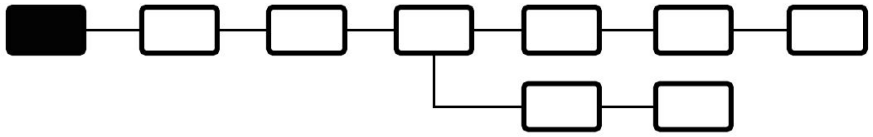
–On the Power of Smart Contracts– The Good and the Bad

Ghada Almashaqbeh
University of Connecticut

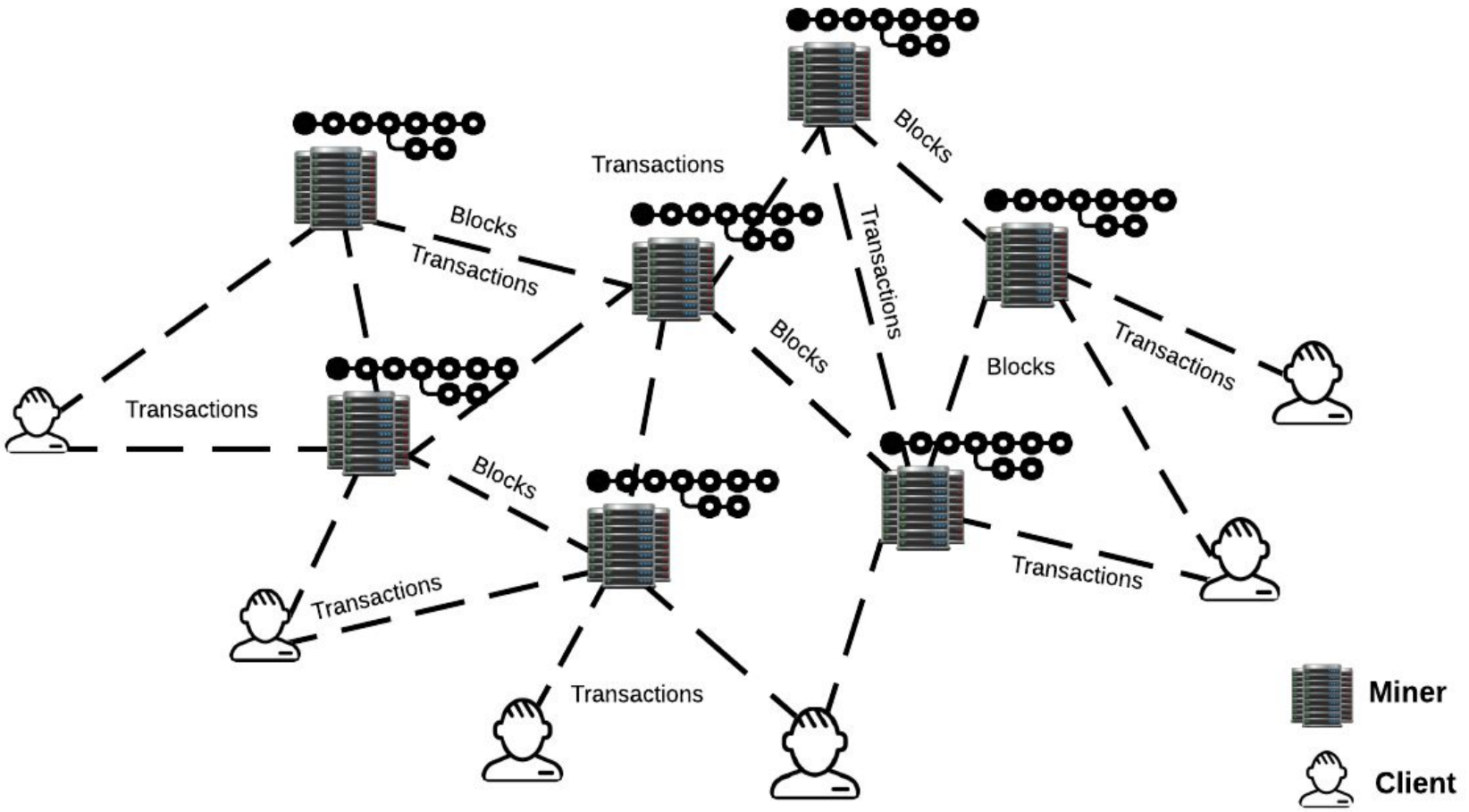
Heritage Medical Systems Annual Meeting
Dec 2022

