UCONN
UNIVERSITY OF CONNECTICUT

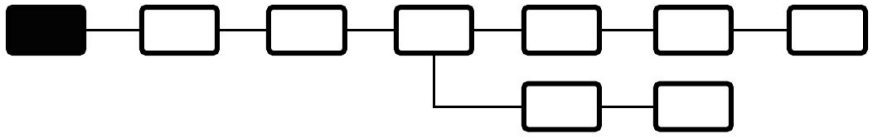
–On the Power of Smart Contracts– The Good and the Bad

Ghada Almashaqbeh
University of Connecticut

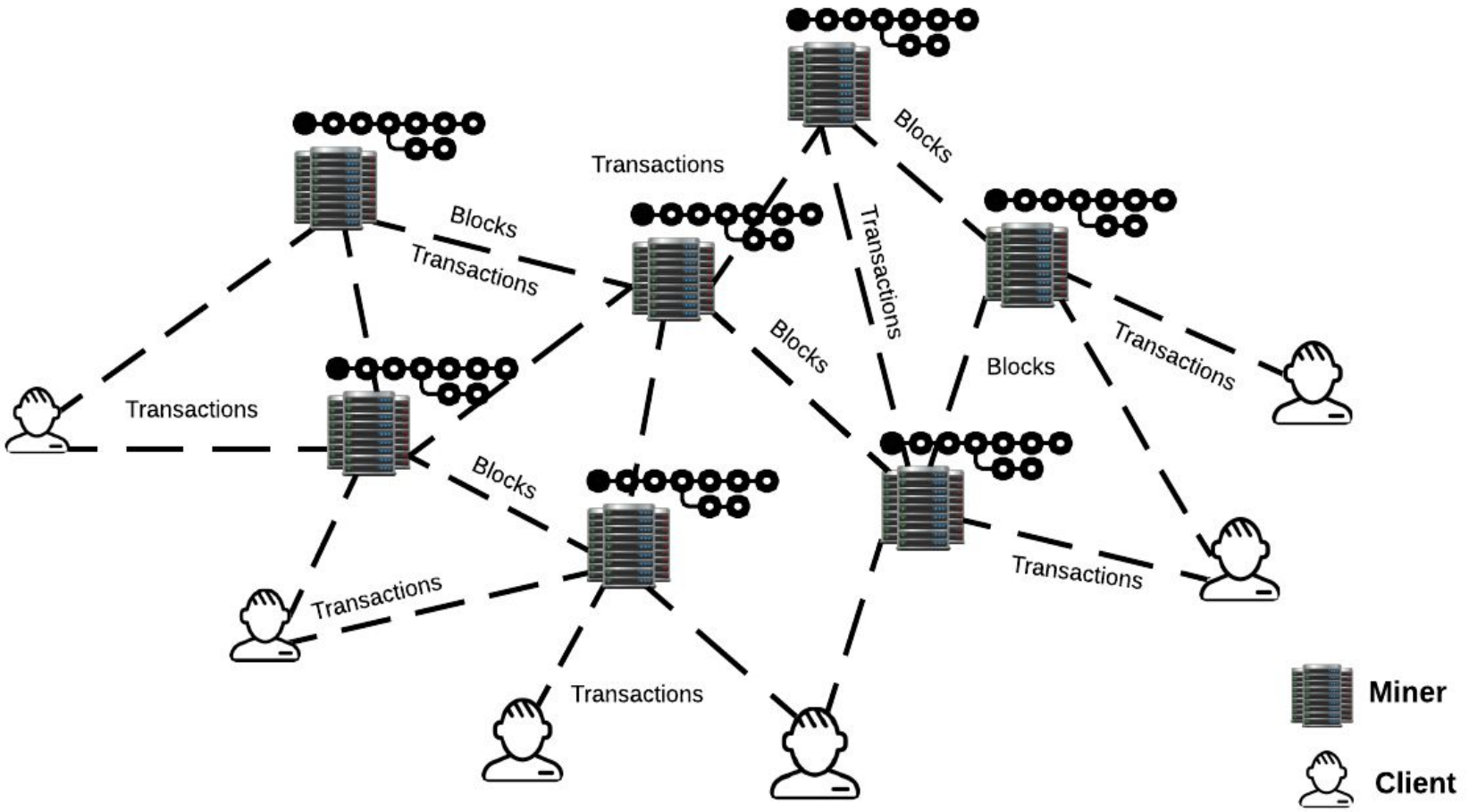
Software Center/MDU Cybersecurity Workshop
Sep 2022

