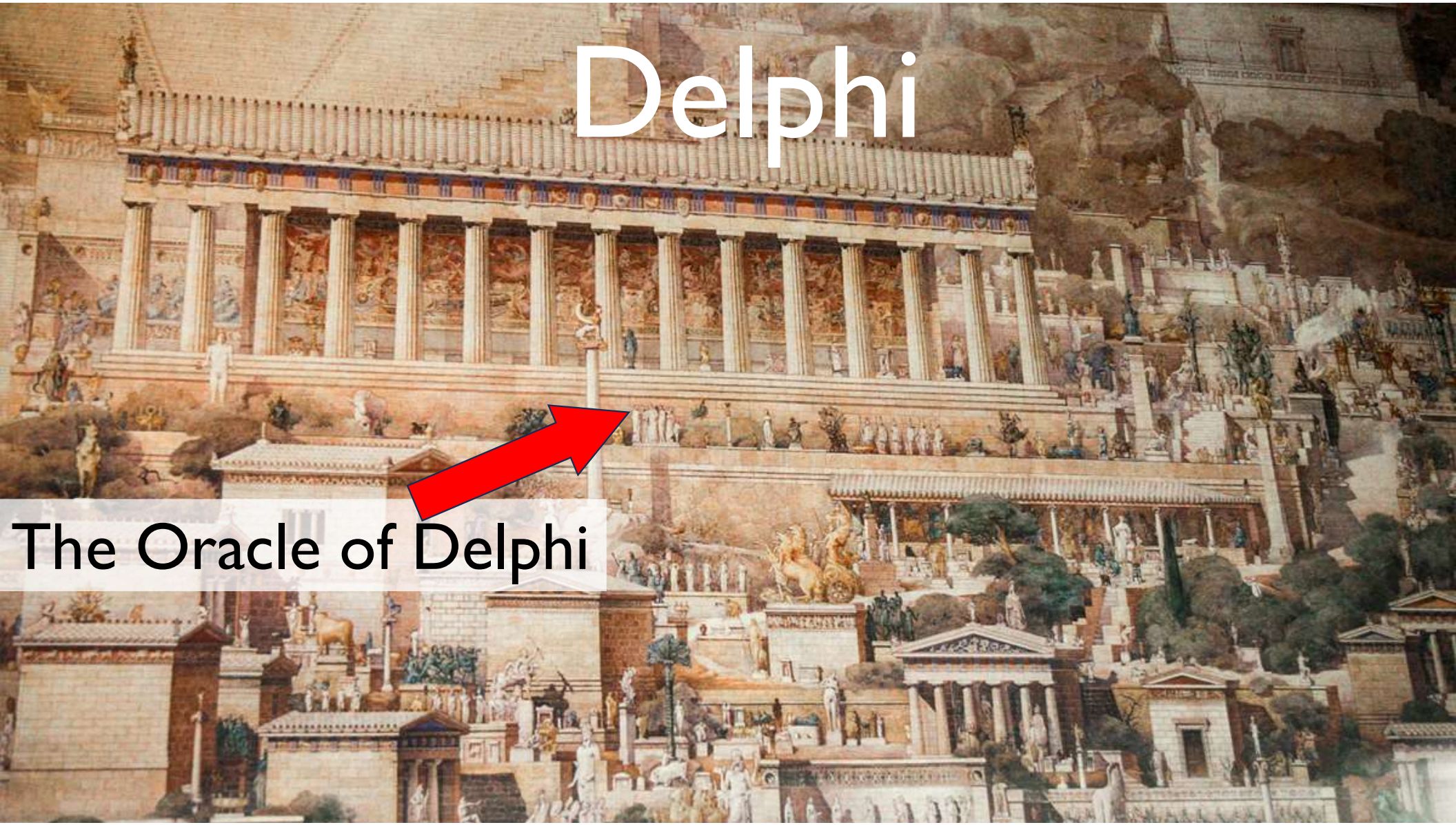
The Oracle:
A Crypto Thriller Novel

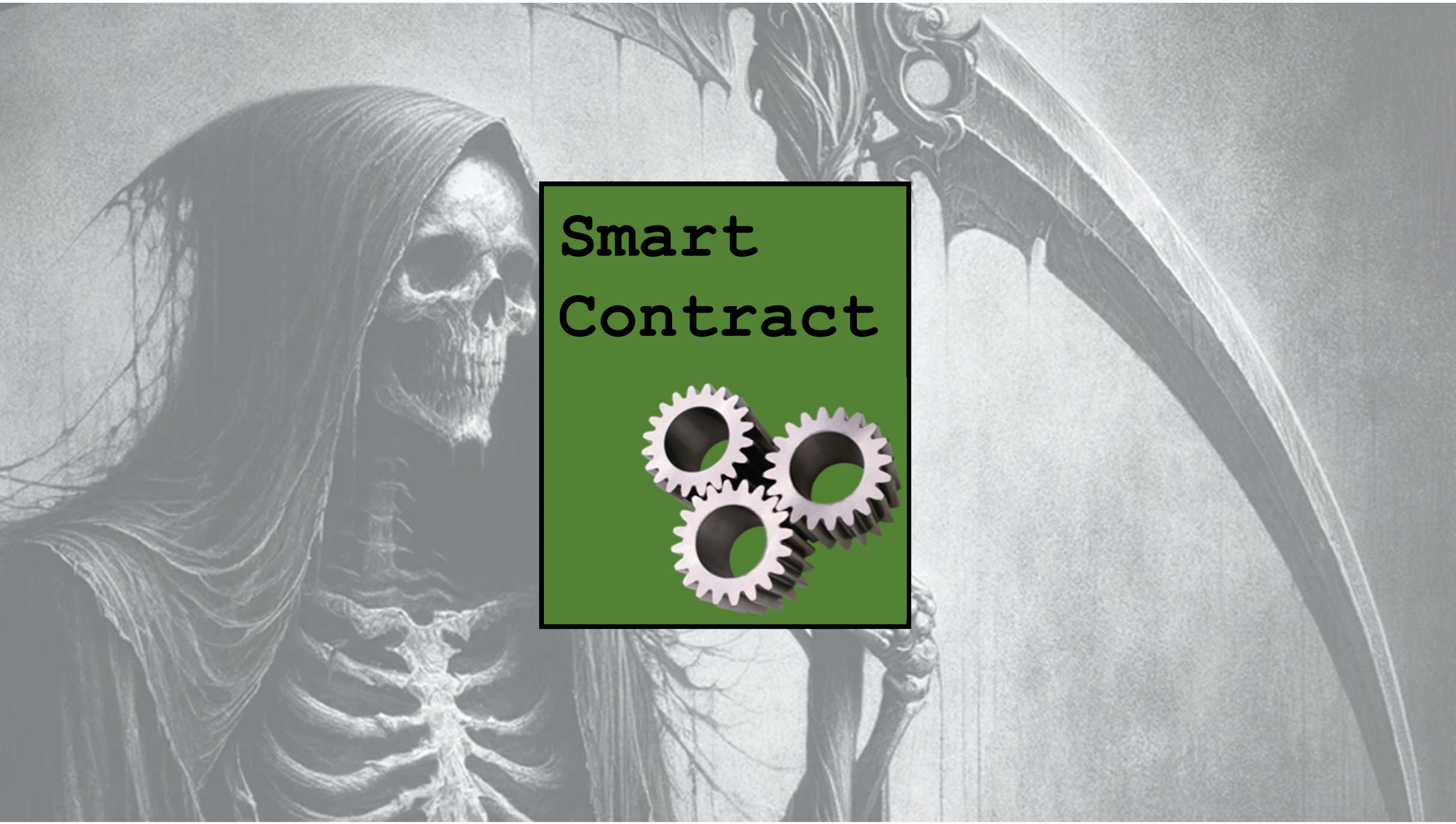
Ari Juels

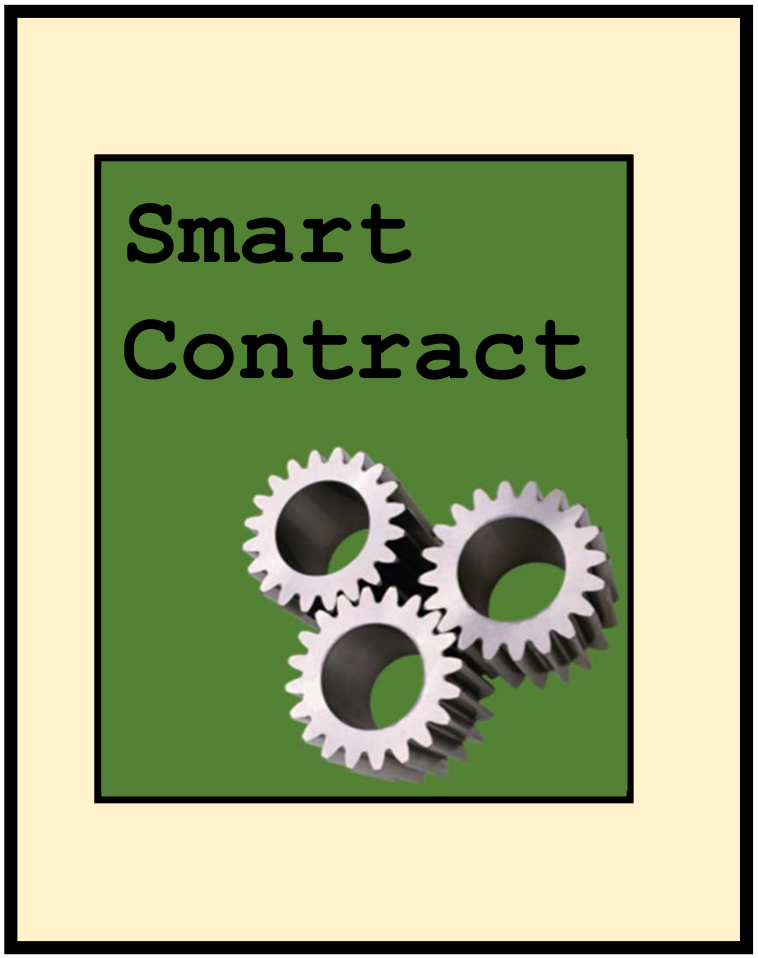