Cryptocurrencies and Blockchain Technology

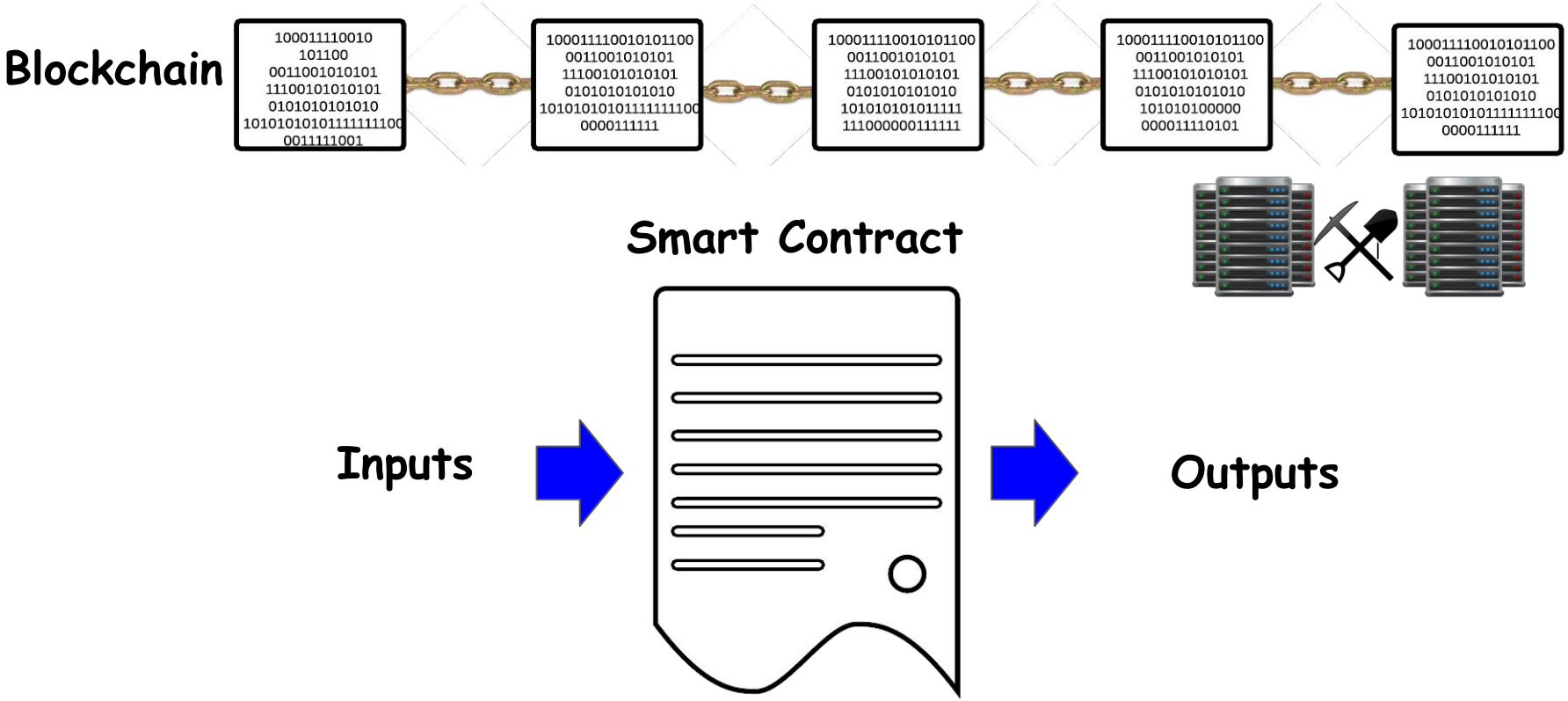
- An emerging economic force with huge interest.
- Early systems focused on providing a currency exchange medium.
- Newer systems provide a service on top of this medium.
  - E.g., Filecoin, Livepeer, NuCypher ....
  - Come under the umbrella of ***Web 3.0***
    - dApps, DeFi, etc.



