CRYPTOCURRENCY: THE SECURITY LANDSCAPE

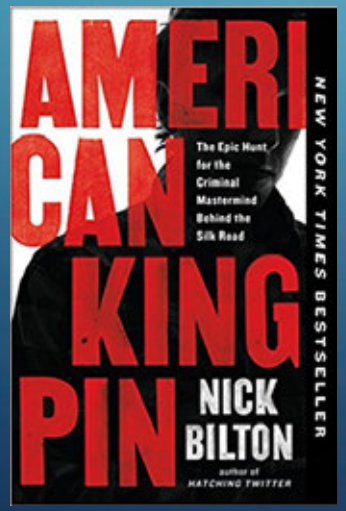
ANITA NIKOLICH

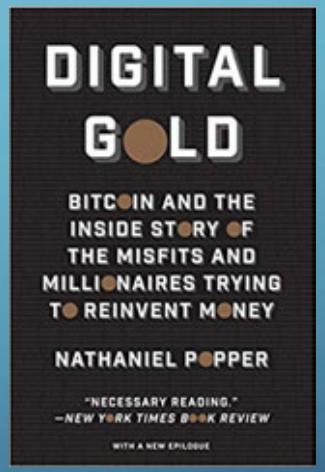
VISITING FELLOW, COMPUTER SCIENCE, ILLINOIS TECH

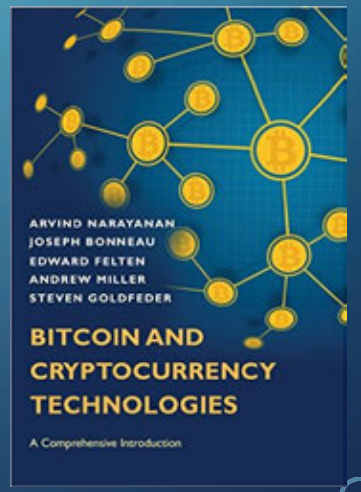
SECURITY CONSULTANT, ERISX

INTERESTING BACKGROUND READING

- Arvind Narayan, *Bitcoin & Cryptocurrency Technologies* (Also a popular Coursera class)
- Nathaniel Popper, *Digital Gold*
- Nick Bilton, *American Kingpin*







FAVORITE BITCOIN QUOTES FROM THE WORLD OF FINANCE

Warren Buffet: "*Bitcoin… is probably rat poison squared*" (2018)

Jamie Dimon, CEO JP Morgan, "*You can't have a business where people can invent a currency out of thin air and think that people who are buying it are really smart.*" (2017)

HAPPY 10 YEAR BIRTHDAY BITCOIN!

- Oct 31, 2008 Satoshi Nakamoto publishes paper "Bitcoin: A Peer-to-Peer Electronic Cash System.“
- May 22, 2010 Bitcoin Pizza Day – 2 pizzas purchased for another enthusiast for 10,000 BTC

….and Happy 5 Year Birthday, Ether…

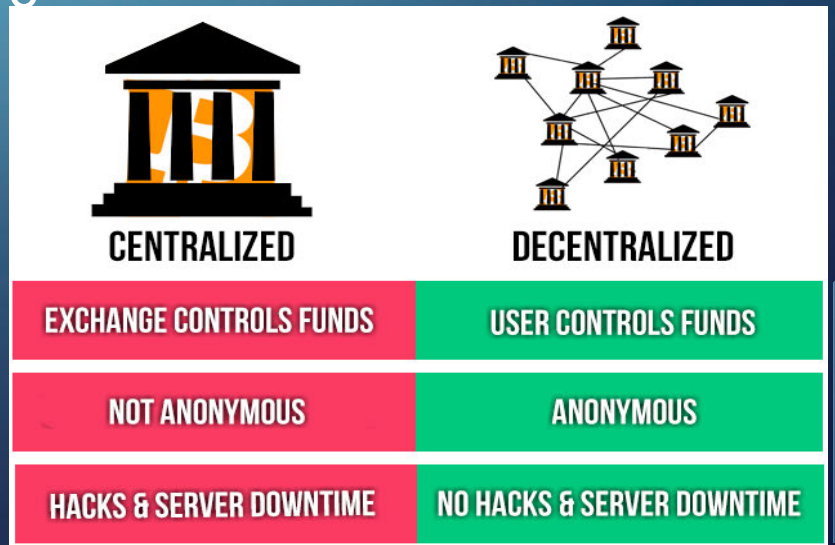
- November 2013 Vitalik Buterin publishes Ethereum White Paper
- 2015 Ether is born

WHAT'S DIFFERENT ABOUT CRYPTOCURRENCY?