Cornell Tech, IC3, and Chainlink Labs

UC Berkeley DeFi course

14 October 2024

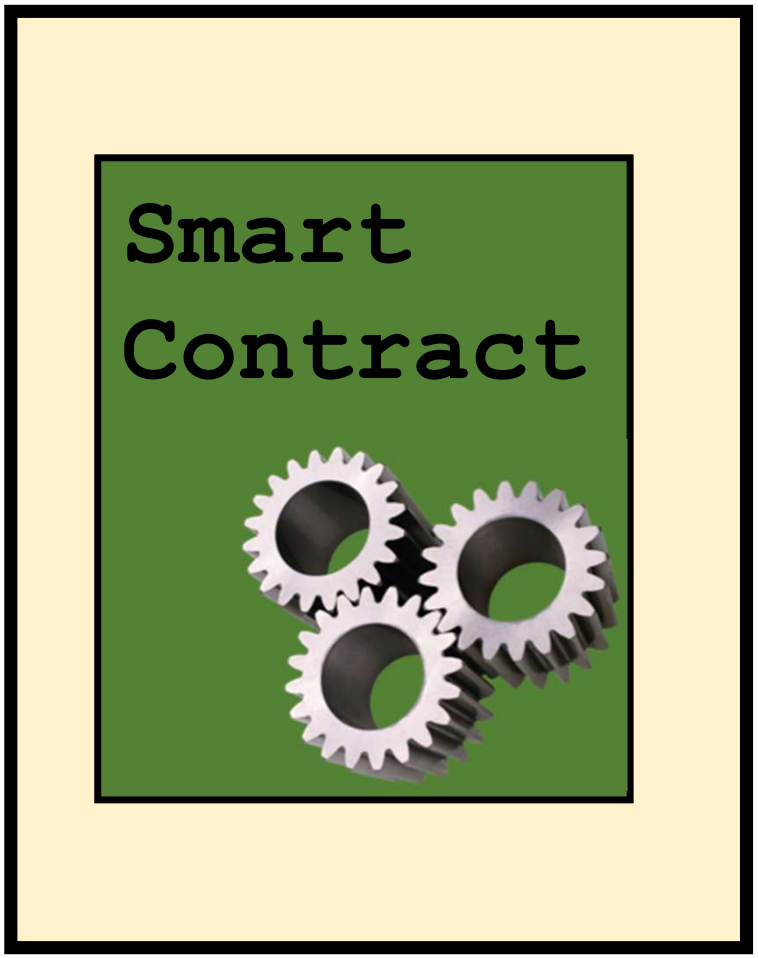

Delphi
The Oracle of Delphi


Smart
Contract



