UNIVERSITY *of* NICOSIA

Session 3

Protecting the Network: From DoS to DeFi Attacks

BLOC 514: Emerging Topics in Blockchain and Digital Currency

Session Objectives

- Understand the types of attacks that can be launched on digital currency networks, such as 51% attacks, DDoS attacks, eclipse attacks, time-jacking, and flood attacks.
- Introduce the concept of selfish behavior in digital currency networks, e.g. selfish mining.
- Explore network design parameters that have been implemented to prevent a digital currency network from being attacked.
- Understand the vulnerabilities of bridges in the context of DeFi.

An open, distributed p2p network implementing the concept of a public blockchain is, almost by definition, vulnerable to a wide array of malicious attacks. Most users have heard of at least one such type of attack (the 51% attack), which, however, is far from being the only or the most dangerous type of attack that can be launched on a digital currency network. In this session, we will outline the most well known types of network attacks and we will discuss how protection is built in network design with references to bridge attacks and their impact.

Agenda

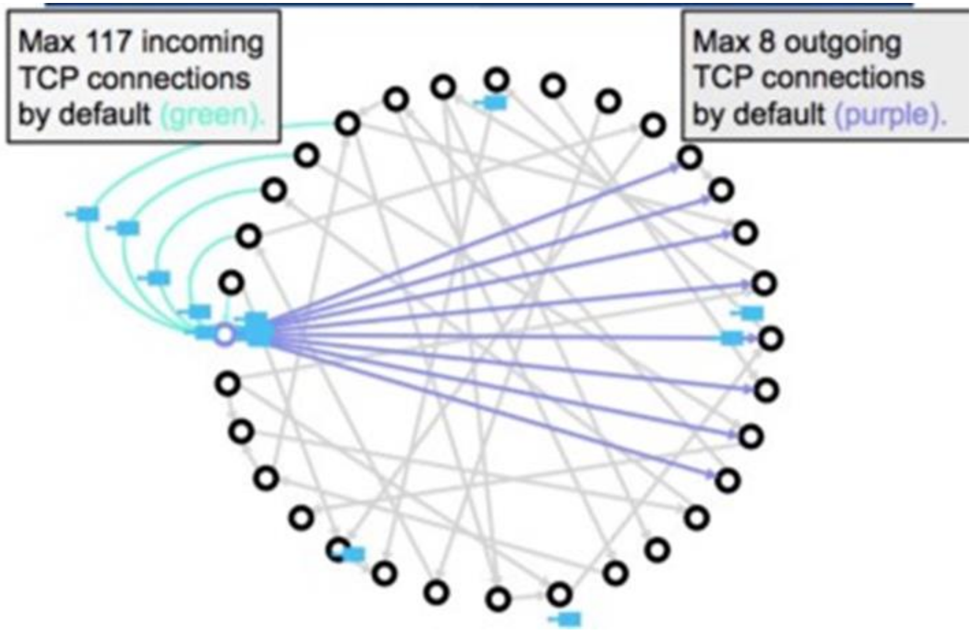
1. Structure of Bitcoin network and related graph metrics
2. "Traditional" attacks
3. Selfish mining
4. Other types of attacks
5. Bridges and DeFi attacks
6. The (important) role of simulations
7. Resources
8. Conclusions

Structure of Bitcoin network

Bitcoin Network Structure

- The Bitcoin network is a peer-to-peer network of distributed nodes.
- By design, each node can have **up to 117 incoming** connections and **up to 8 outgoing connections**.
- When joining the network, nodes connect to each other, thus forming a **gossip network**, where information propagates across the whole network and peers are able to broadcast transactions and blocks.
- There are two major ways of controlling the network:

1. **Controlling the information flow** between peers.
2. **Controlling the computational power** of the network – remember that decisions are based on consensus/majority.



Max 117 incoming TCP connections by default (green).

Max 8 outgoing TCP connections by default (purple).

Basic Graph Metrics

- "Characterising Cryptocurrency Project Networks Using Graph-Based Analysis" by J.Z.H. Wong, 2022
  - See Section 3.3: "Transaction Graph Analysis" (pages 16-19)
  - link
- Fundamental graph components
  - Vertices: addresses
  - Edges: transactions between two addresses
- Metrics:
  - Monthly Transaction Graph
  - Cumulative Monthly Transaction Graph
  - Relative Growth Rate
  - Repetition Ratio
  - Density
  - Reciprocity
  - Assortativity
  - Average Clustering Coefficient
  - Average Shortest Path Length
  - Small World Coefficient

"Traditional" Types of Attacks

51% Attack

- An adversary that controls more than half of the network's computing power can effectively control the entire network.
- When nodes are in doubt (i.e. they receive conflicting information), they trust the majority.
- Hence, an adversary that controls the majority of network resources can propagate information they want to the network.
- While controlling the network, the attacker can:
- Reverse transactions that s/he sends, thus double-spending own funds.
- Prevent other miners from mining valid blocks.
- Prevent valid transactions from gaining confirmations.
- However, the attacker cannot:
- Reverse other people's transactions or spend outputs belonging to others.
- Create new coins.
- Prevent transactions from being sent across the network.

Denial of Service (DoS) Attack

- A **denial of service (DoS)** or **distributed denial of service (DDoS)** attack is an attempt to make an online service unavailable by overwhelming it with traffic.
  - In a typical DoS attack, the attacker will overload a network/computer with requests above the capacity that the network/computer can handle.
  - In Bitcoin, this can be achieved by **sending lots of junk data to a node**. The nodes under attack will not be able to process normal Bitcoin transactions/blocks or receive new ones.
  - The block size limit is a first **countermeasure** against DoS attacks to Bitcoin nodes.
- Bitcoin has **built-in prevention mechanisms** against basic DoS attacks:
  - At the **protocol** level (see next slide)
  - At the **node (peer)** level (see slide after the next)
  - However, the network is still vulnerable to newer, more sophisticated, types of DoS.

