Ransoming Data: Technological and Legal Implications of Payments for Data Piracy

Ian T. Ramsey, Stites & Harbison, PLLC
Edward A. Morse, Creighton University School of Law

CYBERSPACE LAW COMMITTEE
WINTER WORKING GROUP
FORT LAUDERDALE, FLORIDA
JANUARY 29-30, 2016

Ransom and Terrorism

- Ransom payments provide a potentially significant source of terrorist financing.
  - Kidnapping people: 1,283 kidnappings motivated by terrorism were reported in 2012 (U.N. Security Council)
  - Ransom rates are also going up: $4.5M/hostage in 2012, up from $1M in 2011 (U.N. Security Council)

Selected History…

- 1st Reported Ransom Note in American History
  - The 1874 Kidnapping of Charles Brewster Ross
- Charles Lindberg Jr. 1932
  - Beginning of FBI Crime Lab/comparison of handwriting exemplars from suspects
- Peter Weinberger 1956
  - Search of 2 million handwriting exemplars from New York Department of Motor Vehicles

The Biggest Ransom in History?

- 1533: Francisco Pizzaro Takes Atahualpa
- The Inca fill a room 22 feet long, 17 feet wide, and 8 feet high with gold and silver
- =13,000 lbs. gold and 26,000 lbs. silver
- Approximate current value:
  - $226,720,000 in gold
  - $5,824,000 in silver
- But query: does the $1.7B recently paid to Iran on 1/17/16 count as ransom?

Criminal Enterprises

- Most ransom involves criminal enterprises, not terrorist organizations
- Technology emerging: "Virtual" kidnapping
  - Extortion target "off the grid" for a time.
  - Social media allows access to information.
- Technology facilitates, as well as prevents, crime

Riskmap Report: Top 10 Countries

COUNTRIES	2014	2013
MEXICO	01	01
INDIA	02	02
PAKISTAN	03	04
IRAQ	04	10
NIGERIA	05	03
LIBYA	06	14
AFGHANISTAN	07	08
BANGLADESH	08	26
SUDAN	09	20
LEBANON	10	06

Market Responses

- Criminals may also be “outsourcing” and specializing in aspects of crime.
- Insurance markets begin to cover ransom: $500M market in 2011, up from $250M in 2006 (UN Security Council).
- But sanctions regimes may affect ability to collect; some policies are adjusting accordingly (another reason not to pay)

Government Responds

- Cf. History: Barbary Pirates and War (1801-29) https://history.state.gov/milestones/1801-1829/barbary-wars
  - State-sanctioned piracy
  - Challenges of international cooperation
  - Ransoms paid; Marines part of solution.
- Piracy is “primary security concern for maritime industry in 2015” (RiskMap Report 2015).
  - Somali pirates less of a threat than in 2011 due to better security investments, naval strategies.
  - But threat capacity still exists. (See id.)