Cryptocurrencies and Blockchain Technology

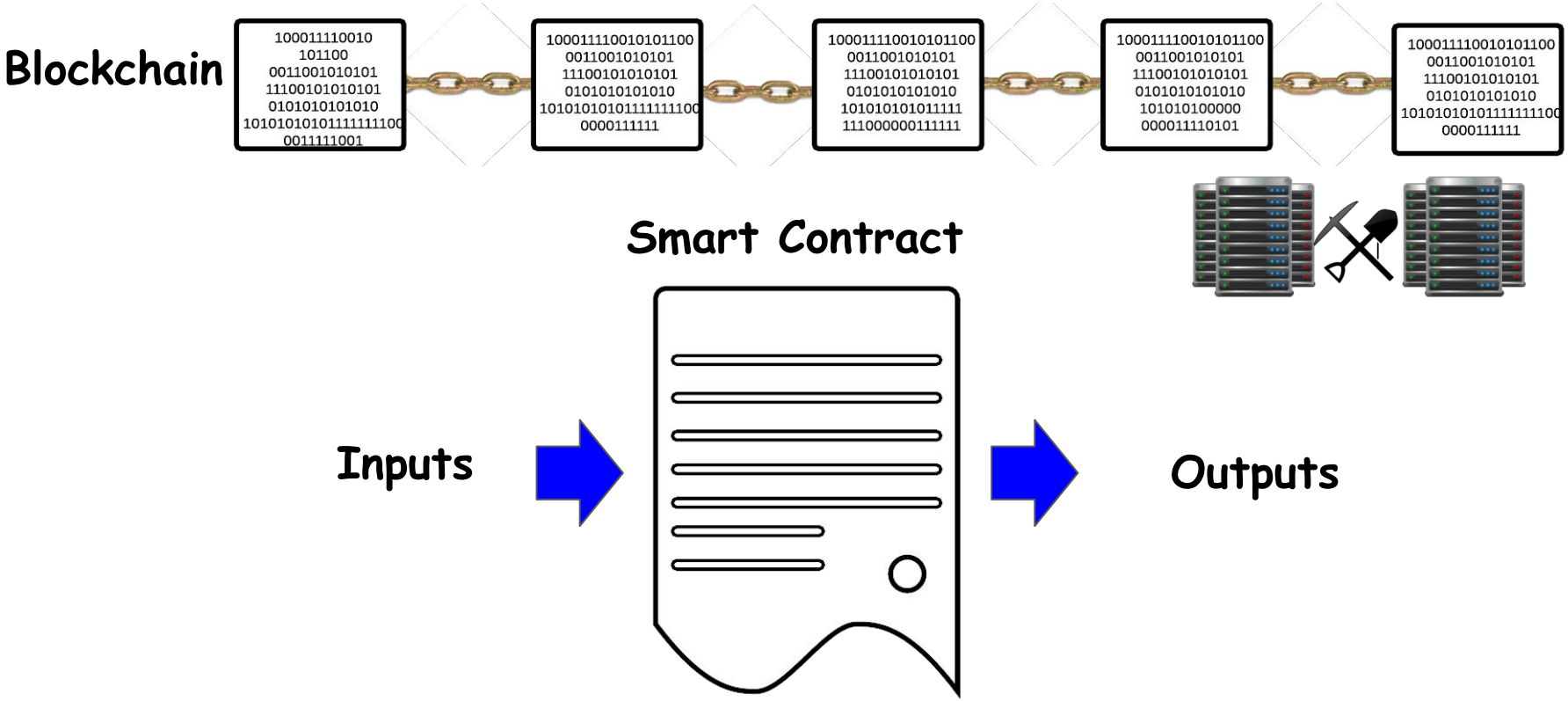
- An emerging economic force with a huge interest.
- Early systems focused on providing a currency exchange medium.
- Newer systems provide a service on top of this medium.
  - E.g., Filecoin, Livepeer, NuCypher ....
  - Come under the umbrella of ***Web 3.0***
    - dApps, DeFi, etc.