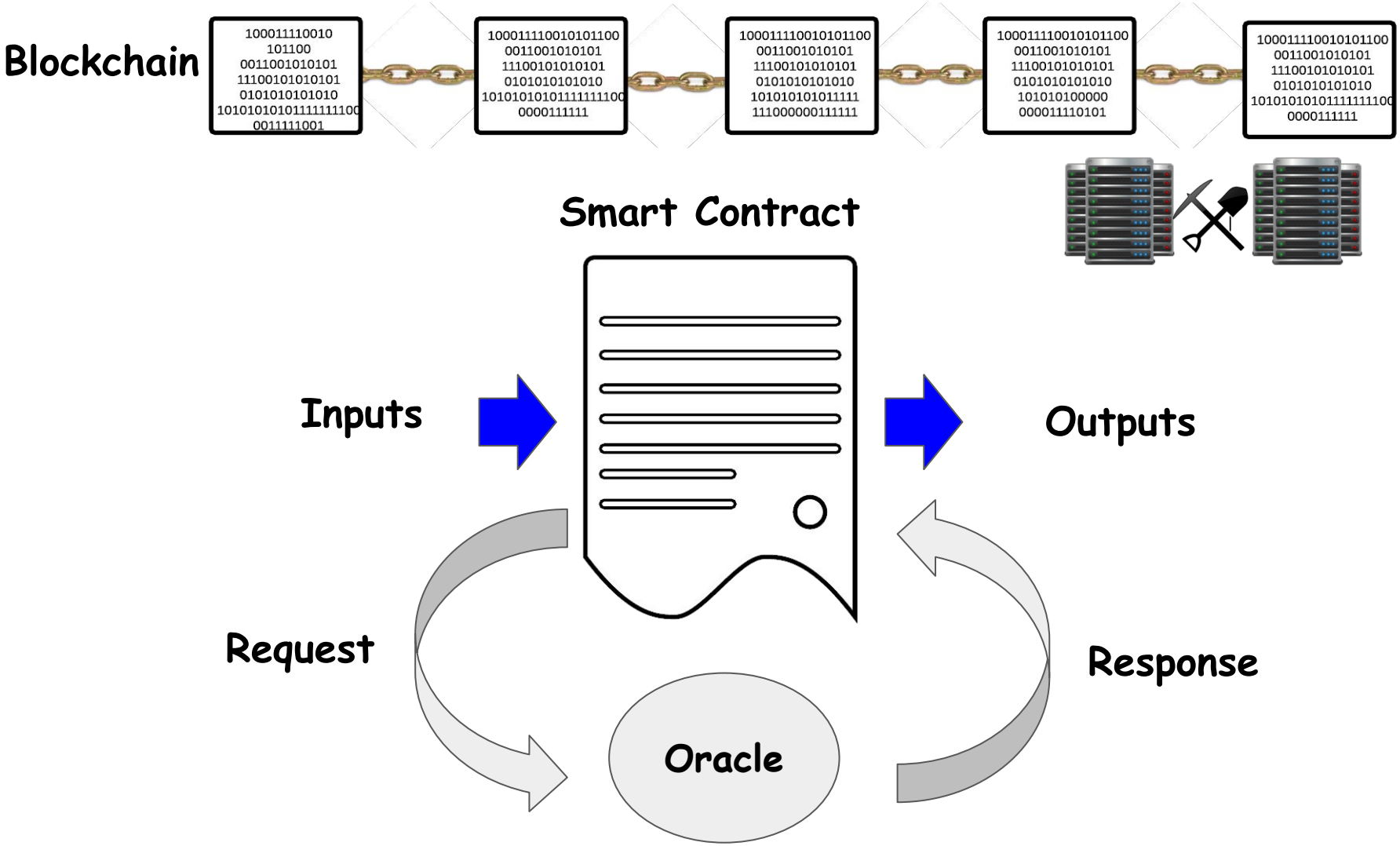
Pictorially



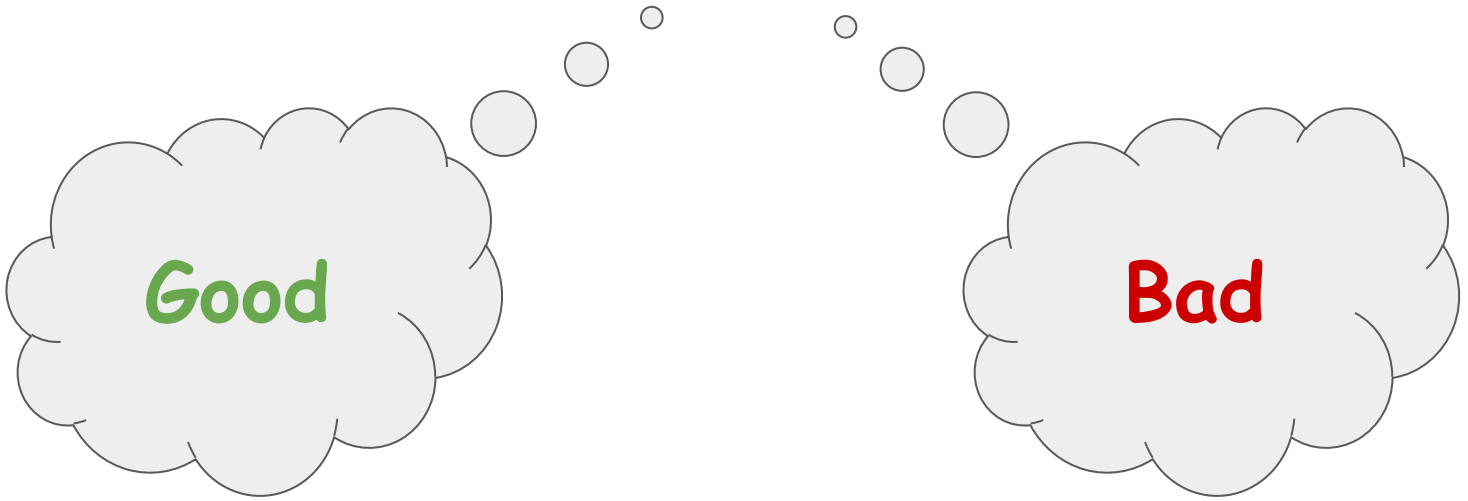
More - Smart Contracts



Even More - Real World Data Feeds

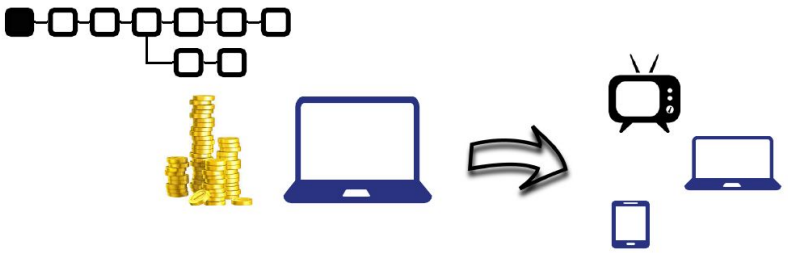


Many (Potential) Applications



Decentralized resource markets

Criminal smart contracts



The Good

Crowdsourcing for benign goals