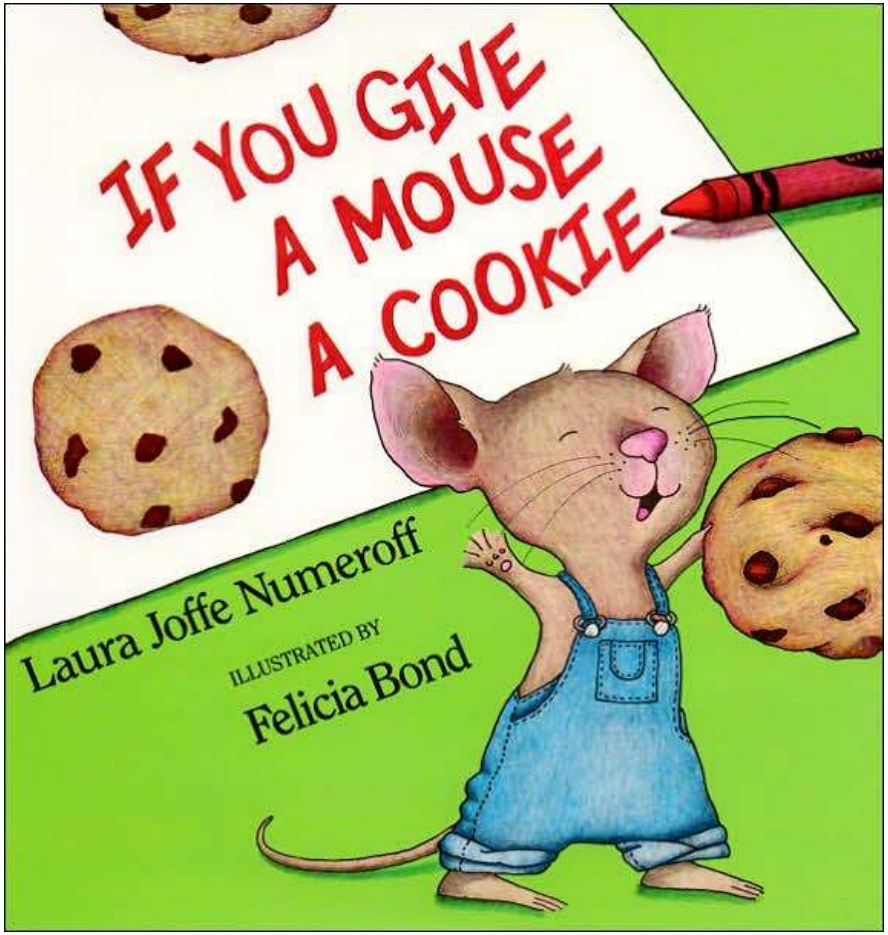
Government Responds

- Modern alternative: Sanctions Regimes
  - Treasury's Office of Foreign Assets Controls restricts ability to transfer funds to individual, firm, or country subject to international sanctions.
  - Sanctions regimes potentially impact ransom payments for piracy, individuals, etc.
- U.S. government also has had a longstanding policy not to deal with kidnappers.
- Sanctions and ransom policy inject friction into the business model for kidnapping (raise transaction costs for both payor and payee).

Government Policy: No Ransom

- Official US Policy: No ransom payments.
- “I firmly believe that the United States government paying ransom to terrorists risks endangering more Americans and funding the very terrorism that we’re trying to stop. And so I firmly believe that our policy ultimately puts fewer Americans at risk.” - President Obama, June 24, 2015

U.S. Policy Illustrated



Government Policy Shift?

- “In particular, I want to point out that no family of an American hostage has ever been prosecuted for paying a ransom for the return of their loved ones. The last thing that we should ever do is to add to a family’s pain with threats like that.” President Obama, 6/24/15
- So, are private ransom payments really OK, even if they violate the sanctions regime?