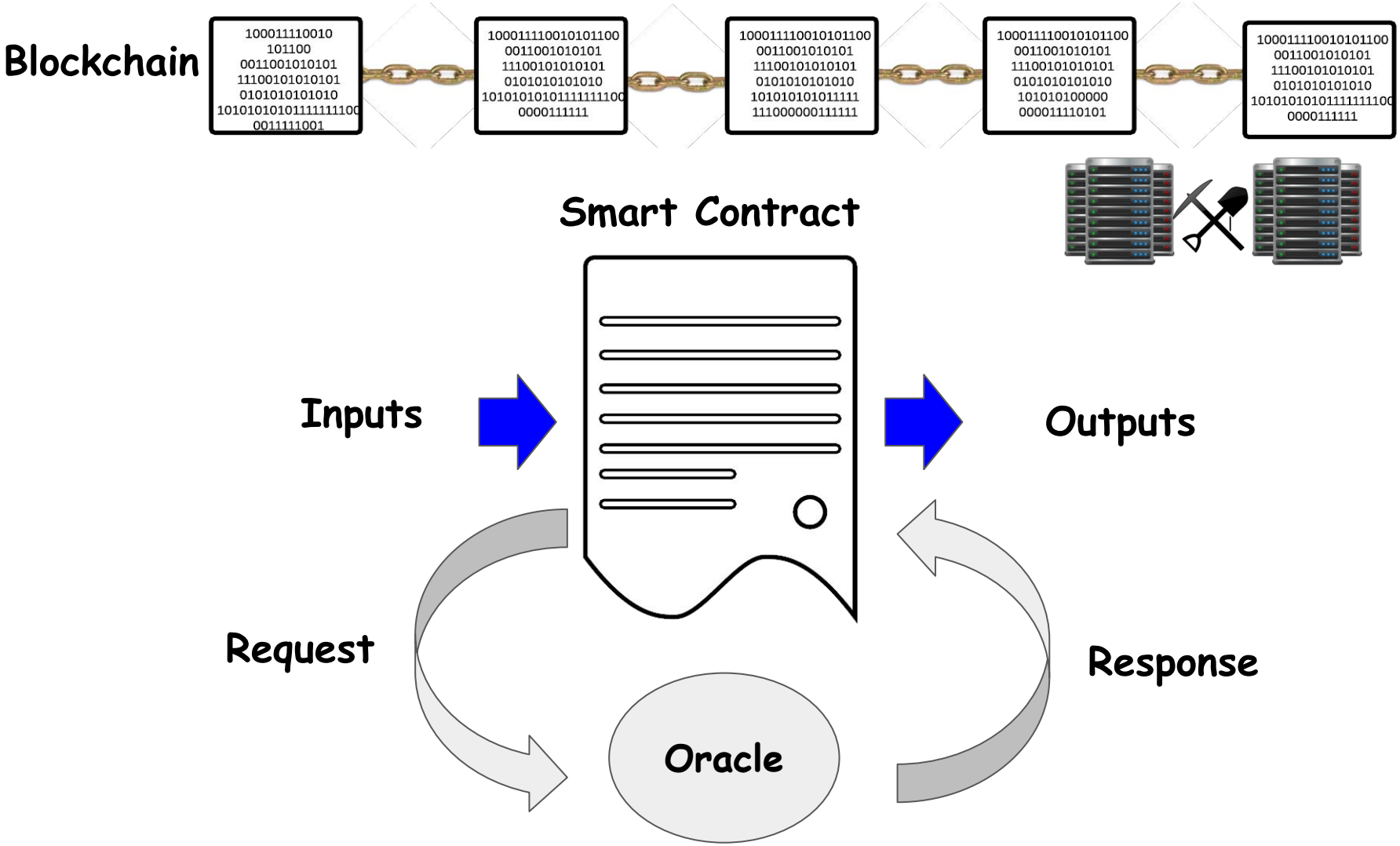
Pictorially



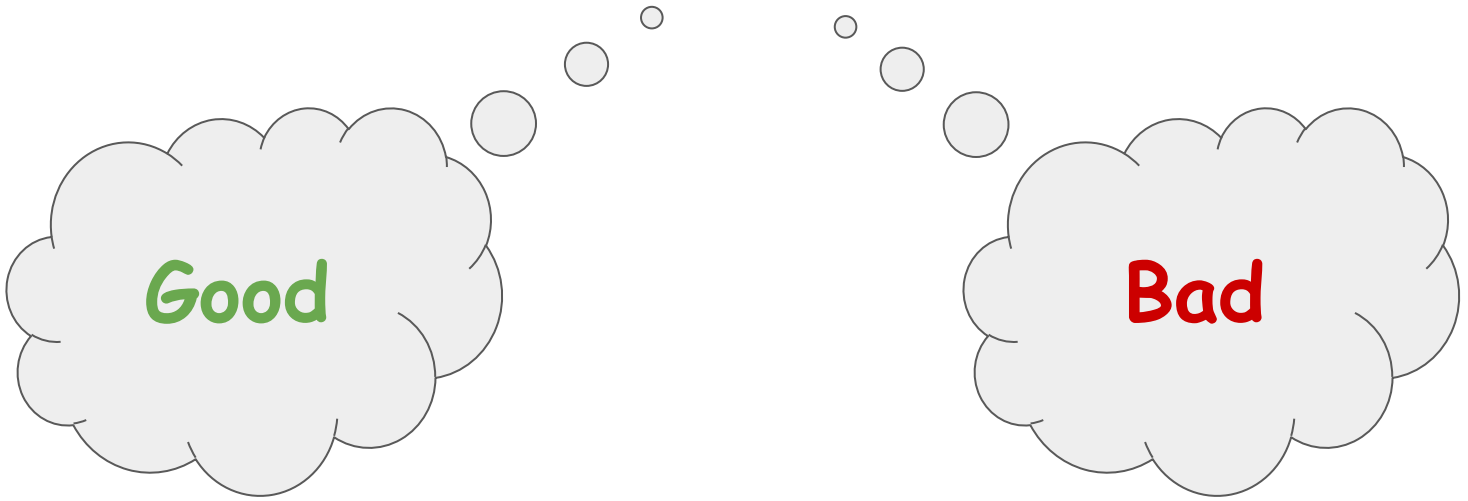
More - Smart Contracts



Even More - Real World Data Feeds

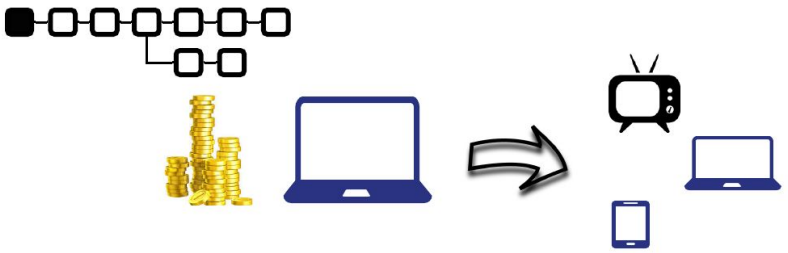


Many (Potential) Applications



Decentralized resource markets

Criminal smart contracts



The Good

Crowdsourcing for benign goals