Protocol-based anti-DoS rules

- Various limitations have been embedded on the Bitcoin protocol to prevent DoS attacks:
    - The **maximum block size**
    - The **maximum number of signature checks** that a transaction or block may request
    - The **maximum script size**
    - The **maximum size of values pushed while executing a script**
    - The **maximum number of "expensive" operations** in a script
    - The **maximum number of keys in multi-sig transactions**
    - The **maximum number of stack elements stored**

Node-based anti-DoS rules

- To prevent DoS attacks, a bitcoin node/peer:
  - Does not store more than 10,000 orphan transactions;
  - Does not forward orphan transactions/blocks;
  - Does not forward double-spend transactions;
  - Does not forward the same block or transaction to the same peer;
  - Does not forward or process non-standard transactions;
  - **Bans IP addresses** that misbehave;
  - Keeps a **DoS score** for each peer;
  - **Penalizes peers** that send duplicate/expired/invalid signature messages;
  - **Disconnects from peers** that send messages that fail to comply with the rules;
  - Stores only UXTO (unspent transaction output set) in memory
  - Checks all inputs are unspent before fetching a transaction from disk to memory – thus preventing a type of DoS, known as **continuous hard disk activity DoS**

Eclipse Attack

- An information eclipse attack is an attack where a malicious user gains control over a node's access to information in the peer-to-peer network.
- An eclipse attack is not easily performed, as it has three prerequisites:
- The adversary should possess a large number of IP addresses and machines (or botnets)
- The victim should have a public IP address (for example, not hidden behind Network Address Translators or not using anonymizer tools, like TOR).
- The adversary is able to make the victim restart its Bitcoin client, for example through a DDoS attack (or if the victim restarts the client due to power/network failure or software update).

Eclipse Attack

- If the above criteria are met then:
  - **The adversary can monopolize all of the victim's outgoing and incoming connections**, effectively isolating the victim from the rest of the network.
  - Thus, the adversary can control the victim's view of the blockchain.
- Further to defrauding the victim, the adversary can use an eclipse attack to:
  - Split the mining power in the network.
  - Perform an 51% attack with less than 50% mining power.
  - Perform selfish mining more easily, by splitting the mining power of honest nodes.
  - Double-spend transactions.
- Some of the countermeasures proposed by E. Heilman (see bibliography) have already been introduced in the Bitcoin client (as of version 0.10.1)

Time-jacking

- The Bitcoin network spans the globe. One of the issues this creates, is that nodes are in different time zones.
- Time is extremely important as it is used to determine the validity of new blocks.
- So, when establishing new connections, the protocol forces nodes to exchange their system time.
- Each node maintains a counter, which represents the median network time of its peers. The counter reverts to system time, if the median differs from it by more than 70 minutes.
- By announcing inaccurate timestamps when connecting to a node, an attacker can alter a node's network time counter and deceive it into accepting an alternate blockchain.
- This can significantly increase the chances of a successful double-spend.

Flood attack

- A flood attack is the process of sending thousands of nano-value transactions, in order to fill the blocks to the maximum size.
- This will create delays to other legitimate transactions, thus delaying the whole network and increasing confirmation time for all transactions.
- A flood attack is performed very easily, with the attacker just sending thousands of transactions to himself.
- However, it is expensive to sustain for a long time, due to transaction fees.
- In July 2015, a flood attack hit the Bitcoin network, leaving more than 80,000 unconfirmed transactions in the mempool.

Selfish Mining

Selfish Mining

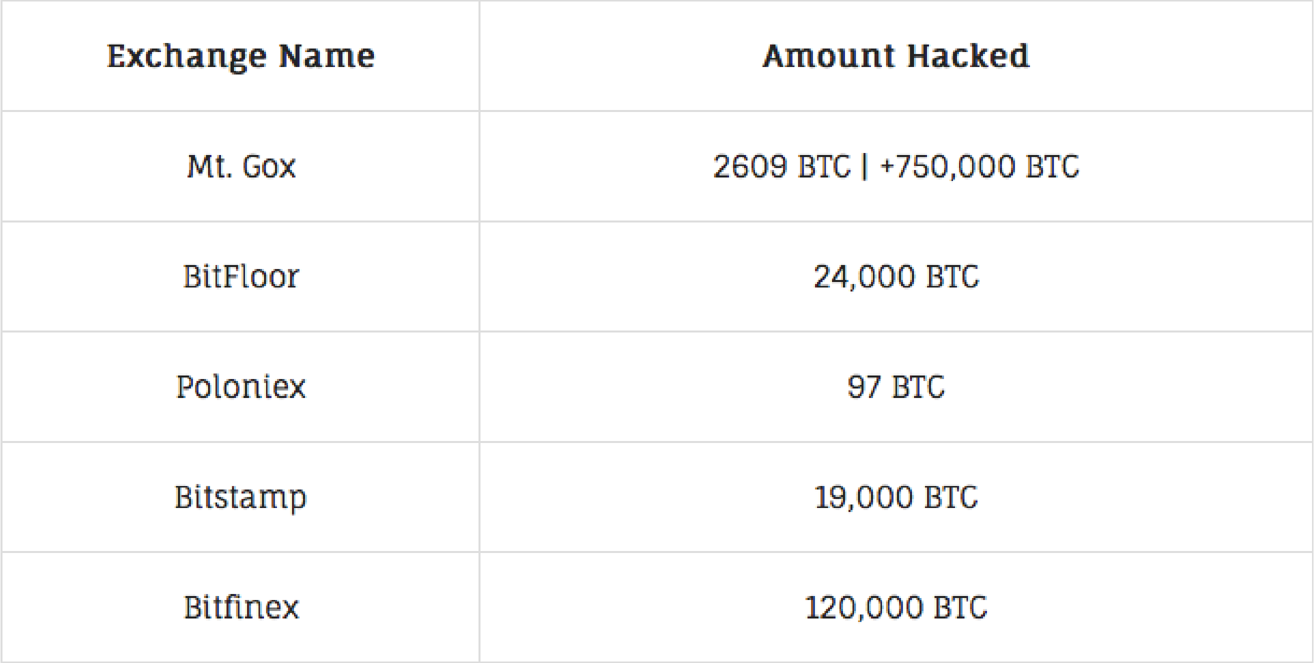
- Selfish mining is an attack on the integrity of the Bitcoin network, which can be used by large miners to increase their returns by not playing fair.
- Here is how it works:
- The selfish miner starts building a chain of blocks, but does not publish and distribute it to the rest of the network. Obviously, the selfish miner needs to have large mining power and a bit of luck to do this.
- When the rest of the network is about to catch up with the selfish miner, the miner a releases a portion of the chain to the public.
- Because the chain of the selfish miner will be longer and more difficult, the rest of the network will discard the blocks of other miners and will adopt the chain of the selfish miner.
- This strategy is repeated to ensure that the private chain built by the selfish miner will always be better (longer and more difficult) that its competitors

Selfish Mining - Consequences

- The computing power of honest miners is wasted, as they repeatedly find themselves working on the wrong chain.
- As a result, selfish miners increase the impact of their own mining power on the network and enjoy additional power and profits.
- Selfish mining increases transaction confirmation times, because transactions confirmed by the selfish miner in private, are not broadcast to the public immediately.
- Selfish mining also increases the threat of double spending, as both honest and selfish miners can add mutually exclusive transactions to the private and public chains.
- It is estimated that a malicious miner needs to control only one third of the network’s mining power to launch and sustain this type of attack (33% attack).