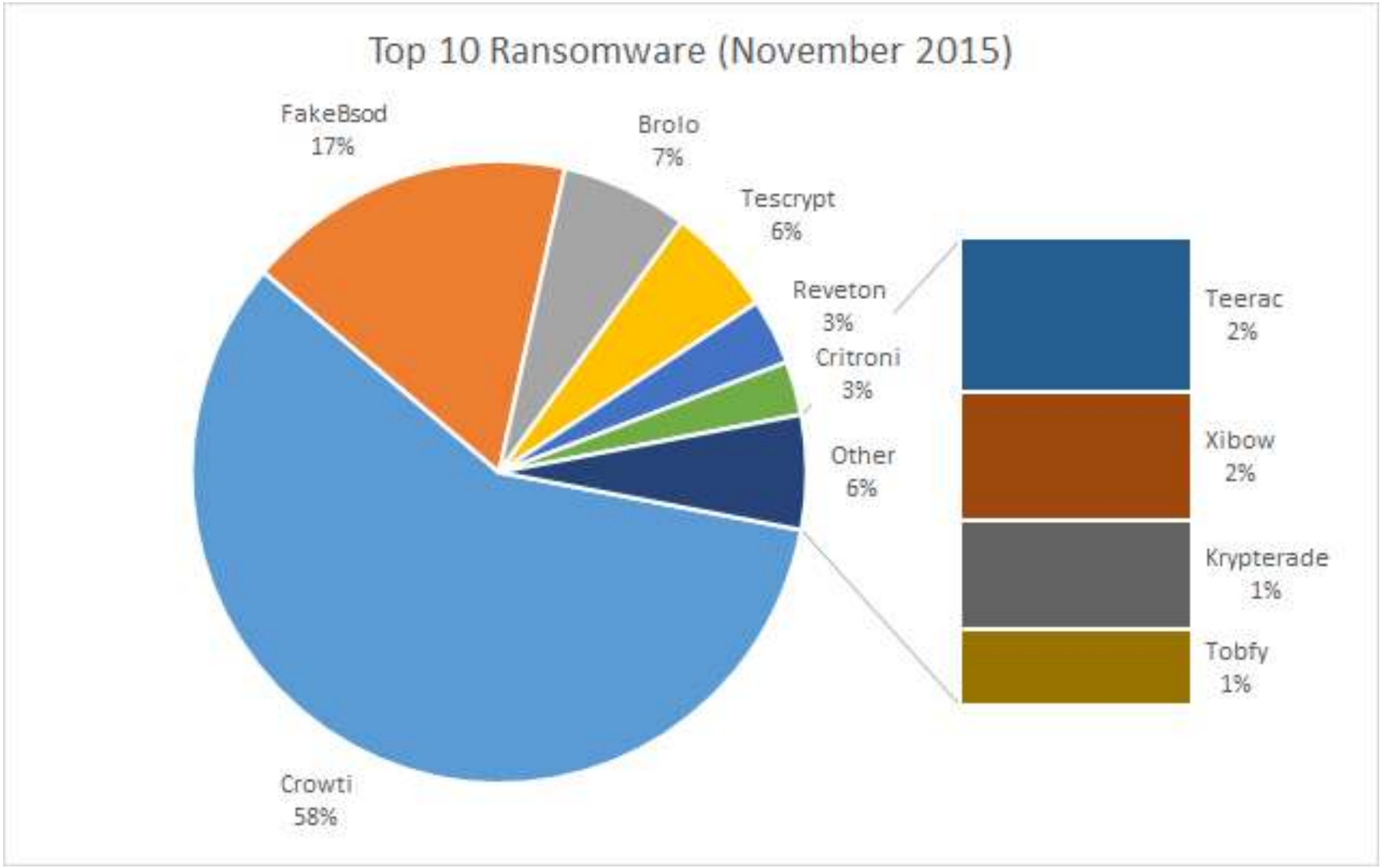
Government Policy Shift?

- Commentators debate whether President Obama's announcement in June will affect the economics of private ransom payments under the sanctions regime.
- Will financial institutions risk facilitating payments without a license from the OFAC?
- Does this announcement incentivize more hostage taking?

Shifting Context: Data Ransom

- Kidnapping and piracy involving people and physical objects can be dangerous (costly).
- Data hacking can occur remotely and without personal risks (less costly)
- Data hacking can be monetized in various ways. E.g.,
  - Identity theft (target the victim's clients).
  - Ransom? (target the victim).
- Risk/Reward Payoff: which would a criminal enterprise prefer?

Microsoft's Top 10 Ransomware for 2015



Approaches to the Problem

- Technological barriers: (self-help, e.g., arm your ships, secure your networks)
- Law enforcement efforts (government-help, e.g., the Marines, the FBI)
- Financial regulations
  - AML regimes. Can we catch cybercriminals through robust monitoring of payment networks?
  - Sanctions regimes. Can we bolster AML with sanctions?
  - Can bitcoin circumvent AML regimes? Does the size of the payment matter? (Corporate vs. individual targets)
- Tax laws? Other criminal sanctions?