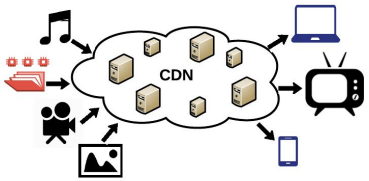
Traditional Service Systems

Central Management

Services

File Storage

justcloud.com OneDrive



Content Distribution

Akamai CLOUDFLARE fastly

Computing

Google Cloud Platform Microsoft Azure

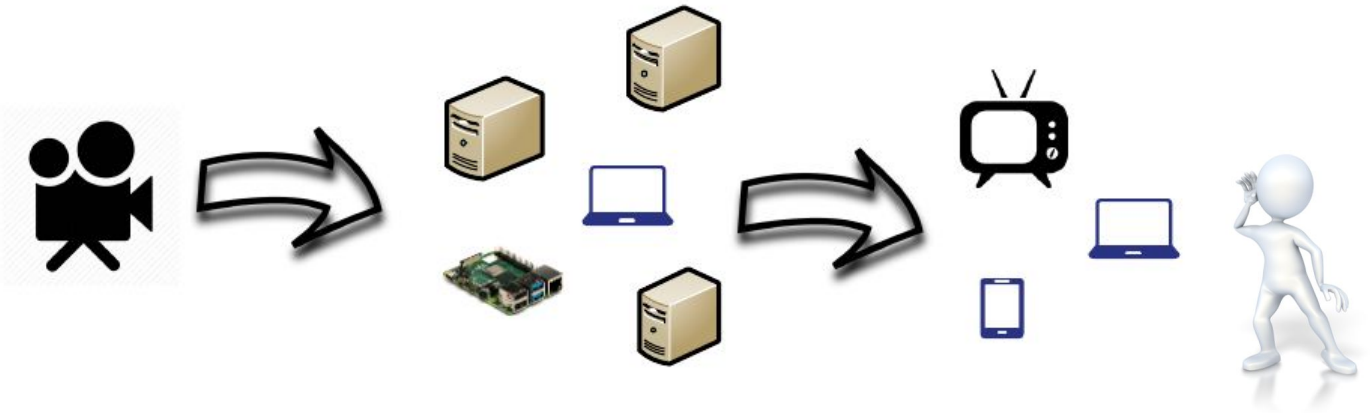
Traditional Service Systems

Central Management