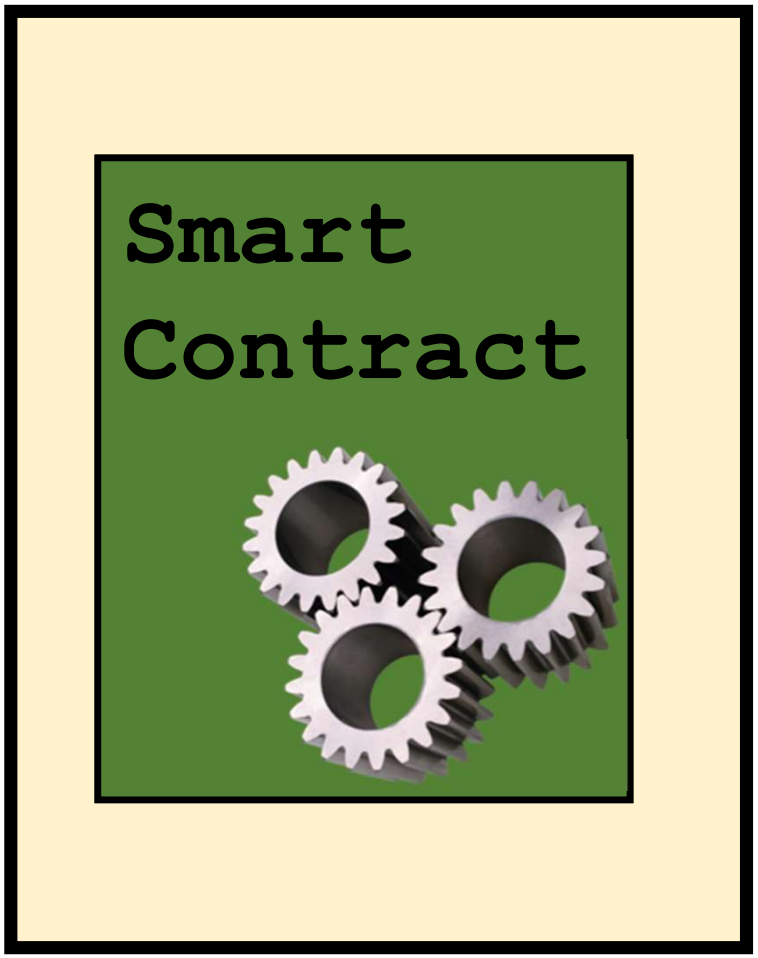
Blockchain

1. **Tamperproof!**
2. **Unstoppable!**
3. **Can hold money** (cryptocurrency)



Example: Betting contract

- Alice and Bob want to bet on a football game
- They each send $1 to smart contract
- Alice wins $2 if **blue** team wins football game
- Bob wins $2 if **red** team wins

