Cybersecurity and Society
– Blockchain Technology –

Ghada Almashaqbeh

Computer Science and Engineering Dept., UConn

The UConn E^2 Program, Summer 2022

About Me

- Columbia (PhD in CS, 2019) ⇒ Entrepreneur (CacheCash, NuCypher) ⇒ UConn (Assistant Prof., 2020)
- Research interest:
  - Cryptography (theory and applied)
  - Security and privacy
  - Distributed systems (blockchain-based ones)
- More: https://ghadaalmashaqbeh.github.io/
- Email: ghada@uconn.edu

Outline

- Motivation
- Decentralized resource markets
- Criminal smart contracts

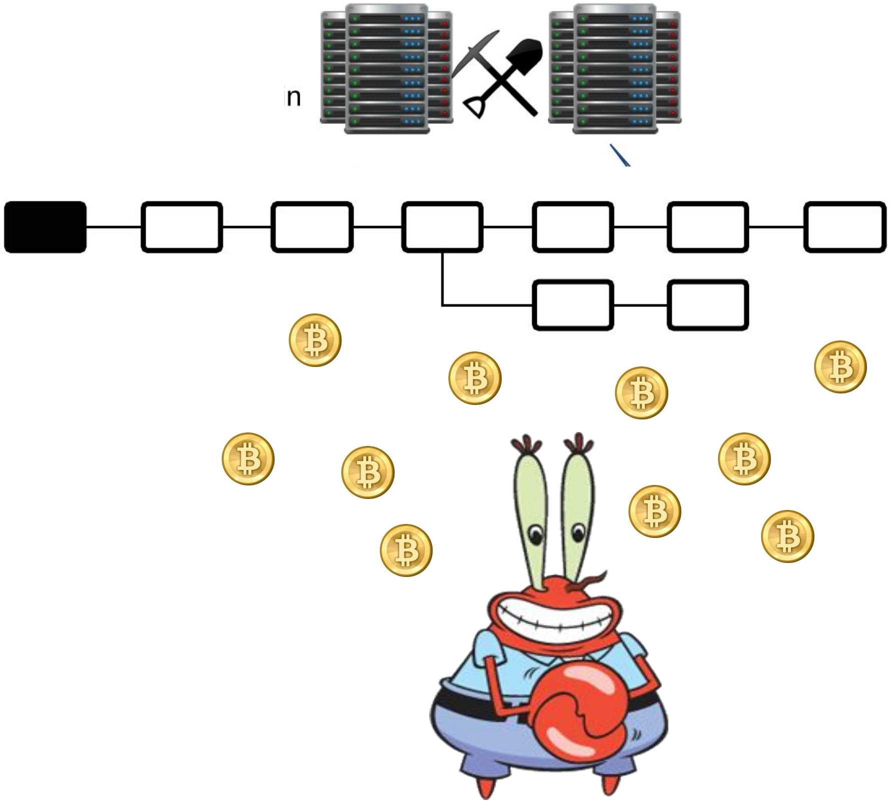
What is cybersecurity? Does it impact you/society?

Heard about blockchains? Do they impact you/society?