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

Decentralized Services

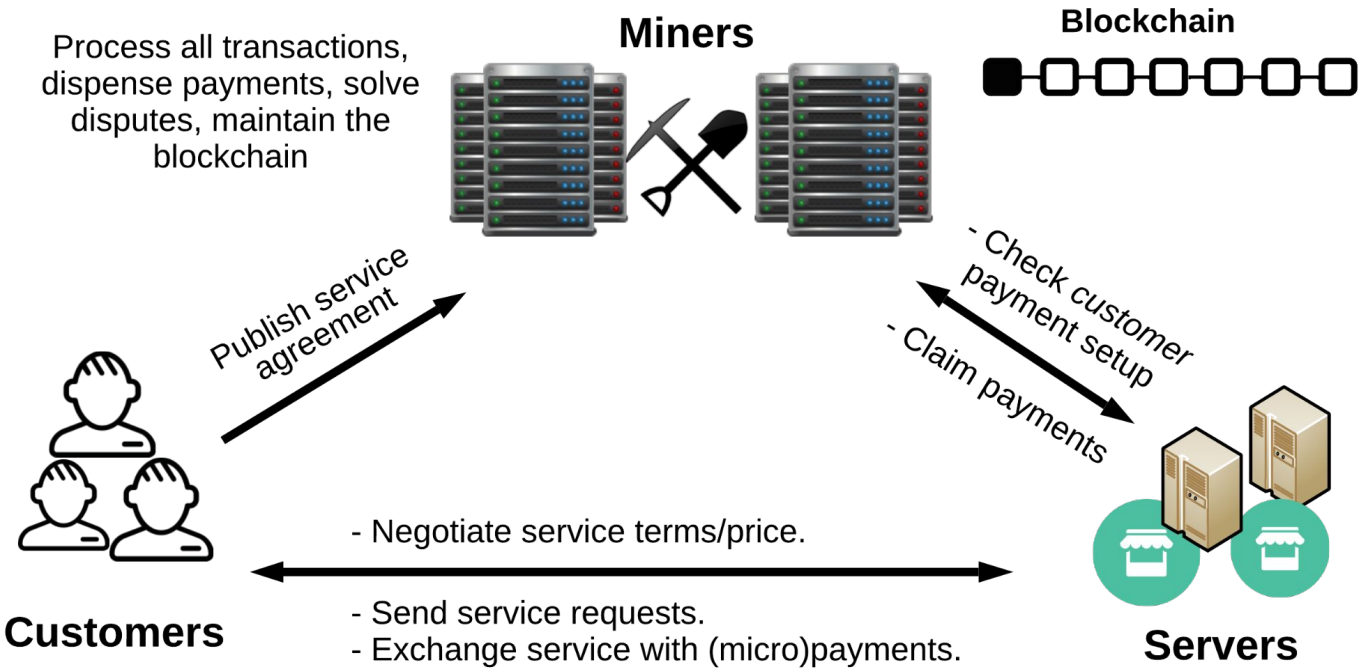
- Utilize P2P-based models to build dynamic systems.
- **Advantages:**
  - Flexible services.
  - Easier to scale with demand.
  - Extended reachability and lower latency.
  - Democratized and transparent ecosystems.