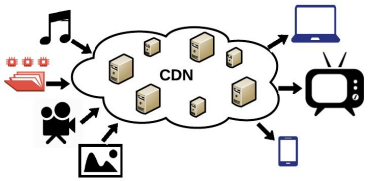
Traditional Service Systems

Central Management

Services

File Storage

justcloud.com OneDrive



Content Distribution

Akamai CLOUDFLARE fastly

Computing

Google Cloud Platform Microsoft Azure

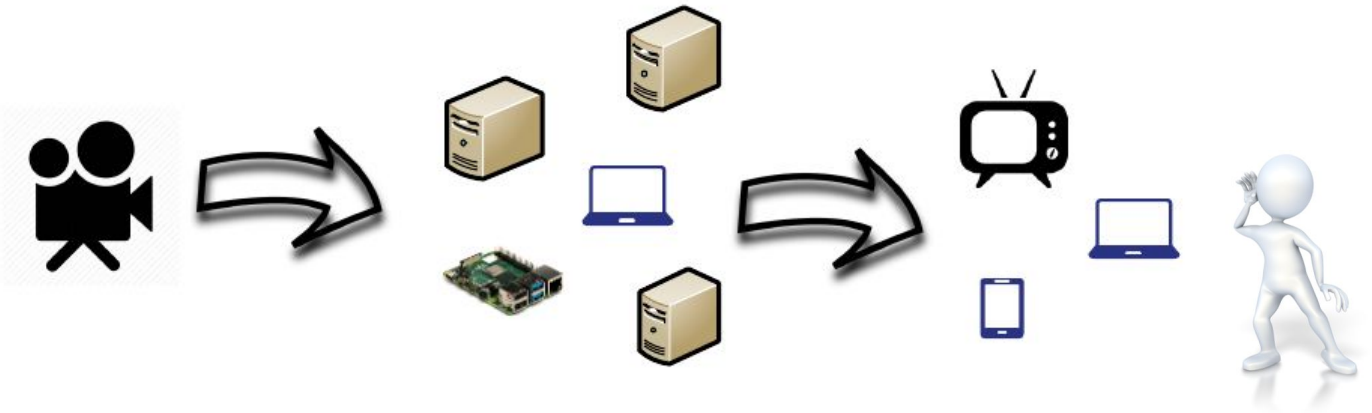
Traditional Service Systems

Central Management