Other types of attacks

- Typical target: third-party (and, thus, centralized) exchanges
- Examples of bitcoin hacks

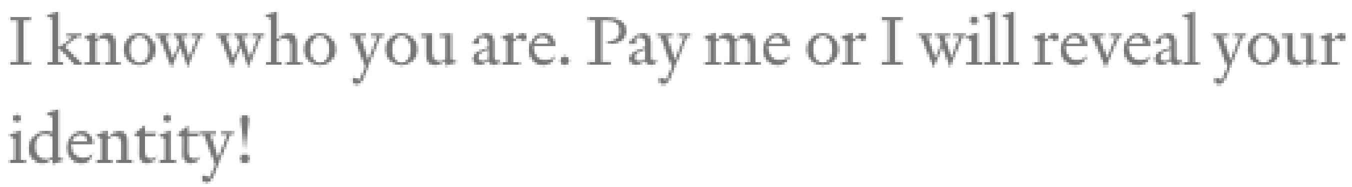


Exchange Name	Amount Hacked
Mt. Gox	2609 BTC | +750,000 BTC
BitFloor	24,000 BTC
Poloniex	97 BTC
Bitstamp	19,000 BTC
Bitfinex	120,000 BTC

Source: https://coinsutra.com/biggest-bitcoin-hacks/

Recently: dusting attack

- Attacker’s goal: to collect (almost) all your addresses
- How: by sending you a tiny amount (“dust”) and then trying to track your UTXOs
- Then: phishing or blackmail

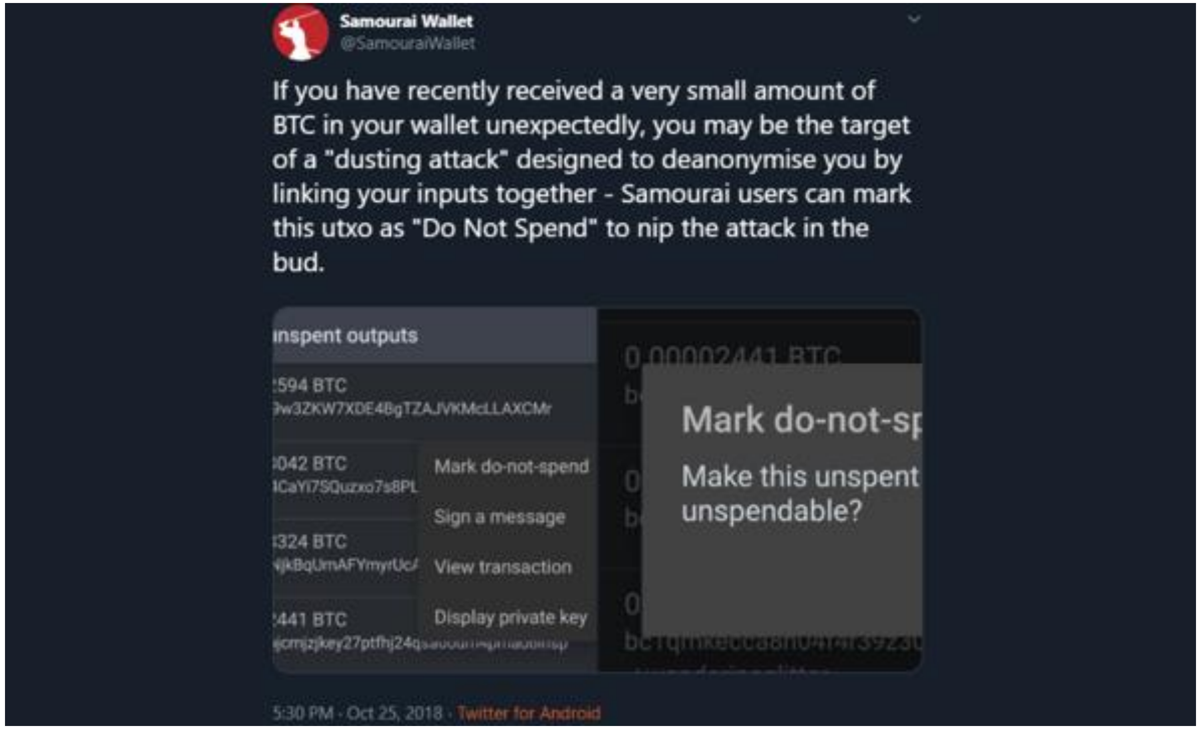


I know who you are. Pay me or I will reveal your identity!

Also: The case of Litecoin

Recently: dusting attack

- Warning by Samourai Wallet



Samourai Wallet
@SamouraiWallet

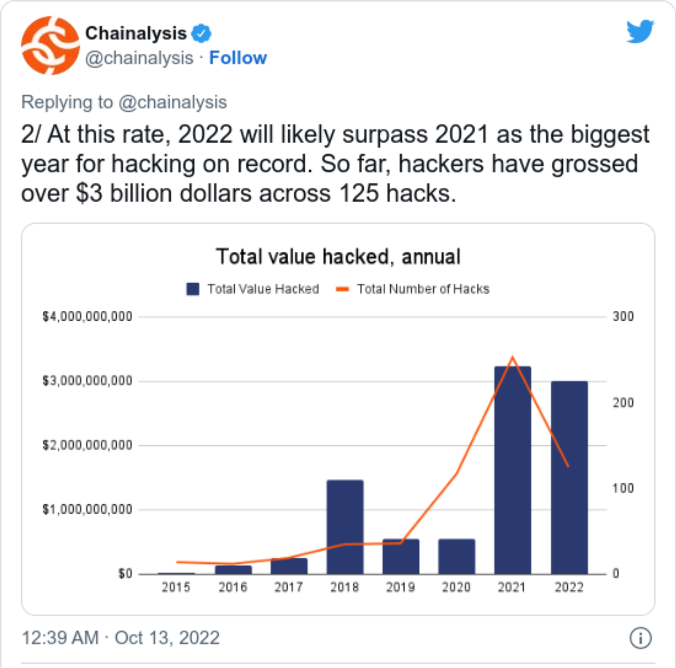
If you have recently received a very small amount of BTC in your wallet unexpectedly, you may be the target of a "dusting attack" designed to deanonymise you by linking your inputs together - Samourai users can mark this utxo as "Do Not Spend" to nip the attack in the bud.