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

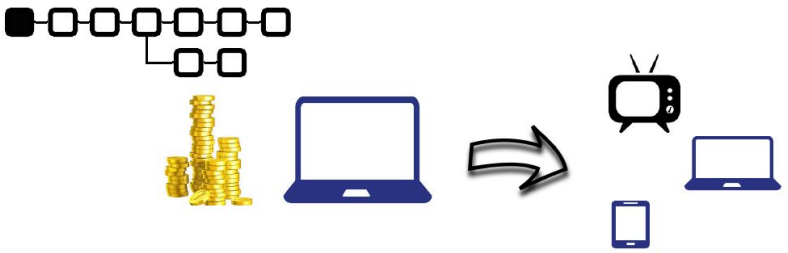
Decentralized Resource Markets



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

Many Challenges and Open Problems

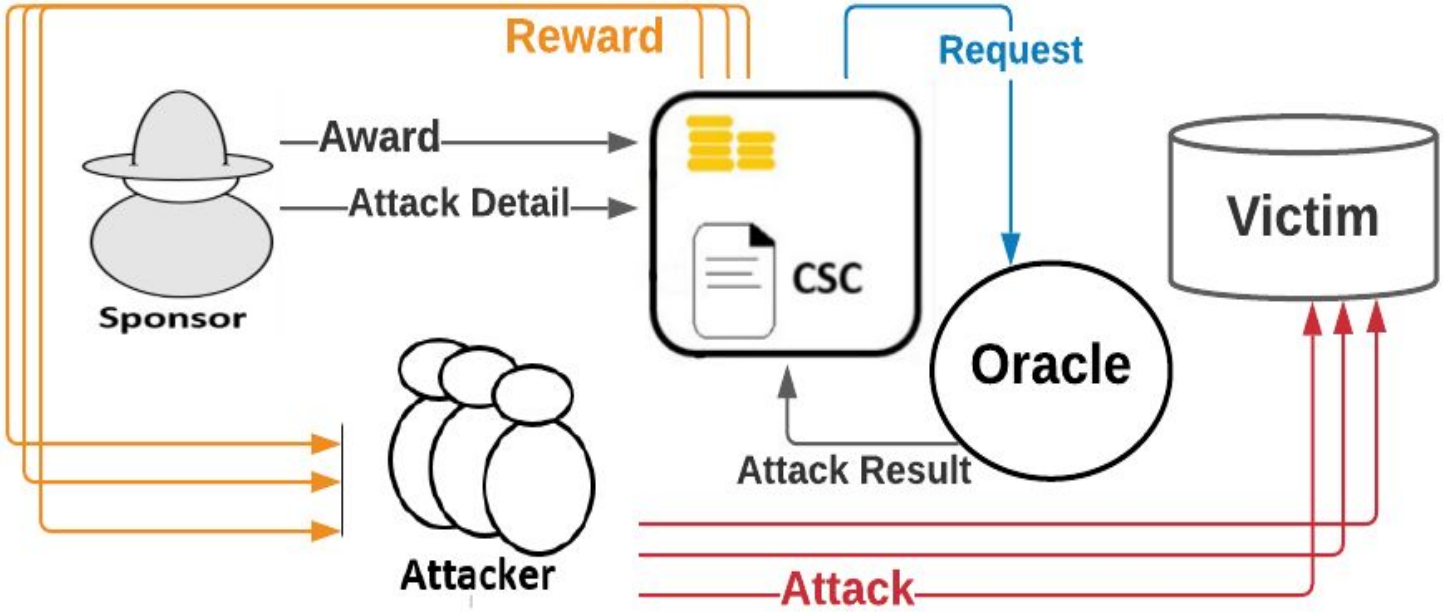
- Viability assessment.
- Threat modeling.
- Service-payment exchange.
- Cryptographic and economic security defenses.
- Scalability and efficiency optimization.
- Privacy and anonymity.
- And many more …