Exploring Sanctions

- Government deters criminal conduct by regulation and penalties in other areas.
  - E.g., UIGEA imposes penalties within payment networks to deter illegal gambling.
- Some regulatory regimes penalize payors, too.
  - E.g., FCPA; criminal sanctions on illegal gambling, drugs, prostitution.
- Could sanctions/penalties for ransom payments be an effective policy tool?
- Where can government(s) exercise effective control in a diffused network?

Law Enforcement Efforts

- Our paper outlines the maze of government agencies with investigative authority over ransomware.
  - Ransomware competes with other crimes for scarce resources.
  - International coordination is a challenge.
- In other contexts, such as the FCPA, financial regulation of payors becomes an important tool, particularly for public companies.

SEC FCPA Prosecutions for 2015

- Bristol-Myers Squibb - Improper payments to obtain sales, $14 million to settle charges. (10/5/15)
- Hitachi – Inaccurate recording improper payments in connection with contracts to build power plants, $19 million to settle charges. (9/28/15)
- BNY Mellon – Provided valuable student internships to family members of foreign government officials, $14.8 million to settle charges. (8/18/15)
- Vicente E. Garcia – Bribed government officials through an intermediary to procure software license sales and receiving more than $85,000 in kickbacks, returned kickbacks plus interest. (8/12/15)
- Mead Johnson Nutrition –Payments to health care professionals to recommend the company's product to new and expectant mothers, $12 million to settle the case. (7/28/15)
- BHP Billiton - Sponsored the attendance of foreign government officials at the Summer Olympics, $25 million penalty to settle the case. (5/20/15)
- FLIR Systems – Financed "world tour", $9.5 million to settle the charges. (4/8/15)
- Goodyear Tire & Rubber Company - Bribes to land tire sales in Kenya and Angola, $16 million to settle the charges. (2/24/15)
- Walid Hatoum / PBSJ Corporation - Bribes and employment to foreign officials to secure Qatari government contracts, $3.4 million to settle. (1/22/15)