Once Upon A Time

Centralized Currency

Decentralized Currency



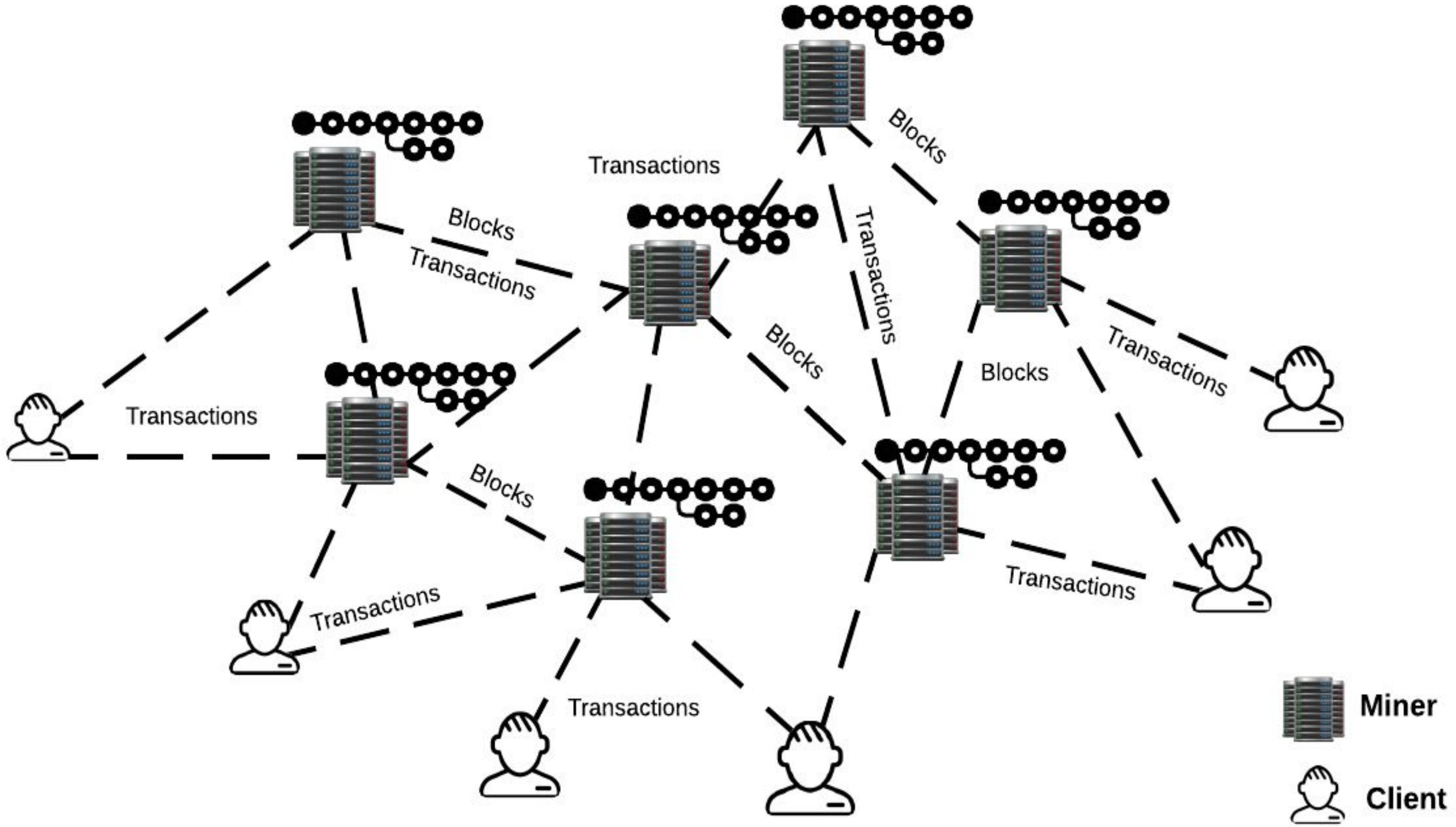
History

- A whitepaper posted online in 2008: “Bitcoin: A Peer-to-Peer Electronic Cash System,” by Satoshi Nakamoto.
- Described a distributed cryptocurrency system not regulated by any government.
- The system went live on January 2009.
- Now “Satoshi Nakamoto” is only associated with certain public keys on Bitcoin blockchain.
    - She/He/They was/were active on forums/emails/etc. until 2010.
- Currently there are hundreds of cryptocurrencies (https://coinmarketcap.com/).

Cryptocurrencies in A Nutshell

- The use of cryptographic primitives and distributed consensus protocols to secure virtual money creation and flow between various parties.
- Main components:
  - Players: miners and clients.
  - Transactions: messages exchanged.
  - Blockchain: an append only log.
  - Mining: extending the blockchain.
  - Consensus: agreeing on the current state of the Blockchain.

Cryptocurrencies Pictorially



Is it only about currency exchange?

- Interest has shifted towards providing a decentralized service on top of this medium.
- Lately blockchains on their own (without involving any currency) are used in several applications.
  - Mainly to support transparency and public verifiability.
  - Examples include healthcare, business management, and supply chains.