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

Decentralized Services

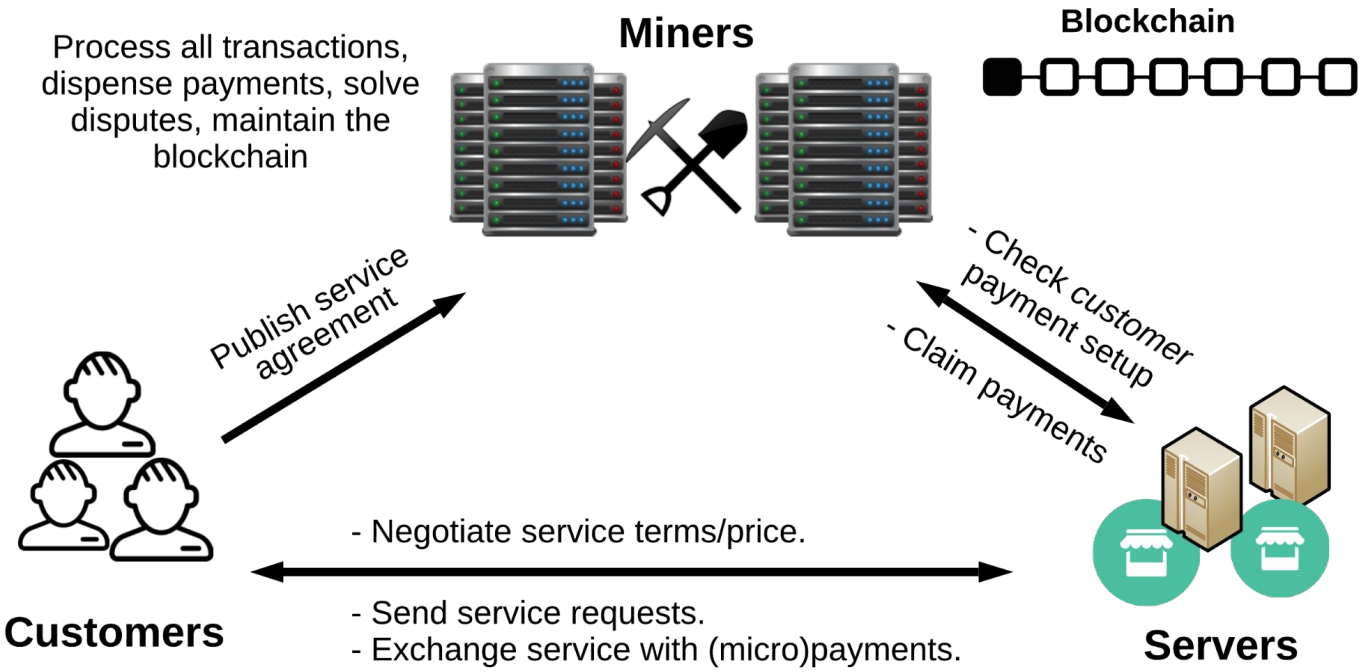
- Utilize P2P-based models to build dynamic systems.
- **Advantages:**
  - Flexible services.
  - Easier to scale with demand.
  - Extended reachability and lower latency.
  - Democratized and transparent ecosystems.