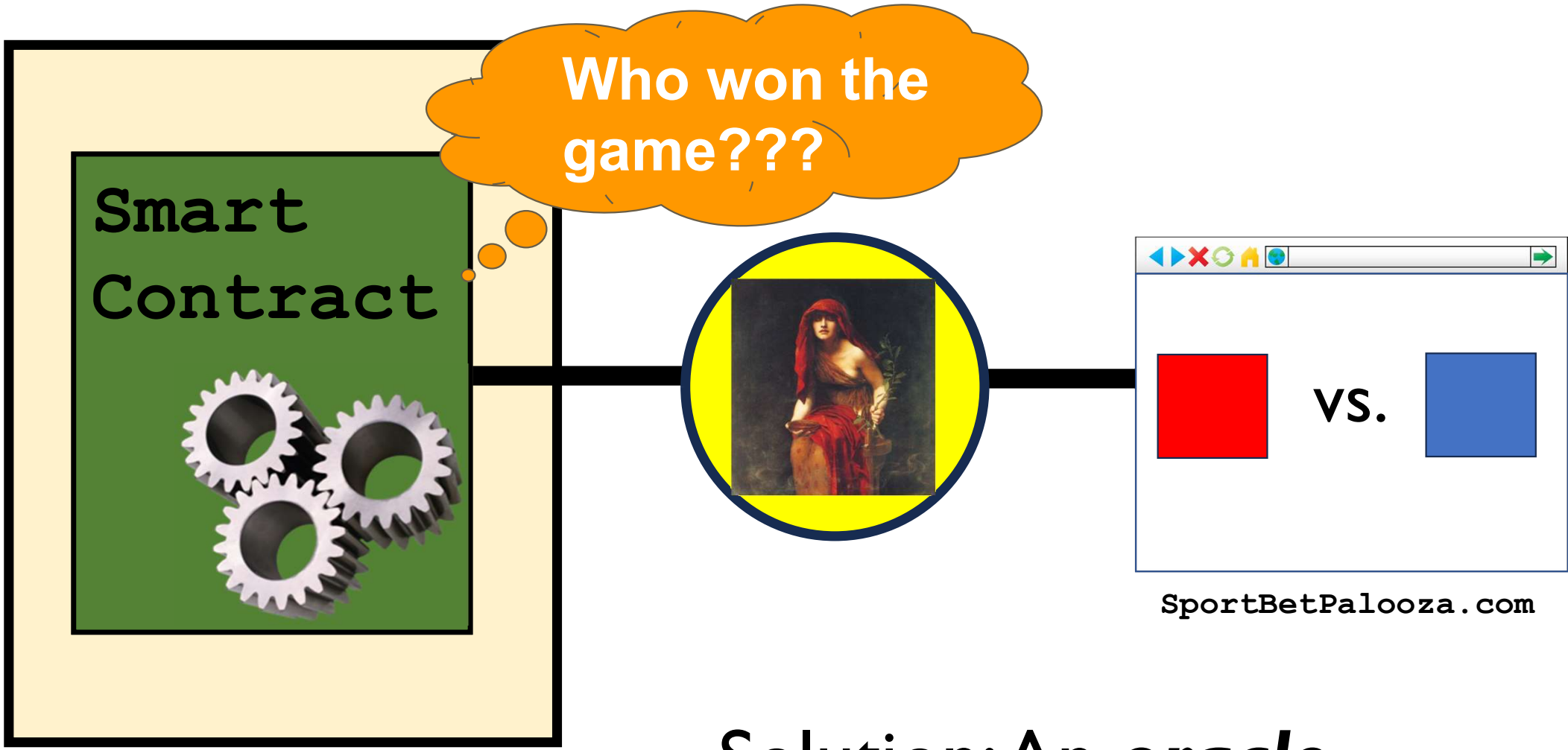


1. **Tamperproof** → money will flow exactly as programmed; *don't need to trust a company / website*
2. **Unstoppable** → guaranteed to pay out
3. **Can hold money** → able to take in and pay out real $$$ (crypto)

Smart Contract

Who won the game???

No connection to websites!



Solution: An ***oracle***

ChainLink

A Decentralized Oracle Network

Steve Ellis, Ari Juels[†], and Sergey Nazarov

4 September 2017 (**v1.0**)

Abstract

Smart contracts are poised to revolutionize many industries by replacing the need for both traditional legal agreements and centrally automated digital agreements. Both performance verification and execution rely on manual actions from one of the contracting parties, or an automated system that programmatically retrieves and updates relevant changes. Unfortunately, because of their underlying consensus protocols, the blockchains on which smart contracts run cannot support native communication with external systems.

Today, the solution to this problem is to introduce a new functionality, called an *oracle*, that provides connectivity to the outside world. Existing oracles are centralized services. Any smart contract using such services has a single point of failure, making it no more secure than a traditional, centrally run digital agreement.

In this paper we present ChainLink, a decentralized oracle network. We describe the on-chain components that ChainLink provides for contracts to gain external connectivity, and the software powering the nodes of the network. We present both a simple on-chain contract data aggregation system, and a more efficient off-chain consensus mechanism. We also describe supporting reputation and security monitoring services for ChainLink that help users make informed

Blockchain oracles

- Aim to be a sources of definitive truth
  - Like oracles in ancient world!
  - For asset prices, cross-blockchain data, (pseudo)randomness, sports, weather and much more!
- But truth can be dangerous… in many ways
  - King Croesus famously misinterpreted a prophesy from the Oracle of Delphi

Croesus on a pyre

Implicit warning about dangers of AI + smart contracts

The Ring of Gyges: Investigating the Future of Criminal Smart Contracts

Ari Juels
Cornell Tech, Jacobs Institute
IC3†
juels@cornell.edu

Ahmed Kosba
University of Maryland
akosba@cs.umd.edu

Elaine Shi
Cornell University
IC3†
rs2358@cornell.edu

†Initiative for CryptoCurrencies and Contracts

ABSTRACT

Thanks to their anonymity (pseudonymity) and elimination of trusted intermediaries, cryptocurrencies such as Bitcoin have created or stimulated growth in many businesses and communities. Unfortunately, some of these are criminal, e.g., money laundering, illicit marketplaces, and ransomware.