FBI Establishes FCPA International Corruption Squads

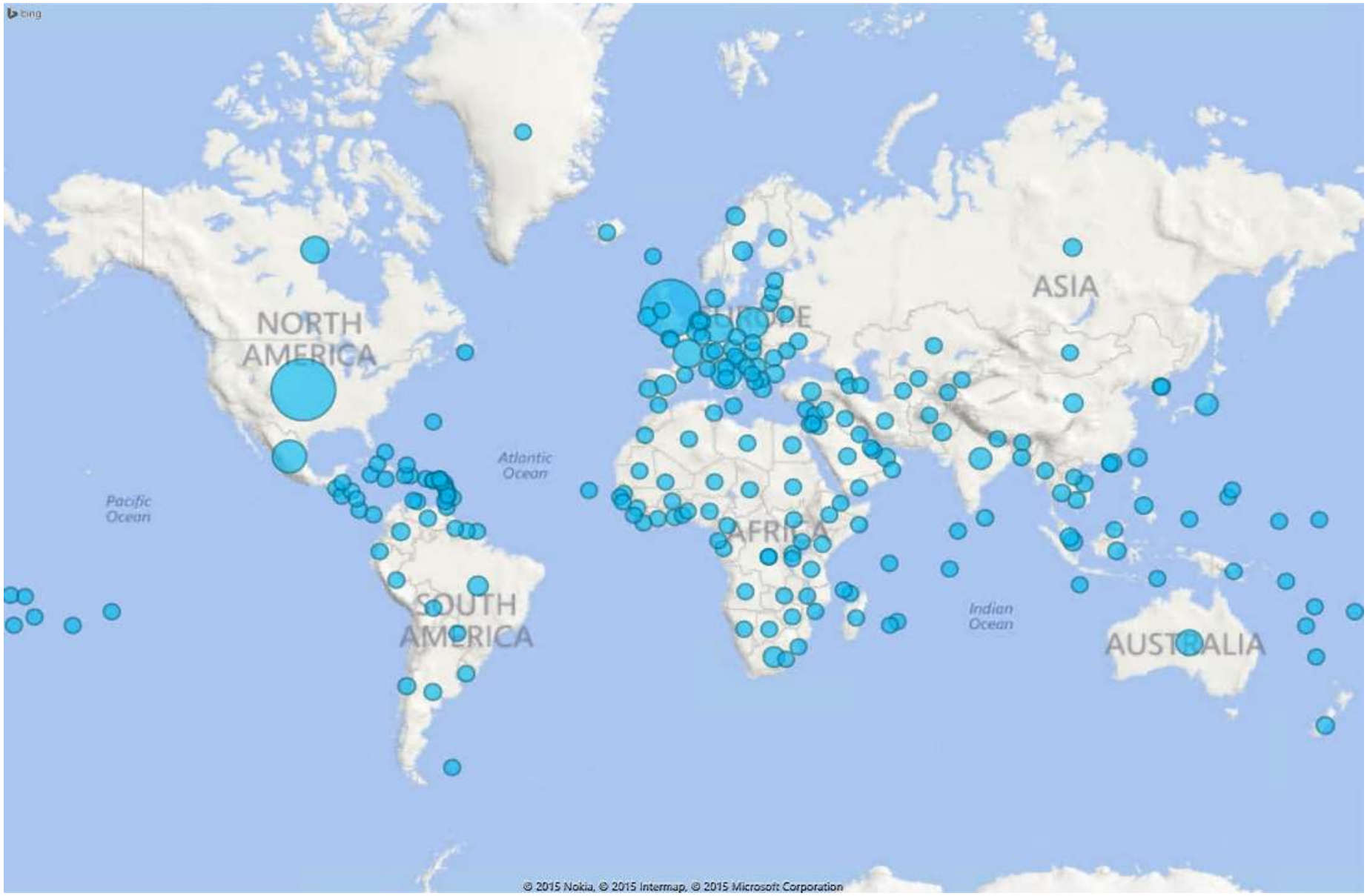
"The FCPA, passed in 1977, makes it illegal for U.S. companies, U.S. persons, and foreign corporations with certain U.S. ties to bribe foreign officials to obtain or retain business overseas. And we take these crimes very seriously—foreign bribery has the ability to impact U.S. financial markets, economic growth, and national security. It also breaks down the international free market system by promoting anti-competitive behavior and, ultimately, makes consumers pay more."

Corruption and Cooperation

- Corruption has a corrosive effect on the prospects for international cooperation, which is critical for global financial networks.
- The following slide shows relative risks of corruption (darker = greater) as measured under the FCPA.
- Malware targets are, not surprisingly, tracking areas of economic developments.
- A more interesting question: where are malware originators?

FCPA Global Risk Map

Microsoft 2015 Malware Heat Map



AML Regulations

- Our paper outlines significant provisions that potentially affect criminal enterprises through payment networks.
  - CID and due diligence requirements require robust identification of account owners.
  - Entities present special challenges, imposing significant burdens on financial institutions where state laws permit relative anonymity.
  - Ongoing monitoring activities may also trigger SAR.

SAR Filings

- In 2014, there were 1.7 million SARS filed.
  - FINCEN, SAR Stats (October 2015)
- Yet fraud remains a significant problem.
- Can 1.7 million incidents really be monitored effectively?
- Anecdotal evidence indicates that some data ransom demands continue to use domestic accounts.

Foreign Payments

- Enhanced AML requirements on cross-border EFT – necessary to target international money movement .
  - But there are a lot of banks out there (and corruption problems, too)
  - Problems of entity formation and anonymity
- Sanctions regimes can encompass countries, payees. But the sanction list will not provide a comprehensive limitation on criminal enterprises.
- Financial network regulation will not be stronger than the weakest link.