- Deposits and Transfers are irreversible and permanent.
- If a private key is lost, it will not be able to be recovered. EVER!
- Can be pseudo anonymous. (Some is actually anonymous (zCash))
- No one is in charge! No central bank, no 3rd party, no middleman
- The blockchain consensus mechanism is hard to break
- Difficult for average investor to access, though that is slowly changing
- KYC/AML can be more challenging and labor intensive.
- Assets can have a history/provenance. Unlike paper cash, financial Institutions have to decide how to handle Crypto formerly used in dark markets.

WHERE IS CRYPTO BOUGHT/SOLD/KEPT/TRADED?

- Explosion of Cryptocurrency Exchanges with varying reputations and fees
- Most Exchanges are “Centralized” – deposit your cryptocurrency, allow you to trade using their matching engine, Exchange keeps funds safe (or not)
- Some Exchanges are “Decentralized” – they do not hold customer funds. No need to trust the security or honesty of the exchange since the funds are held by you in your personal wallet



TRADITIONAL INVESTMENT FIRMS ARE (SAFELY) GETTING INTO CRYPTO – VIA CUSTODY SERVICE

- Fidelity Digital Services (2018) - new company that will deal exclusively with cryptocurrency custody and trade execution
- Northern Trust – Custody offering
- Komainu = Nomura + Ledger – Custody offering
- Goldman Sachs considering Custody offering

Regulated crypto custody will allow more institutional buyers -- such as hedge funds and pensions -- to invest in cryptocurrency

ROAD TO LEGITIMACY IS PAVED WITH REGULATION

- SEC - Regards nearly all digital tokens (ICOs) as securities
  - Issued many investor alerts, bulletins and statements on ICOs and cryptocurrency-related investments.
  - Refuses to approve cryptocurrency ETFs, citing concerns over investor safety and lack of market liquidity.
  - Cyber Unit established 2017. ~250 cyber related investigations going.
- Commodity Futures Trading Commission (CFTC) -
  - 2015 - virtual currencies such as Bitcoin are commodities subject to oversight
  - Takes action against unregistered Bitcoin futures exchanges
  - May 2018 guidance for clearinghouses and exchanges planning to list cryptocurrency-related derivatives products.
- DOJ/SEC/FTC, etc -Task Force on Market Integrity and Consumer Fraud (July 2018)

SECURITY THREATS ASSOCIATED WITH CRYPTO

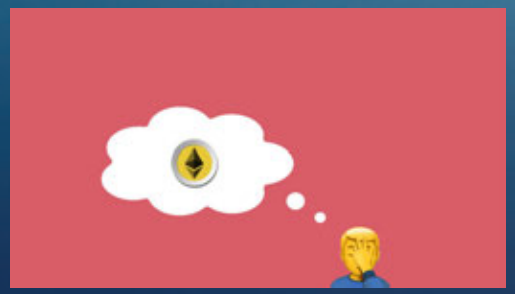
- 51% attack: Single or group of miner's hashing power accounts for more than 50% of the total hashing power
- Eclipse attack: monopolize the victim's incoming & outgoing connections to isolate the victim from the other peers in the network
- Smart Contract bugs and inherent weaknesses in Ethereum Solidity code language – ie 2016 DAO "recursive call bug" was used to make multiple withdrawals when only one should be allowed. $40M USD Ether stolen
- BGP Hijacks – April 2018 myetherwallet.com users directed to bogus site