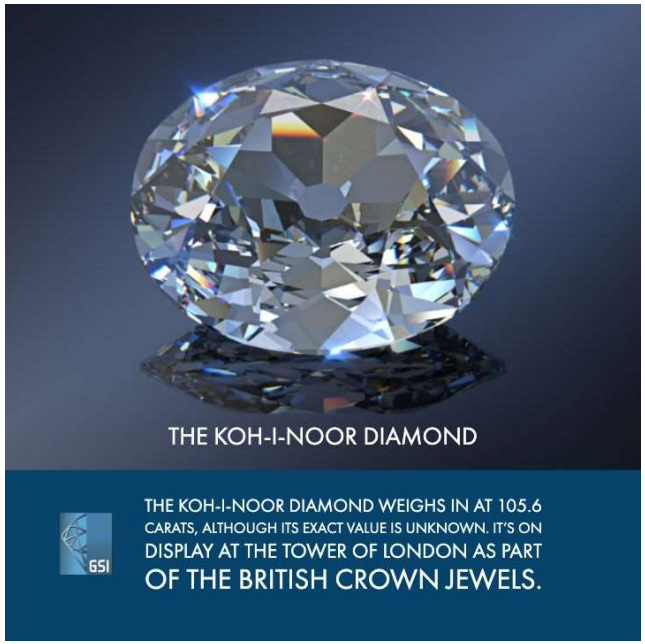
Next-generation cryptocurrencies such as Ethereum will include rich scripting languages in support of *smart contracts*, programs that autonomously intermediate transactions. In this paper, we explore the risk of smart contracts fueling new criminal ecosystems. Specifically, we show how

"[On wearing the ring,] no man would keep his hands off what was not his own when he could safely take what he liked out of the market, or go into houses and lie with anyone at his pleasure, or kill or release from prison whom he would... " —Plato, *The Republic*, Book 2 (2.360b) (trans. Benjamin Jowett)

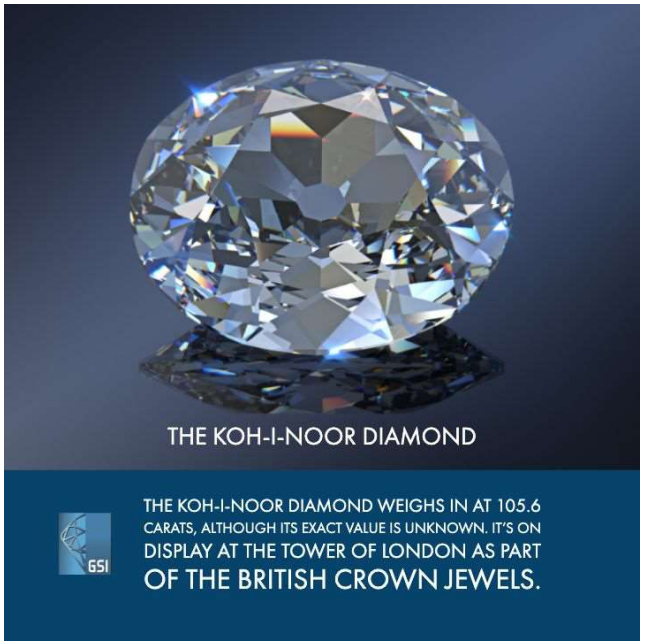
1. INTRODUCTION

Cryptocurrencies such as Bitcoin remove the need for trusted third parties from basic monetary transactions and offer anonymous (more accurately, pseudonymous) transactions