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.
  - Murder/etc.

Several CSC Types

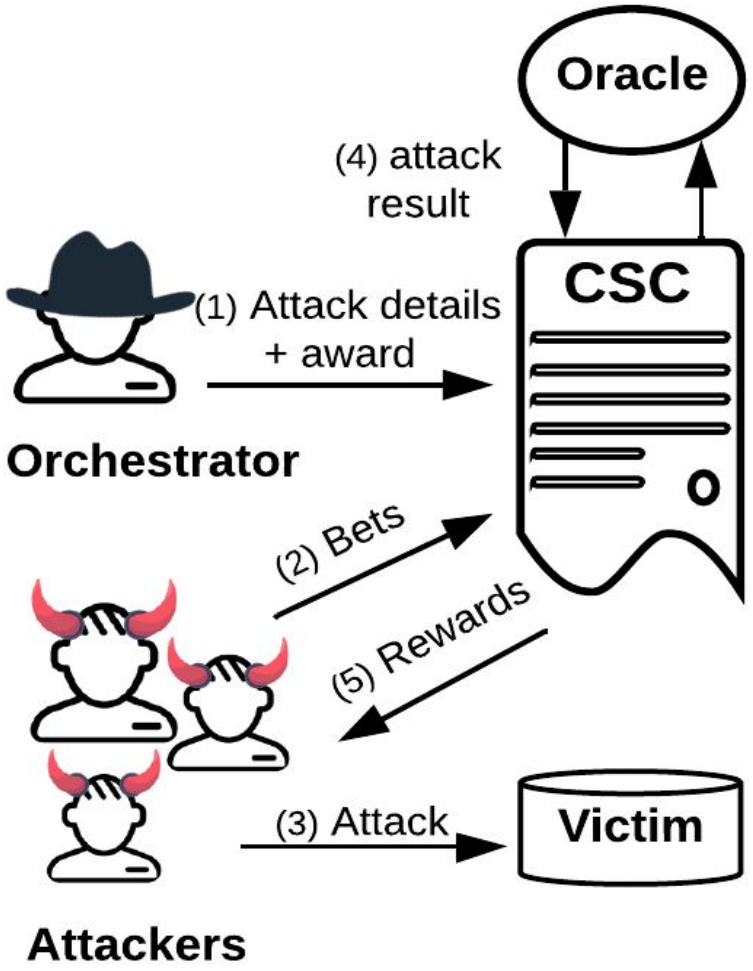
- Solo attacker vs collaborative attackers.
- Target inside the blockchain ecosystem vs real world targets.
  - Miner bribery
  - Ransomware and private information leaks.
  - DDoS.
  - Murder/etc.

Solo + inside/outside targets

Collaborative + inside targets

Bet and Attack Paradigm

- Trustless attackers collaborate with each other to achieve a common goal.
- Formally showed that our mechanism is incentive compatible.
- Thus, attackers are incentivized to contribute in proportion to their bets.



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

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