Decentralized Resource Markets

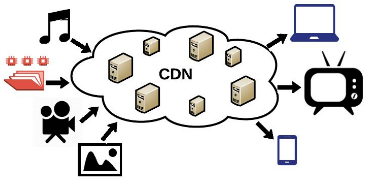
Traditional Service Systems

Central Management

Services

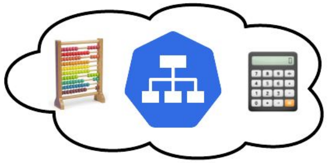
File Storage

justcloud.com OneDrive



Content Distribution

Akamai CLOUDFLARE fastly



Computing

Google Cloud Platform Microsoft Azure

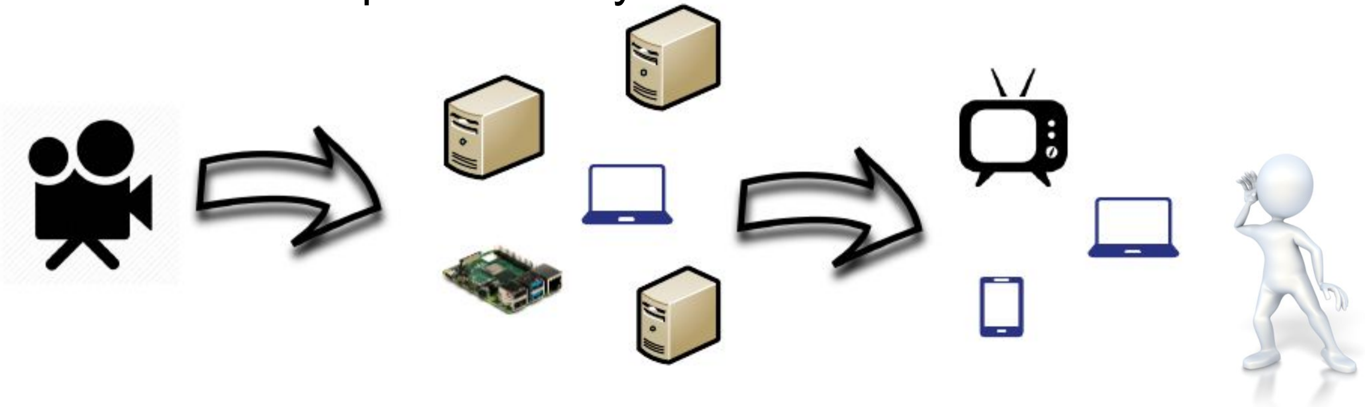
Traditional Service Systems

Central Management

- **Drawbacks:**
  - Costly and complex business relationships.
  - Over-provisioning service needs.
  - Issues related to reachability, visibility, flexibility, etc.

Decentralized Services

- Utilize P2P-based models to build dynamic systems.
- **Advantages:**
  - Flexible services.
  - Easier to scale with demand.
  - Extended reachability and lower latency.
  - Democratized and transparent ecosystems.

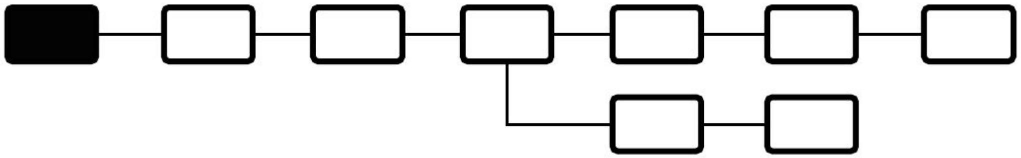


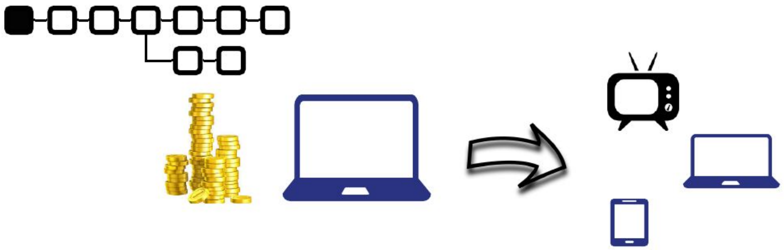
Cryptocurrencies and their blockchains ⇒