Bitcoin and Virtual Currency: An Alternative

- Regulation of bitcoin exchanges continues to present challenges, particularly for payments originating through domestic firms, as transactions may generate AML inquiries:
  - Converting cash to bitcoin
  - Converting bitcoin to cash.
- Stephen T. Middlebrook and Sarah Jane Hughes, Regulating Cryptocurrencies in the United States: Current Issues and Future Directions, 40 William Mitchell L. Rev. 813 (2014).

Bitcoin and the Blockchain

- Ownership of Bitcoins can be anonymous but the Blockchain is not
- The Blockchain only tracks what it is given
- The Blockchain utilizes a consensus mechanism to confirm transactions, i.e., so that transactions can be tracked backwards arguably to an owner
- Note that Blockchain technology is not necessarily limited to Bitcoin transactions:
  - Dyed Bitcoin dust to represent bonds, shares or units of precious metals
  - Real Property Titles
  - Smart Contracts (crowdfunding)
- Distributed Ledgers-the next generation Ethereum

A Moment to Explain the Blockchain

Making a hash of it

INPUT

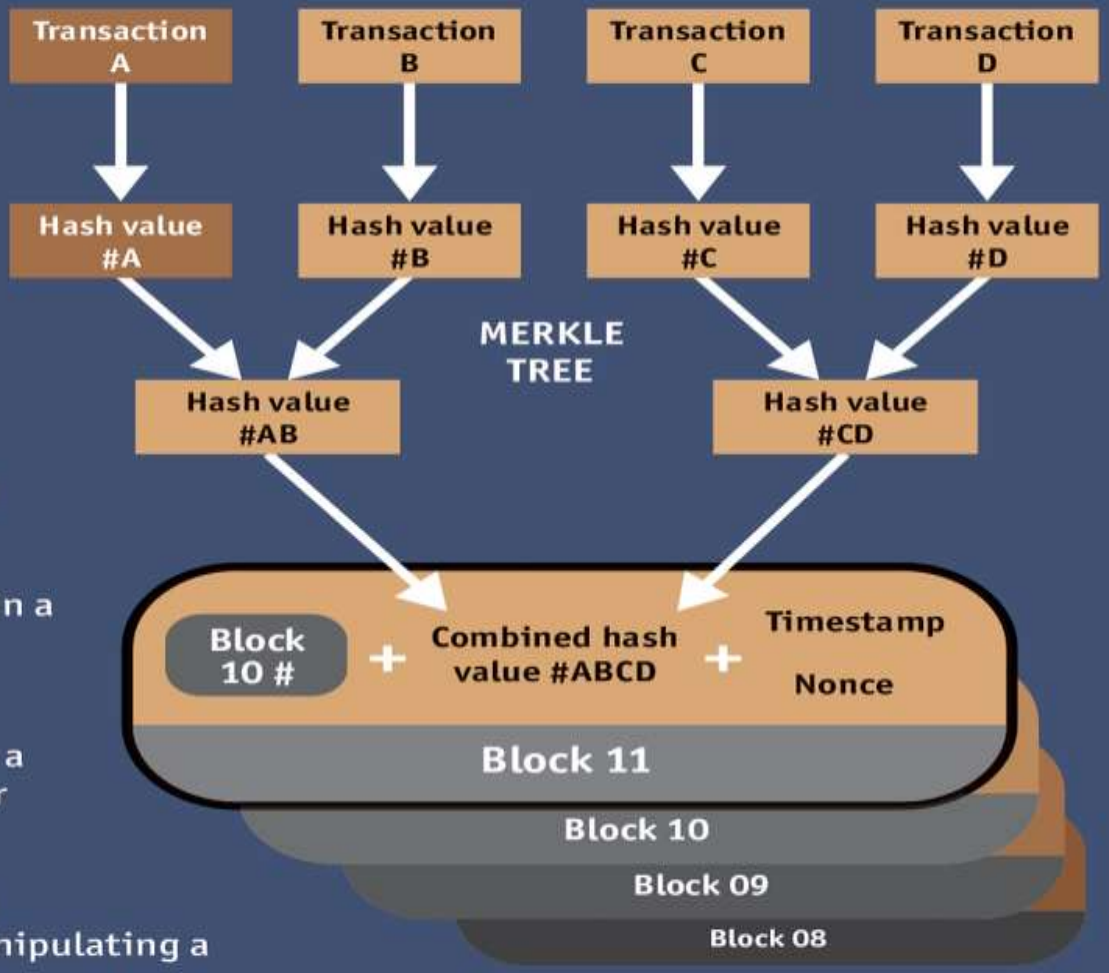
Transaction A

Any length of data

OUTPUT #A

#DFCD 24D9 AEFE 93B9

Unique hash value of fixed length



Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.

Hash values are further combined in a system known as a Merkle Tree.

The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.

The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.

Once a solution is found the new block is added to the blockchain.

Economist.com

Wall Street Journal's Bitcoin Headlines

- Reported Bitcoin founders home raided in Sydney Australia (December 9, 2015)
- Bitcoin Frenzy Back As Epic Bust Fades (November 4, 2015)
  - From $13 to $1,000
- Bitcoin Fund Linked To Currency's Rally (December 6, 2015)
  - Bitcoin Investment Trust: $250 to $450
- Is Bitcoin Breaking Up? (January 17, 2016)
  - Legitimacy v. Disrupter
- Corruption Currents: Dutch Bust Bitcoin Dark Web Ring (January 20, 2016)

Anonymous Currency

- Zooka Wilcox and Zcash
- Zero-Knowledge Proof
