the massive WannaCry ransomware attack”** - Browne, R. CNBC Special Report. Aug 3, 2017
- Bitcoin associated with large financial gain/loss or a lack of security:
  - **“Will bitcoin ever be a safe investment or always a gamble?”** - Hickey, S. The Guardian. Oct. 1, 2017
  - **“I Forgot My PIN’: An Epic Tale of Losing $30,000 in Bitcoin”** - Frauenfelder, M. Wired. Nov. 29, 2017

Cryptocurrencies on the Rise

- Bitcoin has passed the $10,000 mark!
  - Current exchange rate: 1 BTC = $10,083
  - Cryptocurrencies becoming part of the global economy

- Cyber-attacks involving financial extortion are also on the rise!
  - Cryptocurrencies used as tools by ransomware and extortionists
  - WannaCry infected computers in 150 countries and made attackers about $120,000 in BTC during May 2017

- How much will a global ransomware attack next year net for cyber-attackers?

Paying the Ransom in Bitcoins?

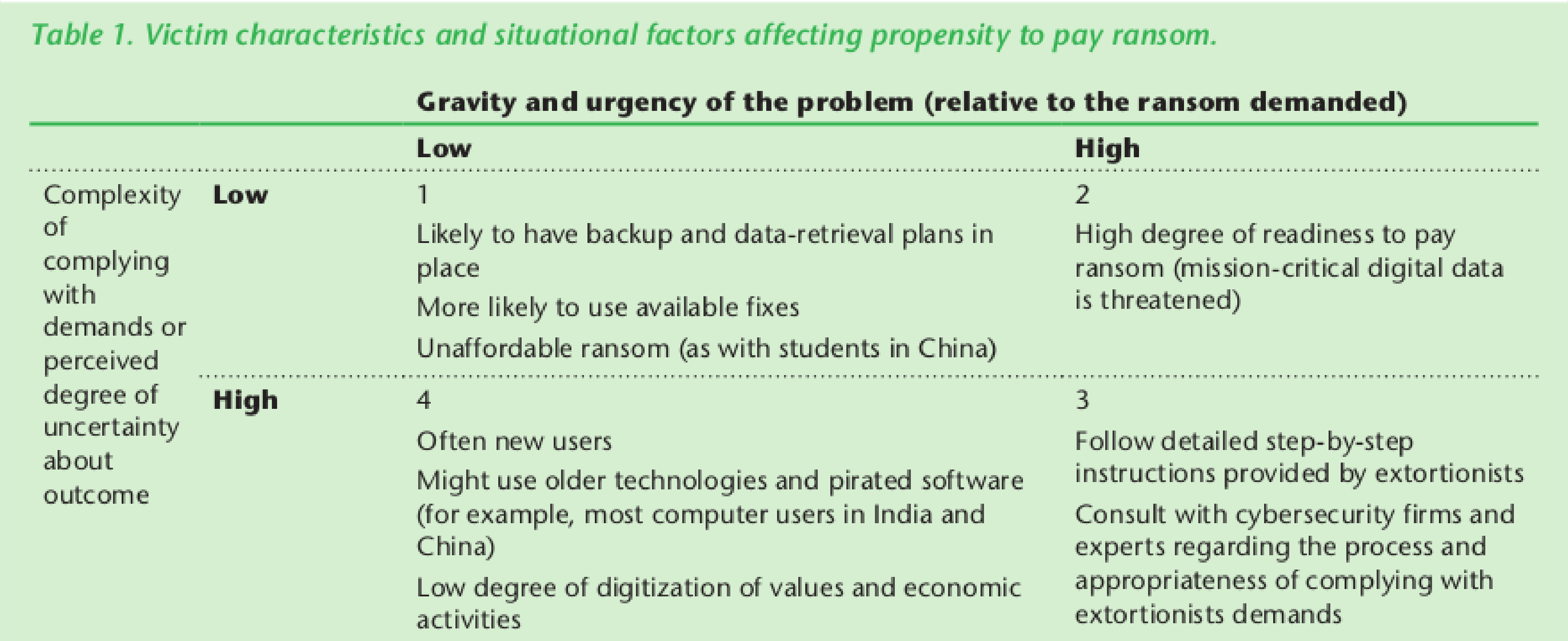


Table 1. Victim characteristics and situational factors affecting propensity to pay ransom.