support payments,

accountability,

and governance in a fully decentralized way

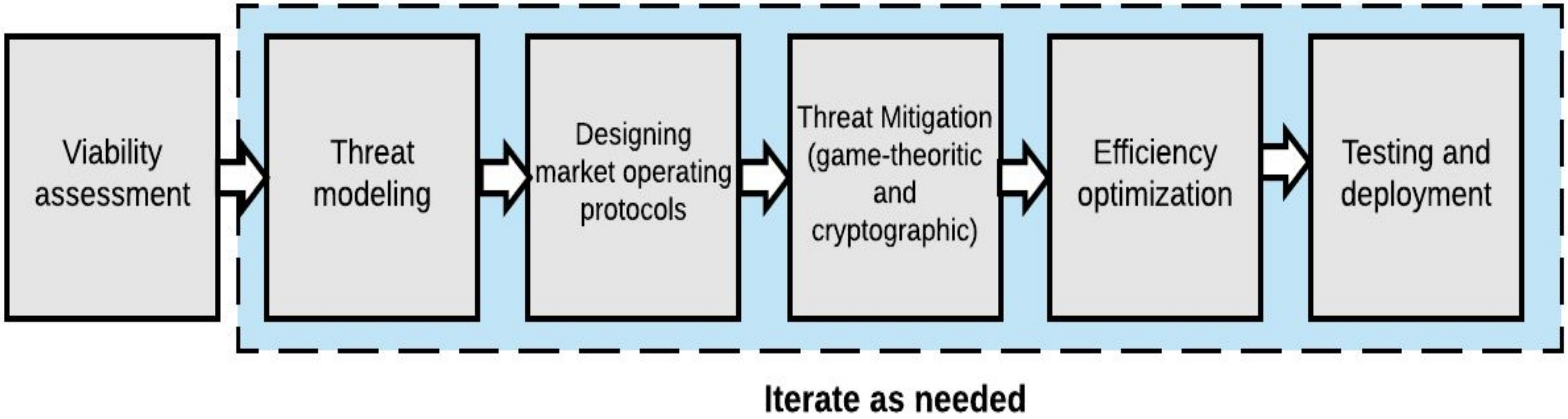




Problem solved?!

Open access work model, large scale system with monetary incentives ...

A Design Framework for Distributed Resource Markets



Viability assessment

Threat modeling

Designing market operating protocols

Threat Mitigation (game-theoritic and cryptographic)

Efficiency optimization

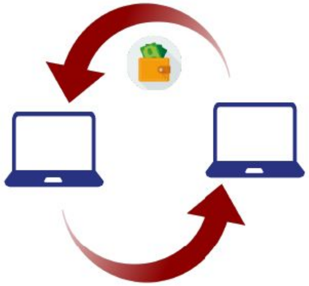
Testing and deployment

Iterate as needed

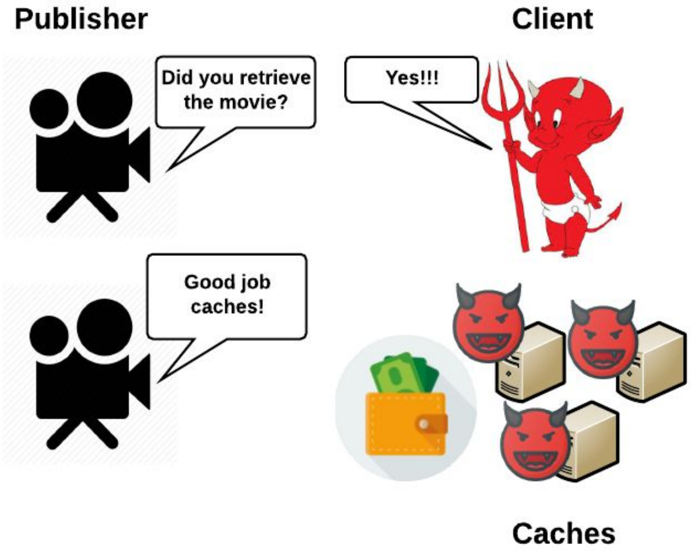
Threat Modeling

- An essential step to investigate all potential security risks.
  - A guiding design map, as well as a tool for assessing security.