5:30 PM · Oct 25, 2018 · Twitter for Android

The case of bridge attacks

Attacks on bridges

- Briefly: the broad field of DeFi has experienced a massive wave of attacks
- Why? Technical flaws related to interoperability (among others)
- Indicative examples (source: Bloomberg)

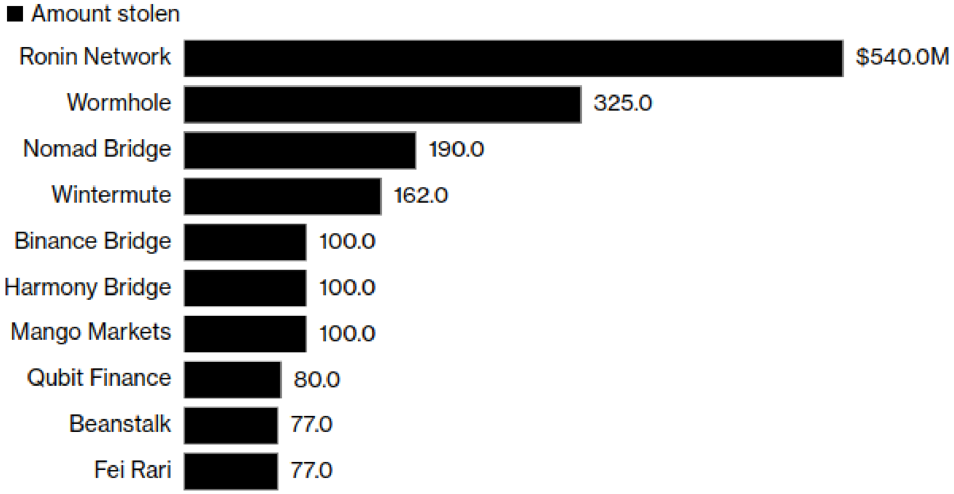


Chainalysis
@chainalysis · Follow

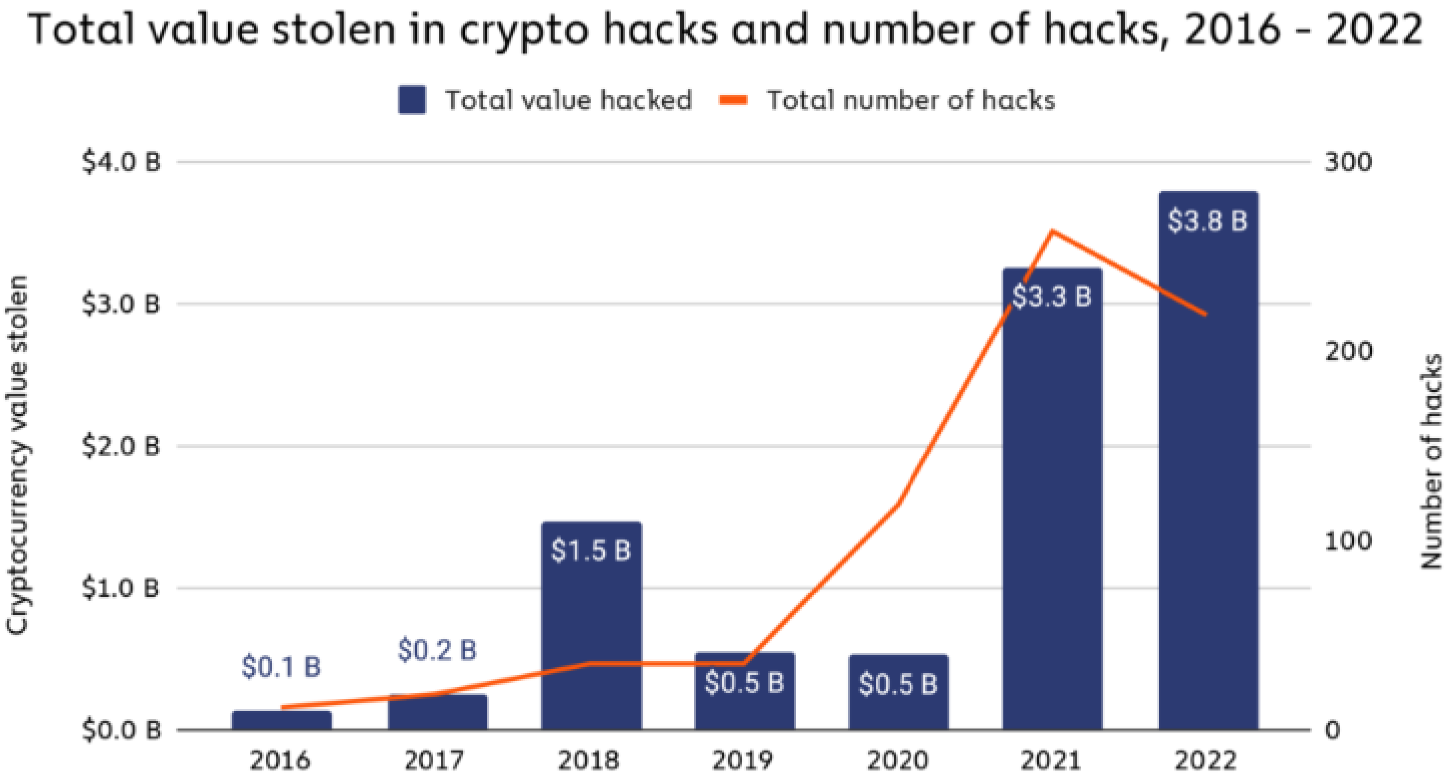
Replying to @chainalysis

2/ At this rate, 2022 will likely surpass 2021 as the biggest year for hacking on record. So far, hackers have grossed over $3 billion dollars across 125 hacks.