		Gravity and urgency of the problem (relative to the ransom demanded)	
		Low	**High**
Complexity of complying with demands or perceived degree of uncertainty about outcome	**Low**	1 Likely to have backup and data-retrieval plans in place More likely to use available fixes Unaffordable ransom (as with students in China)	2 High degree of readiness to pay ransom (mission-critical digital data is threatened)
	High	4 Often new users Might use older technologies and pirated software (for example, most computer users in India and China) Low degree of digitization of values and economic activities	3 Follow detailed step-by-step instructions provided by extortionists Consult with cybersecurity firms and experts regarding the process and appropriateness of complying with extortionists demands

Kshetri, N. Voas, J. "Do CryptoCurrencies Fuel Ransomware?"
IT Trends, IEEE IT Professional (Vol. 19, Issue. 5, 2017).

Attacked at the weakest point

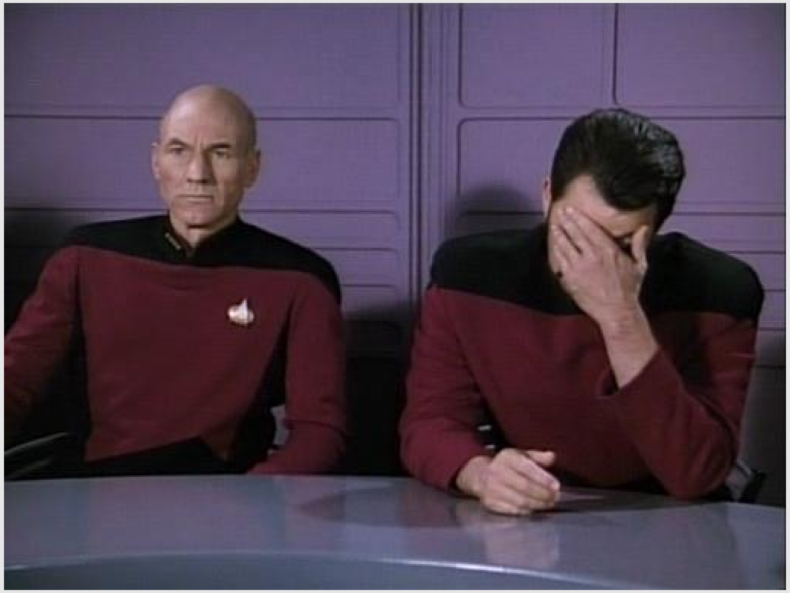
- Weakness is not within Bitcoins or cryptocurrency technology!
- Weakness is within users' **UNDERSTANDING** of the technology!

- Majority of successful attacks initiated by social engineering attacks
  - Phishing/spear-phishing
  - Drive-by-downloads
  - Physical infiltration
- Many data and financial loss events are caused by human error
  - Lack of good planning and back up procedures
  - Lack of good security practices and continued vigilance

Star Trek Technobabble

“The Enterprise computer system is controlled by three primary main processing cores cross linked with a redundant melacortz ramistat and fourteen kiloquad interface modules. The core element is based on an FTL nanoprocessor with twenty-five bilateral kelilactirals with twenty of those being slaved into the primary heisenfram terminal. You do know what a bilateral kelilactiral is?”

- *Star Trek: The Next Generation* (S06-E07: “Rascals”)



Effing the Ineffable

- Using Lego to explain Blockchain technology to techs and non-techs

Beginning a transaction

The completed blockchain
(3 blocks high)

Maxwell, D. Speed, C. Campbell, D. "'Effing' the Ineffable: Opening up Understandings of the Blockchain." *British HCI '15 Proceedings of the 2015 British HCI Conference. 2015.*

Analogical Reasoning

- Defined by Stanford Encyclopedia of Philosophy:
  - An analogy is a comparison between two objects, or systems of objects, that highlights respects in which they are thought to be similar. Analogical reasoning is any type of thinking that relies upon an analogy.

- Can we use analogies to help us explain these complex cryptographic technologies to the general public?