Cryptocurrency/Blockchain Utility

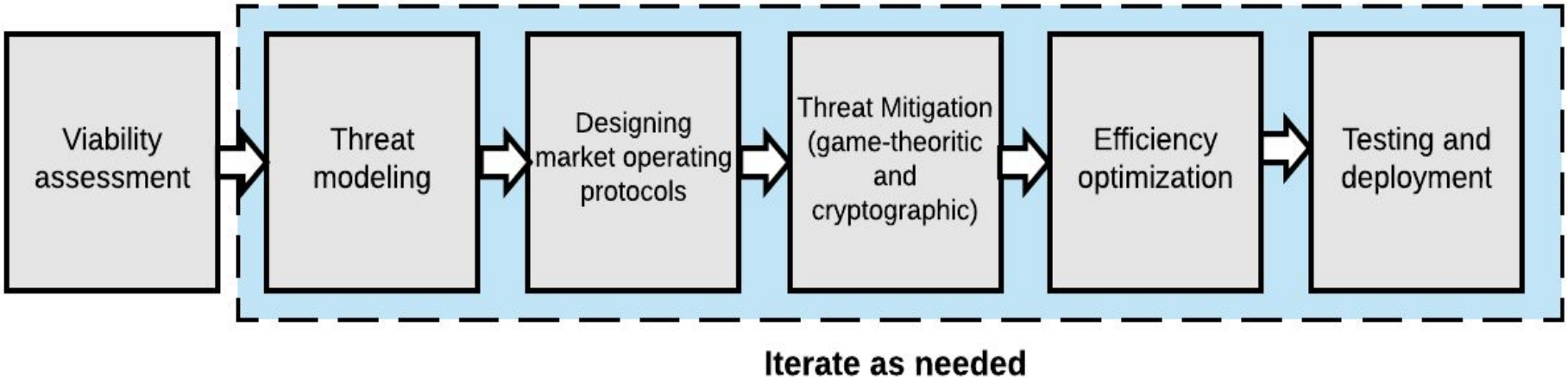
- Decentralized monetary incentives.
- Public verifiability and transparency.
- Automatic contract enforcement and decentralized governance.
  - Smart contracts come handy here!
  - E.g., the paradigm of tokens on top of Ethereum.
  - Main engine of Web 3.0

Decentralized Resource Markets



* G. Almashaqbeh, "Rethinking Service Systems: A Path Towards Secure and Equitable Resource Markets." USENIX ;login: Magazine, 2021.