Unique Issues in Distributed Resource Markets



Fair exchange is impossible



Accounting attacks

Cryptographic and Economic Security Measures

- Dealing with monetary incentives is challenging!
- Financially-motivated threats require economic mitigation techniques.
  - E.g., Detect and punish, service pricing.
- Usually rely on assuming rational players.

Optimize for Efficiency

- Seeking a practical adoption?
  - Testing and deployment.
  - Exploit every opportunity to boost system’s performance.
  - Look for the right trade-off between security and efficiency.

These markets are about crowdsourcing for benign purposes:

Creating equitable and transparent services

Criminal Smart Contracts

What is a smart contract?

- Simply an arbitrary program deployed by a user on a blockchain
- Miners will execute the code on demand
- Anyone can see the code and anyone can invoke that code
- So they are a form of decentralized computer programs!

Ethereum was born

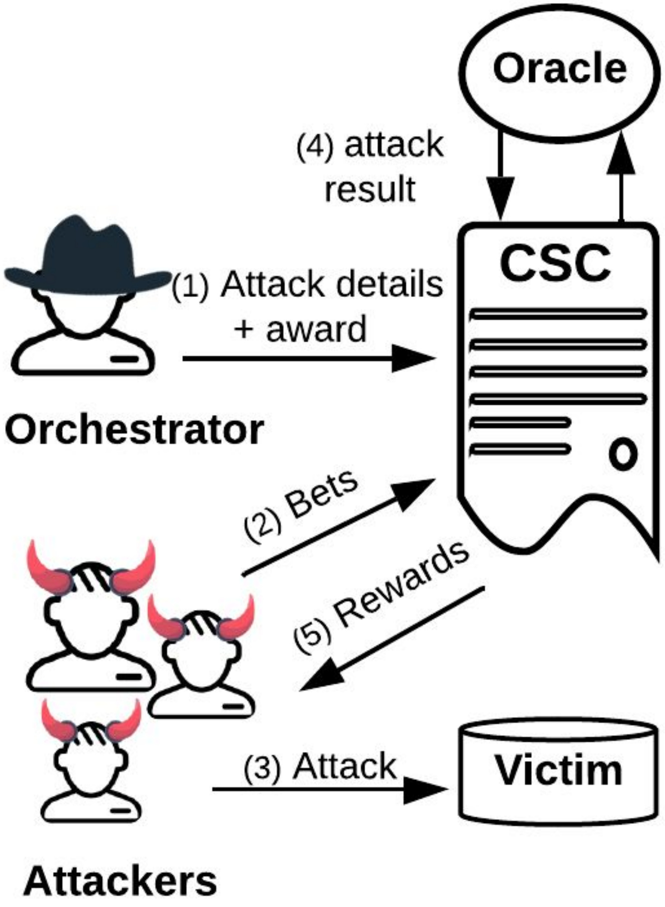
- The second biggest cryptocurrency after Bitcoin
- Launched in 2015
- View the miners as a global virtual computer to execute smart contracts. It is called Ethereum virtual machine (or EVM)
- These smart contracts are called dApps, and they are the core component of the Web 3.0 movement

Smart Contracts for Governance

- Encode all rules of a crowdsourcing activity.
  - So markets discussed earlier can utilize that.
- But attackers can utilize that as well:
  - A contract orchestrates an attack against real world targets.
  - Ransomware, denial of service, leaking secret documents, etc.

Criminal Smart Contracts

- Oracles play an important role
- A betting framework to allow collaboration of trustless attackers
- Incentive-based approach



Defending against CSCs is still an open problem

Conclusion

- Cybersecurity is crucial for daily life activities.
- Emerging technologies create new opportunities, but also new attacks.
- Continuous efforts are needed to keep our ‘digital’ society safe.

THANK YOU