12:39 AM · Oct 13, 2022



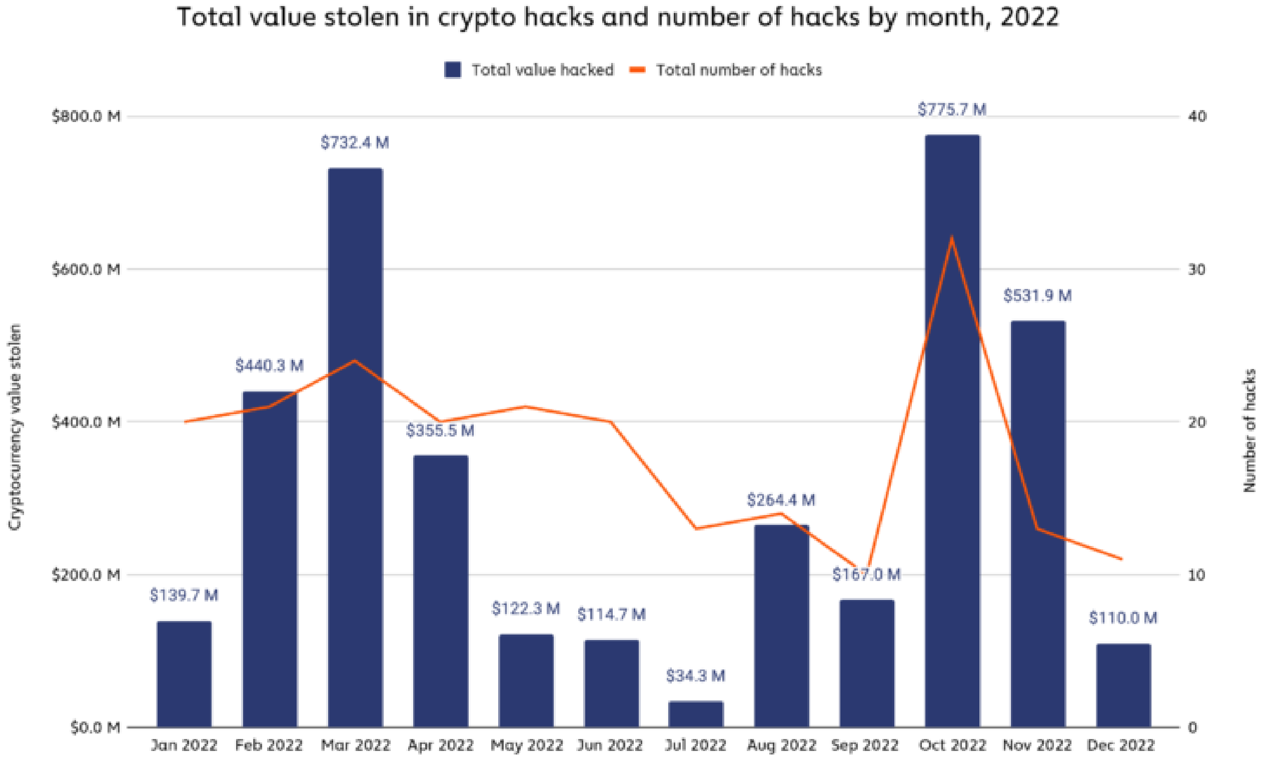
The size of hacks and the (recent) position of DeFi



Updated compared to previous slide (retained for comparison purposes)

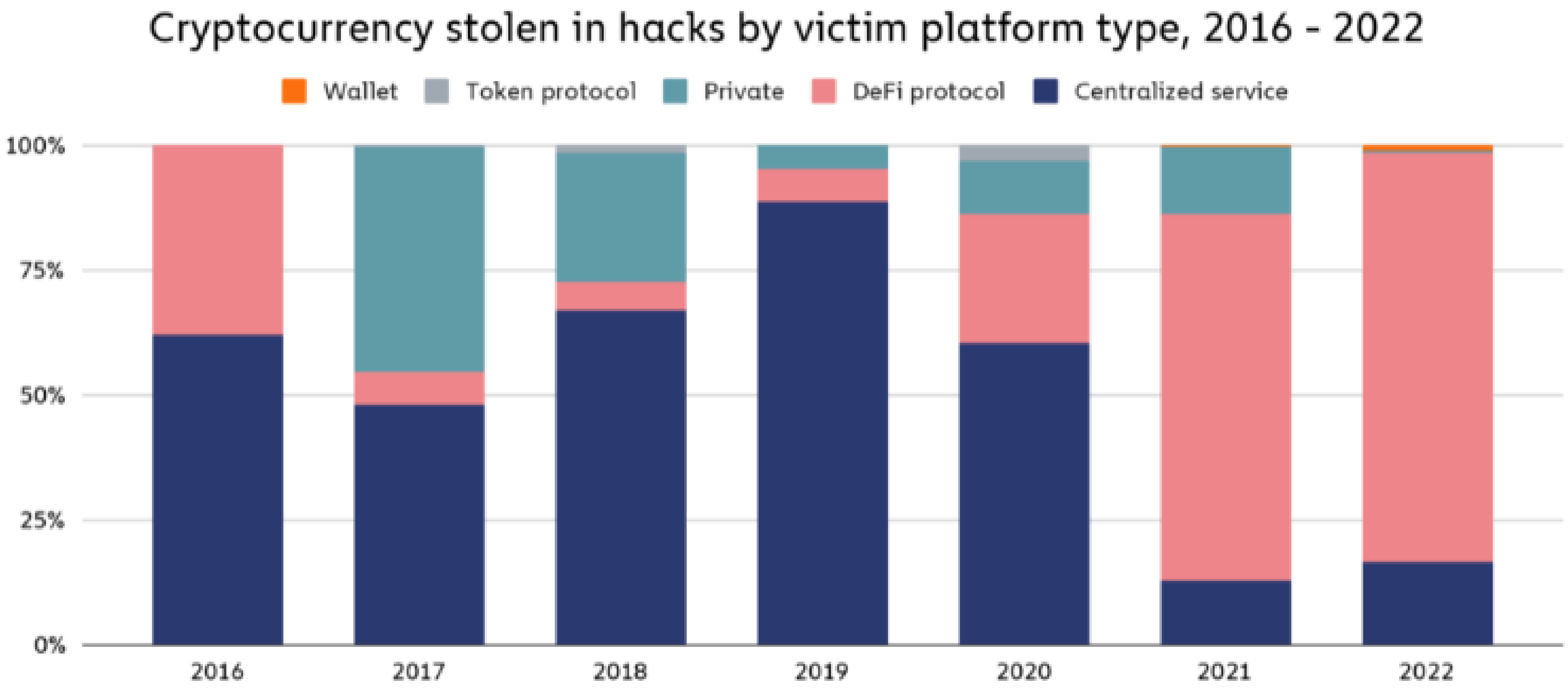
Source: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

The size of hacks and the (recent) position of DeFi



Source: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

The size of hacks and the (recent) position of DeFi



Source: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

Attacks on bridges

- In Web3, interoperability has a key position (plus, expected to play an instrumental role)
- Bridges: a relatively recent technical term referring to the technological solution enabling the cross-chain operations (more about interoperability in future sessions)
- In the context of cross-chain communication (quick reminder: blockchain as a distributed network relying on message exchange) different protocols need to communicate
- This “diversity” opens the gates for malicious exploitation
- Let’s discuss. Why?
- Different designs & implementations (often relying on different assumptions)
- Often ad-hoc integration schemes including the exchange of data (this is also related to lack of purpose-specific standards)
- [more to discuss]

Attacks on bridges

- In this article a number of exploits are reported as follows:
  - Flaws in validators
  - Control of validators
  - Falsified deposits
- In addition, human factors also are part of this ‘game’:
  - All imaginable aspects to social engineering
  - Including phishing attacks
- Measures:
  - Continuous learning
  - Continuous auditing and monitoring at various levels, i.e., not only the source code of smart contracts, but also other network/protocol measurements

Web3 attacks: Protection framework

- In this a16z's article a general framework is proposed aiming to help us better understanding, at a high-level, the majority of recent Web3 attacks.