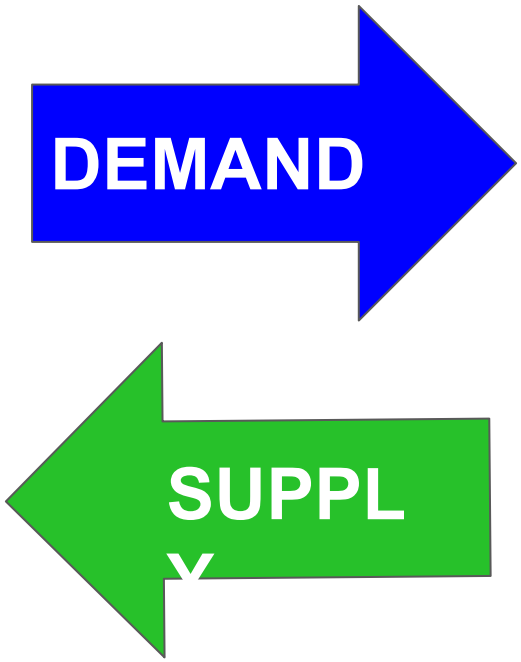
A Design Framework for Distributed Resource Markets



Viability Assessment

- An important step to assess the potential for practical adoption.

- Two sides of the equation:

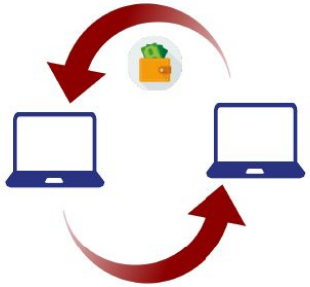


Threat Modeling

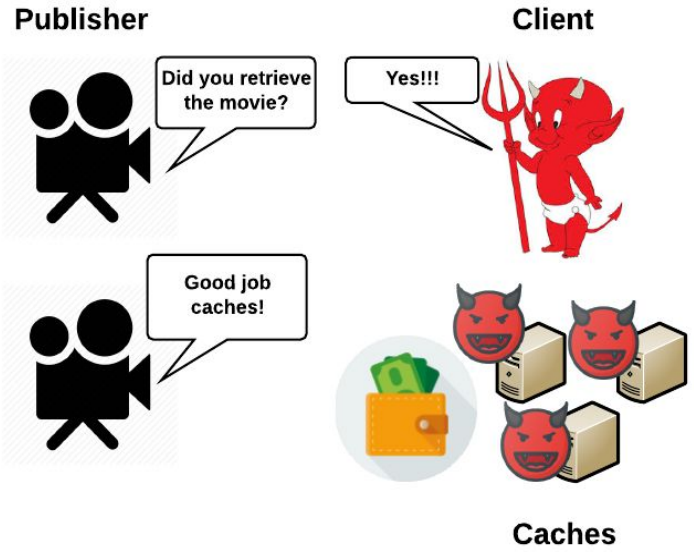
- An essential step to investigate all potential security risks.
  - A guiding design map, as well as a tool for assessing security.
- Requires frameworks capable of:
  - Dealing with large scale systems.
  - Explicitly account for financial motivations of attackers.

Unique Issues in Distributed Resource Markets

- **Fair-service exchange is impossible**.
  - Pay first or serve first?



- **Accounting attacks**.
  - Do servers earn their payments?