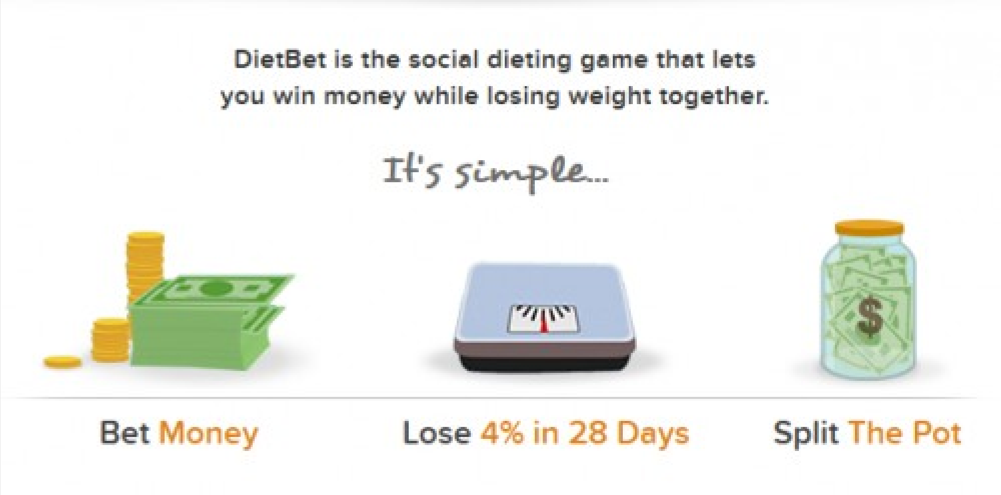
Analogy for **Proof-of-Work**: Fitness for points or profit

WSU Heskett Center:
F45 Team Training

- work out in a team for points

- whichever team has the highest points wins that round

dietbet.com



DietBet is the social dieting game that lets you win money while losing weight together.

It's simple...

Bet Money

Lose 4% in 28 Days

Split The Pot

Analogy for **Proof-of-Burn**: Memento Coin Presses

A penny press at Disneyland

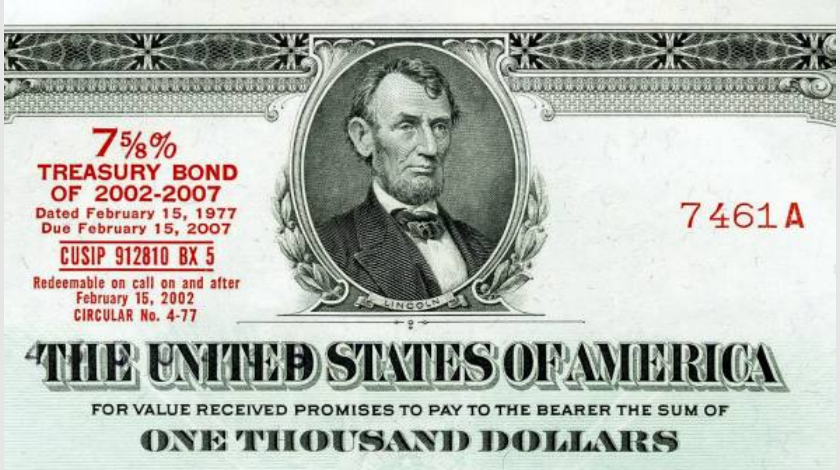
Pressed Disney “memento” pennies

- no longer legal tender, but sometimes worth a lot more!

From: *disneyland.disney.go.com*

Analogy for **Proof-of-Stake**: Treasury Bonds

- Proof of Stake (PoS) concept:
  - “… a form of proof of ownership of the currency. … Philosophically speaking, money is a form of ‘proof-of-work’ in the past thus should be able to substitute proof-of-work all by itself.” - King, S. & Nadal, S. “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.” 2012.
- Treasury Bonds:
- “...pay a fixed rate of interest every six months until they mature. They are issued in a term of 30 years.” - treasurydirect.gov



7⅝%
TREASURY BOND
OF 2002-2007
Dated February 15, 1977
Due February 15, 2007

CUSIP 912810 BX 5

Redeemable on call on and after
February 15, 2002
CIRCULAR No. 4-77

7461A

THE UNITED STATES OF AMERICA

FOR VALUE RECEIVED PROMISES TO PAY TO THE BEARER THE SUM OF

ONE THOUSAND DOLLARS

To Conclude

- Cryptocurrencies will become more complex yet more mainstream
- Ransomware and cyber-extortion will continue to rise
- Security of user data will continue to be very important
- Developing understandable ways to explain technology as important as developing the technology itself
  - Heuristic: use simple models to give meaning to complexity
  - Analogical: explain fundamentals with real world comparisons
  - Association: relate explanations to the user’s world view

- Above all, pretend to not have a degree in Computer Science and use less of the *Star Trek technobabble*!

Thank You!

Ben Roose: ben.roose@wichita.edu

These slides can be found at:
https://github.com/benroose/presentations

Any Questions?

Ben Roose is an employee of
Wichita State University