- This framework is quite simple, yet very informative, taking into account the following aspects:
  1. Profile of attackers
  2. Level of sophistication
  3. Degree of automation

- Also, the framework is applied across a range of domains spanning from supply chains to market manipulations

Bridge Attacks: Still a Thread in 2023

- According to this article, bridge attacks will remain a hot spot in 2023.
- Also, a series of related views are reported which are summarized as follows:
  - Bridges exhibit “inherent vulnerability”, e.g., one point of failure affects the whole system.

    - Theo Gauthier, founder and CEO, Toposware

  - Zero-knowledge proofs can contribute to the security of bridges in contrast to traditional interoperability techniques which rely on the exchange of states between the connected networks.

    - Mudit Gupta, Chief Information Security Officer, Polygon

  - Machine learning (ML) can be utilized for detecting abnormal network behaviors that are associated with attacks on bridges. For this purpose, ML can be combined with security techniques.

    Gustavo Gonzalez, Developer, Open Zeppelin

The (important) role of simulations

Simulations

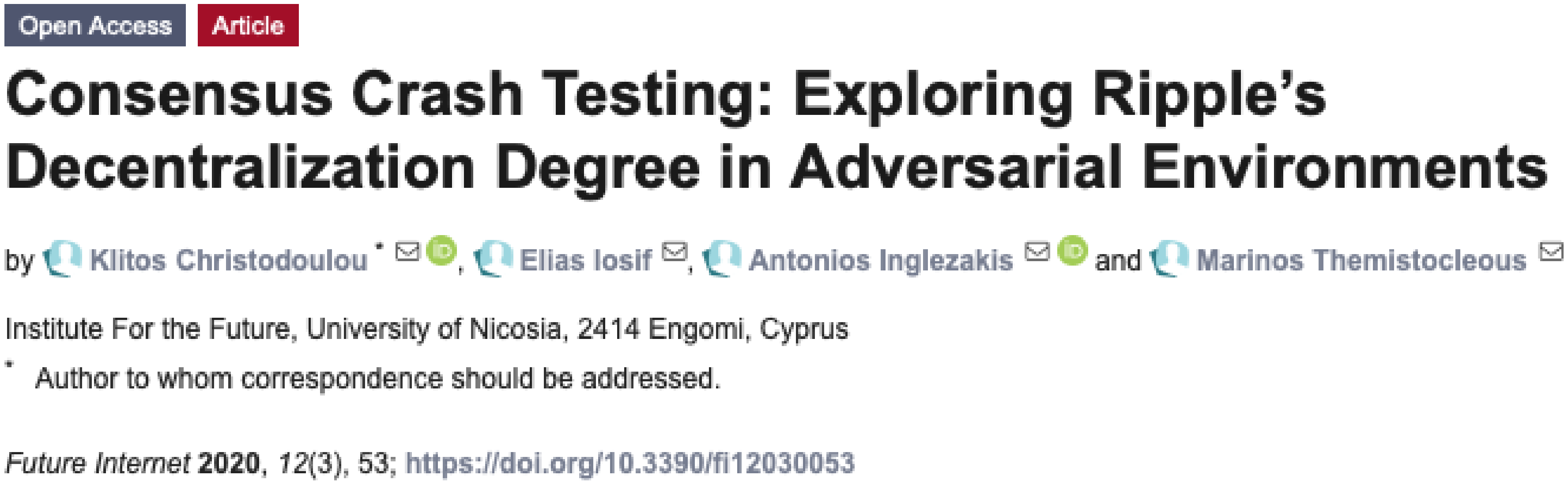
- Simulators can have a key contribution to the study of attacks as well as related scenarios
- Also, widely-used in numerous other domains, e.g., civil aviation
- Unfortunately, this area is relatively under-developed for the case of blockchains

- Examples of recent studies:
  - BlockSim: An Extensible Simulation Tool for Blockchain Systems (2020)
  - BlockSim: Blockchain Simulator (2019)

- Such studies can be regarded as a good baseline, however many enhancements are needed as
  - Often, they require intervention at the code level
  - Certain hypotheses are adopted
  - The supported configuration is appropriate for certain scenarios

Simulations: XRP ledger

- In many cases, simulations let us better study and understand other aspects, such as decentralization
- Use case: Ripple (XRP ledger)



Open Access Article

Consensus Crash Testing: Exploring Ripple's Decentralization Degree in Adversarial Environments

by Klitos Christodoulou *, Elias Iosif, Antonios Inglezakis and Marinos Themistocleous

Institute For the Future, University of Nicosia, 2414 Engomi, Cyprus

* Author to whom correspondence should be addressed.

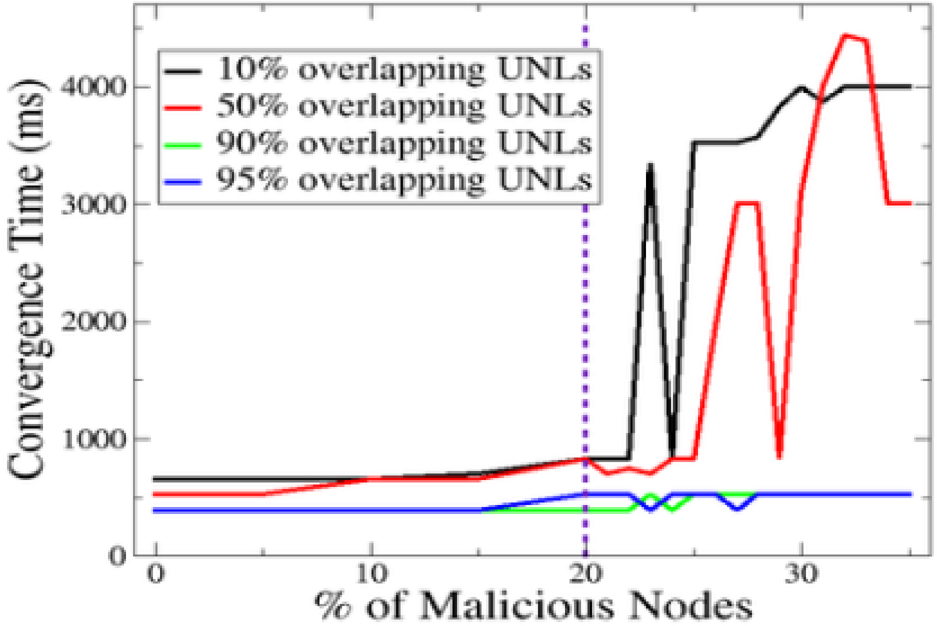
Future Internet **2020**, *12*(3), 53; https://doi.org/10.3390/fi12030053