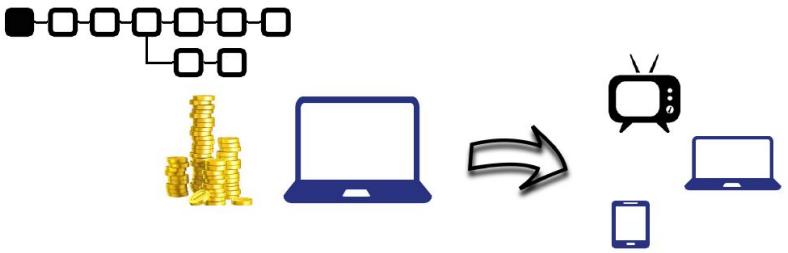


Cryptographic and Economic Security Measures

- 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

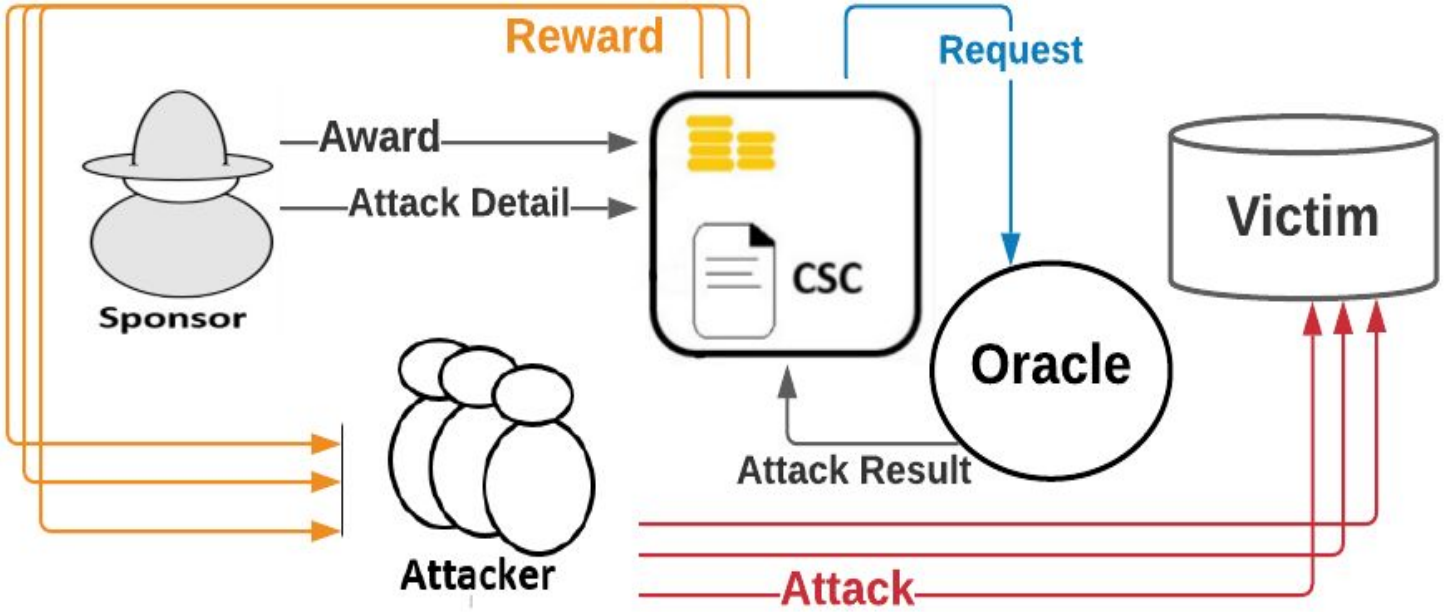
- Seeking a practical adoption?
  - Testing and deployment.
  - Exploit every opportunity to boost system's performance.
  - Look for the right trade-off between security and efficiency.



The Bad

Crowdsourcing for Malicious goals

Criminal Smart Contracts



* Z. Motaqy, G. Almashaqbeh, B. Bahrak, B., N. Yazdani, "Bet and Attack: Incentive Compatible Collaborative Attacks Using Smart Contracts." GameSec, 2021

Several CSC Types

- Solo attacker vs collaborative attackers.
- Target inside the blockchain ecosystem vs real world targets.
  - Miner bribery
  - Ransomware and private information leaks.
  - DDoS.
  - And many more …

Solo + inside/outside targets

Collaborative + inside/outside targets

Several CSC Types

- Solo attacker vs collaborative attackers.
- Target inside the blockchain ecosystem vs real world targets.
  - Miner bribery
  - Ransomware and private information leaks.
  - DDoS.
  - And many more …

Defending against CSCs is still an open problem!

Conclusion

- Smart contract-enabled blockchains pioneered the Web 3.0 movement.
- An effective way for decentralized crowdsourcing.
- Similar to any other technology, bad actors may use it for malicious purposes.
- There is still a long way ahead of us.


THANK YOU