Example: AI-powered rogue smart contract

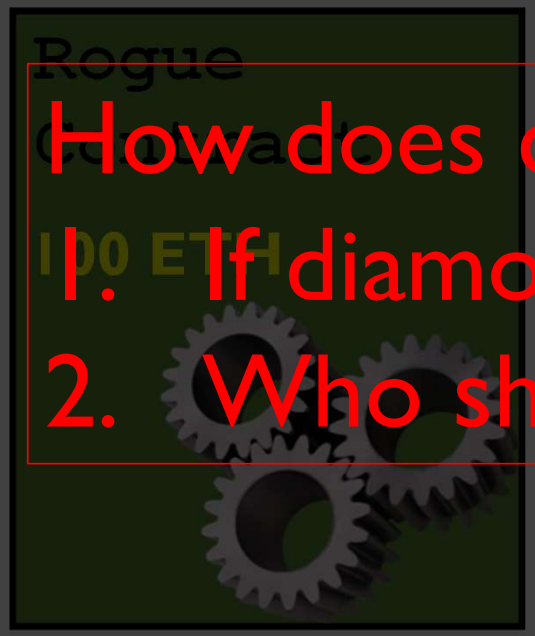


Example: AI-powered rogue smart contract



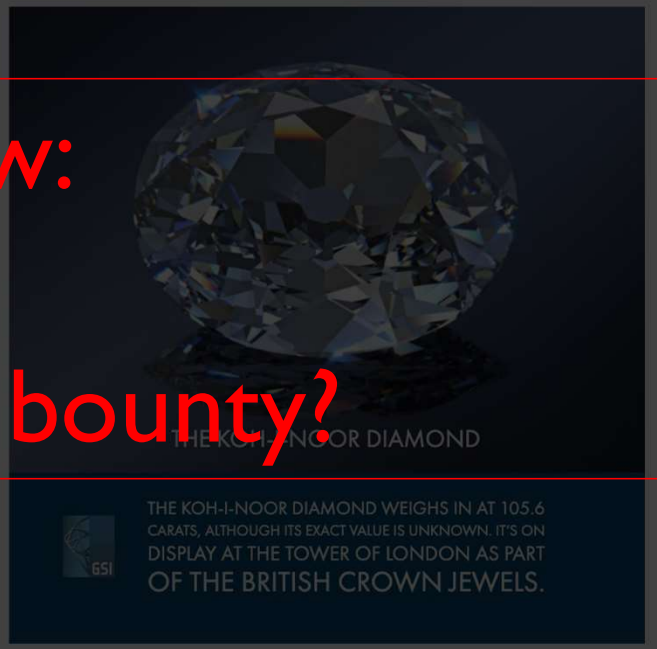
Bounty: $100,000 to steal Koh-I-Noor diamond

Example: AI-powered rogue smart contract



How does contract know:

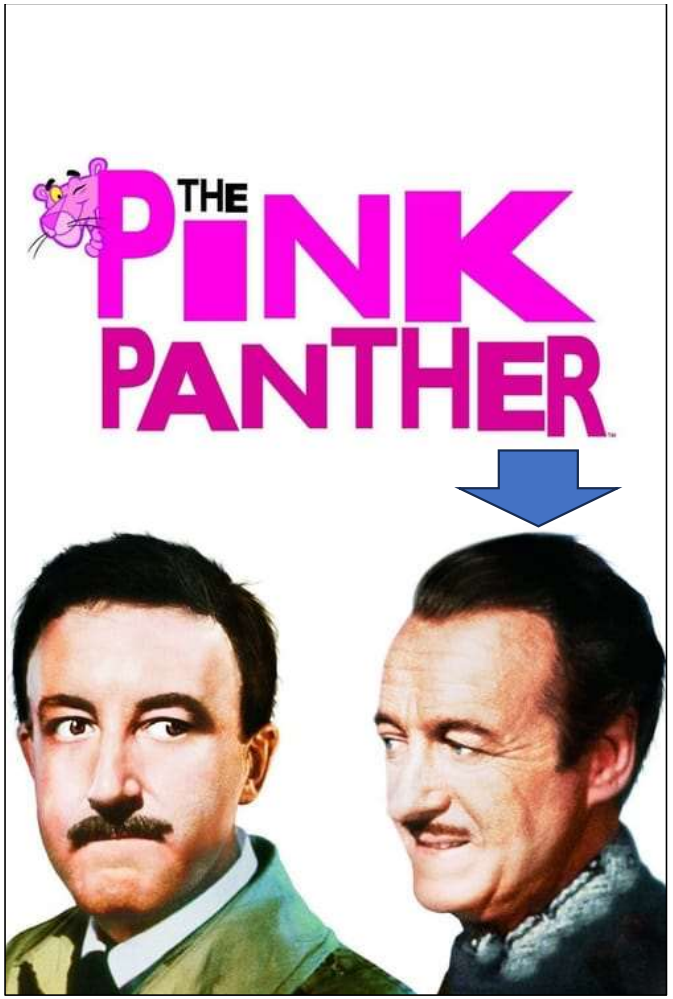
1. If diamond is stolen?
2. Who should receive bounty?



Bounty: $100,000 to steal Koh-I-Noor diamond

Calling card

- Exotic detail at crime scene
- Intentionally identifies criminal to world
- E.g., the Phantom
- Calling card: Glove with ‘P’ monogram



cc

Would-be thief

Rogue Contract

$100,000

Koh-I-Noor stolen!
'P'-monogrammed
glove found!

reveal cc

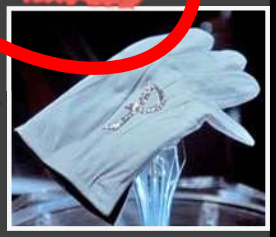
$100,000

Rogue Contract

$100,000

Koh-I-Noor stolen!
‘P’-monogrammed
glove found!

decrypt cc



Rogue
Contract

100 ETH

AI-powered oracle here!