- Source

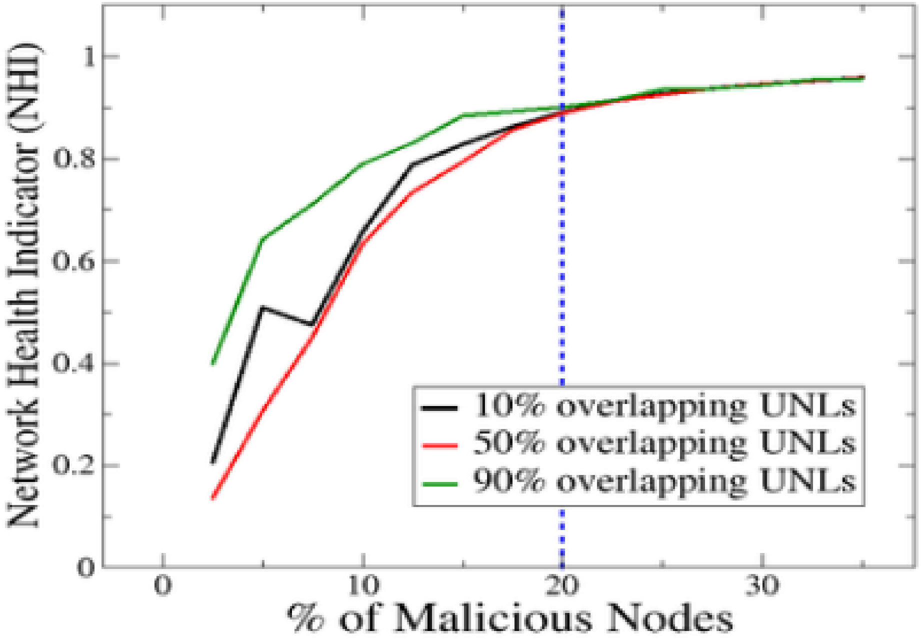
Simulations: XRP ledger - Parameters

- Percentage of malicious nodes in the network
- Percentage of UNL overlap
  - UNL: a mission-critical list containing the validators
- Performance-related metrics
  - Convergence Time
  - Network Health Indicator

Simulations: XRP ledger - Results



Simulations: XRP ledger - Results

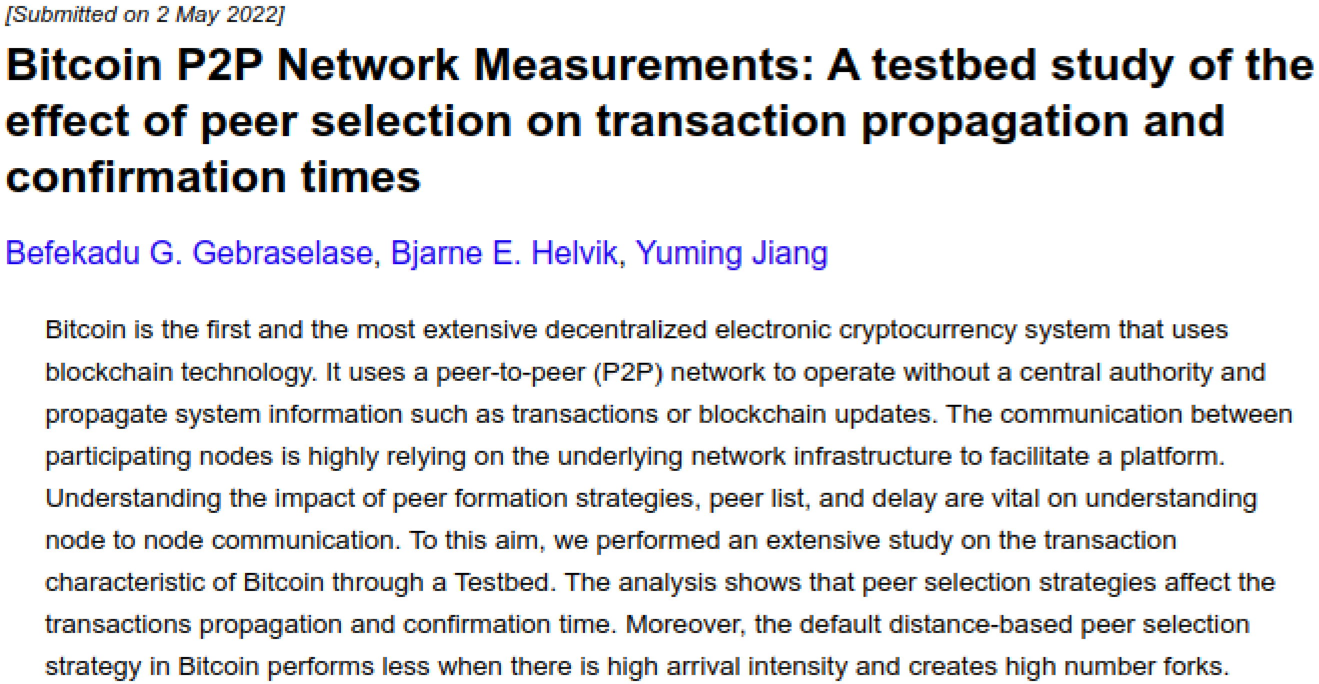


Simulations: XRP ledger - Conclusions

- When a low percentage (0–20%) of malicious nodes is present, the **centralization degree** of the network, as implemented by the UNL's percent overlap, can be significantly **relaxed**.
- A strong UNL overlap, for example 90–99%, is needed only when the percentage of malicious nodes exceeds a critical threshold, which equals to 20%.
- Opportunity for engineering an **adaptive scheme** for dynamically determining an **optimal** (or nearly-optimal) UNL overlap.
- The **optimization problem** deals with the identification of the lowest possible UNL overlap (thus **enhancing the decentralization degree** of the network)

Simulations: Benchmark by Befekadu et al.