  - Cryptography method where one party (prover) can prove to another (verifier) that a given statement is true without conveying any information apart from the fact that the statement is indeed true

Blockchain v. Zero-Knowledge Proof

Should financial transactions be transparent?

Virtual Currency Prosecutions

- May 2013 ($6 B in Cybercrime Transactions)
  - Liberty Reserve
- January 2014 (Silk Road Drug Purchases)
  - Charlie Shrem: BitInstant
  - Robert Faiella: Bitcoin exchanger
- November 2014 (Global Cybercrime Network)
  - Anthony Murgio: Coin.mx
  - Gery Shalon, Joshua Aaron, Ziv Orenstein
- May 2015
  - Ripple Labs, Inc.

Other Laws

- Other laws: e.g., FATCA Account Compliance. Massive information collected about identity of account holders, but role in crime prevention is likely limited.
- Tax laws: Information reporting regimes present interesting compliance challenges for ransom payments.
  - E.g., 6041A(a): payments for services of $600+
  - Penalties for noncompliance, but relief when "due to reasonable cause and not to wilful neglect?
- Withholding regimes could impact international payments to foreign payees. (IRC 1441, 1442).
  - You may be liable for unpaid withholding tax (IRC 1461)!

Other Laws

- Could a ransom payment to a criminal also engaged in crimes against humanity generate civil liability under the Alien Tort Statute of 1789?
  - Outline addresses multiple barriers to this kind of threat.
- FCPA as currently formulated also provides unlikely source of risk for payment.

Altering the Legal Regime: Some Considerations

- Ransom reduces risk for payor, but may raise risk for all targets by incentivizing more ransomware activity.
- Jurisdictional constraints affect policy choices: target where you can effect change.
- Could enhanced information reporting assist law enforcement efforts?
- Would payor penalties nudge toward enhanced security investments? Or displace crime to other targets? (e.g., EMV?)
- What would a penalty regime look like?
  - Definitional problems (legitimate services vs. ransom).
  - What penalties would be effective?
- Discussion?