SECURITY THREATS TO CRYPTO EXCHANGES

- DDoS Attacks on Exchanges. July – Sept 2017 74% of bitcoin exchanges targeted with DDoS attacks (data based on 5700 network DDoS attacks). 8th most targeted sector.
- KYC/AML Evasion – Fake ID/persona
- Money Laundering by spreading coins across various exchanges.
- Access to Users' private keys – once lost or stolen, they money is gone forever; vulnerable to hackers, and lost funds are hard to track, much less recover.
- Insider Threat

IT'S ALL ABOUT KEEPING WALLETS SECURE

- Your wallet IS the cryptocurrency
- Wallets = private keys = are strings of numbers
- Hot wallet = private keys online.
- Cold wallet = private keys offline on a non-Internet connected device. Hardware wallet, paper wallet, "brain wallet"



CUSTODY

- Custody = hold digital currency on behalf of client. Technical process of securely storing digital assets is outsourced to a trusted third-party to minimize the risk of loss due to theft or operational errors.
- Legalities around what custody means for cryptocurrency – still unclear.
- Custody is expensive and vulnerable. Roughly $100,000 setup fee, 10 basis points per month, and a minimum balance of $10 million.
- Takes up to 48 hours to take money out of cold wallet custody. Various "liveness checks" and operational processes to prove authorization and authentication to move funds to hot wallet.

THE EMERGING "THREAT MODEL"

- Social Engineering magnified. Twitter scams impersonating famous people – "send .2 ETH and I'll send you back 2 ETH"
- Human Risk. Traders have been taken at gunpoint and forced to tell kidnappers their wallet password. Some have a "duress wallet".
- Phishing – Gain access to users' exchange or wallet passcodes. Use 2FA!
- Pump and dump schemes – with smaller coins
- Exchange hacks – DDOS attacks, insider threat, code bugs

SECURITY-RELATED BEST PRACTICES

- Adapt and follow NIST guidelines
- Implement Multi Signature Wallets – a digital signature scheme with the requirement of more than one signee to approve a transaction.
- Keep only a fraction of the cryptocurrency in a “hot wallet” online.
- Stringent operational processes around cryptographic keys, including schema to shard backup keys into pieces and keep in secure locations, only to be reassembled if necessary and with witnesses and multiple employees.
- Strong Software Integrity checks and QA process

IDENTIFYING FRAUD AND MANIPULATION

- Fraud and manipulation flags:
  - Pattern of strangely specific order sizes - some of which extend to over 5 decimal places.
  - Acquiring but not selling cryptocurrency
  - Users using location and identity cloaking services such as hidden proxies, RDP protocol, VPNs and the TOR browser to avoid fingerprinting.
  - Email addresses - old social media profiles related to that email address may provide useful information
- Commercial Analysis tools such as Chainalysis, Elliptic, etc evaluate provenance of coins in order for institutions to make a decision

RESEARCH CHALLENGES IN CRYPTOCURRENCY

- Bitcoin Covenants (2016) Malte Moser, Ittay Eyal, Emin Gun Sirer: Disincentivizes theft of coins using a mechanism that prevents attacker from gaining full control over funds despite stealing the private keys. A recovery key.
- Improving consensus mechanisms – speed is an issue
- Improving scalability and performance to increase speed of transactions
- Correctness by Design – ability for developers to produce secure protocols and code, by utilizing programming language techniques to create correct code, and cryptographic protocols with security proofs.

ERISX: CHICAGO BASED CFTC REGULATED CRYPTO EXCHANGE

- Backed by TD Ameritrade, DRW, Digital Currency Group, Cboe, Virtu, others
- Bitcoin (BTC), Ether (ETH), Bitcoin Cash (BCH), and Litecoin (LTC)
- Launching a derivatives exchange (DCM) and clearing organization (DCO) that will include fully regulated digital asset futures and spot contracts on one platform.
- ErisX.com

INTERESTED IN WORKING IN CRYPTO? ERISX IS HIRING SECURITY ENGINEERS!

ANY INTERESTING RESEARCH CHALLENGES? IIT IS DOING BLOCKCHAIN RESEARCH! ANIKOLICH@IIT.EDU