- “Bitcoin P2P Network Measurements: A testbed study of the effect of peer selection on transaction propagation and confirmation times” (2022)
- Link to arxiv



[Submitted on 2 May 2022]

Bitcoin P2P Network Measurements: A testbed study of the effect of peer selection on transaction propagation and confirmation times

Befekadu G. Gebraselase, Bjarne E. Helvik, Yuming Jiang

Bitcoin is the first and the most extensive decentralized electronic cryptocurrency system that uses blockchain technology. It uses a peer-to-peer (P2P) network to operate without a central authority and propagate system information such as transactions or blockchain updates. The communication between participating nodes is highly relying on the underlying network infrastructure to facilitate a platform. Understanding the impact of peer formation strategies, peer list, and delay are vital on understanding node to node communication. To this aim, we performed an extensive study on the transaction characteristic of Bitcoin through a Testbed. The analysis shows that peer selection strategies affect the transactions propagation and confirmation time. Moreover, the default distance-based peer selection strategy in Bitcoin performs less when there is high arrival intensity and creates high number forks.

Simulations: Benchmark by Befekadu et al.

- “Bitcoin P2P Network Measurements: A testbed study of the effect of peer selection on transaction propagation and confirmation times” (2022)
- Overview of benchmark setup (for details see Section III of paper)

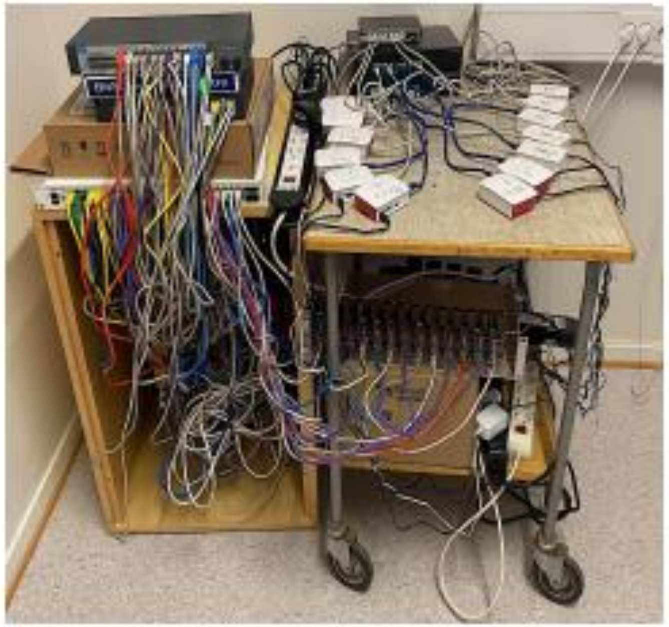


Figure 1. Testbed setup (104 Raspberry pis, 6 switches, 2 blade rack)

Simulations: Side note

- In many cases, in the literature/communities/etc. the relation of AI and blockchain technologies is mentioned/glorified/etc.

- Unfortunately, for the vast majority of those cases this relation is not explained.
  - Why?

- Consider, for example, the finding:

  "The **optimization problem** deals with the identification of the lowest possible UNL overlap (thus **enhancing the decentralization degree** of the network)"

  - Do you see any AI-related contribution here?

Bibliography

References

- Karame and Elli Audroulaki (2016). “Bitcoin and Blockchain Security”. Artech House, Inc., Norwood, MA, USA.
  - Chapter 4
- Research article (Section III and Section IV)
  - Mauro Conti, Sandeep Kumar E, Chhagan Lal and Sushmita Ruj (2017). “A survey on security and privacy issues of bitcoin” arXiv preprint https://arxiv.org/pdf/1706.00916.pdf

    This article stands a systematic survey of the current security and privacy issues of the Bitcoin blockchain.Numerous attack types are presented along with the respective countermeasures. In addition, this article covers privacy and anonymity issues.

Additional Bibliography (optional)

- Ittay Eyal, Emin Gun Sirer. **Majority is not Enough: Bitcoin Mining is Vulnerable** (here)
- Ethan Heilman. **One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner** (here)
- Ethan Heilman, Alison Kendler, Aviv Zohar, Sharon Goldberg. **Eclipse Attacks on Bitcoin's Peer-to-Peer Network** (here)
- Marie Vasek, Micah Thornton, Tyler Moore. **Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem** (here)
- Neil Levine, Brian & Shields, Clay & Boris Margolin, N. **A Survey of Solutions to the Sybil attack. Technical Report of Univ of Massachussets Amherst.** (here)
- Pass , R., Seeman, L., Shelat, Abhi . **Analysis of the Blockchain Protocol in Asynchronous Networks** (here)

Additional Bibliography (optional)

- Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. **Optimal Selfish Mining Strategies in Bitcoin**. (here)
- Garay, Juan & Kiayias, Aggelos & Leonardos, Nikos. **The Bitcoin Backbone Protocol: Analysis and Applications**. (here)
- Decker, C., Wattenhofer, R. **Bitcoin transaction malleability and MtGox**. (here)
- Siamak Solat, Maria Potop-Butucaru. **ZeroBlock: Preventing Selfish Mining in Bitcoin**. [Technical Report] UPMC University of Paris 6 (here)

- Lightweight article summarizing Vitalik's opinion about the future of rollups

- Video including a number of zero-knowledge proof examples

Conclusions

Conclusions

- A wide number of malicious attacks can be launched on a digital currency network.
- One type of attacks involves controlling the network's mining power. The aim here may be to increase own profits (e.g. selfish mining), double-spend (e.g. 51% attack) or simply attack the network (e.g. flood attack).
- Another type of attacks involves attacking individual nodes. The goal here may be to steal from the nodes under attack or simply remove their mining power from the network (e.g. information eclipse attack, time-jacking, DoS attack).
- The Bitcoin protocol, as well as the core Bitcoin client, have built-in countermeasures to deal with the most common types of attacks.
- New protection mechanisms are continuously incorporated in new editions of client software.
- As the network becomes larger and more diversified, it essentially protects itself from certain attacks (for example, it would be very difficult today to acquire the mining power needed to launch a 51% attack).
- Interestingly, large miners may have more incentives to protect the network (and hence their investments) rather than attacking it.

UNIVERSITY *of* NICOSIA

Instructor’s Email:

iosif.e@unic.ac.cy