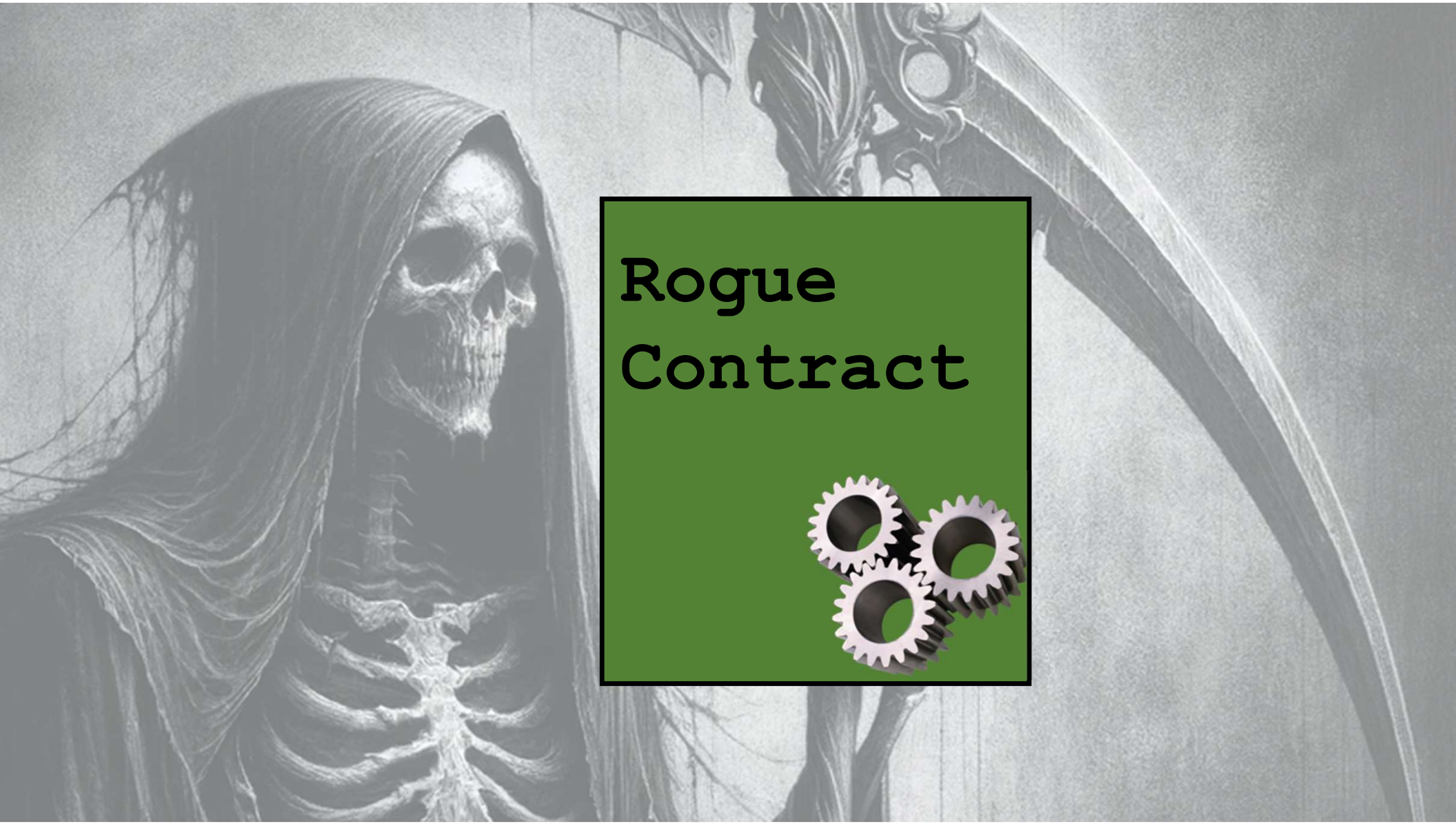
Koh-i-Noor stolen!
'P'-monogrammed glove found!

Rogue Contract

$100,000

reveal cc

A bunch of other details…


Rogue
Contract

Note well

- Rogue contracts are ***technically feasible***…

…but ***not possible*** with today's infrastructure

…yet

- *The Oracle* is a cautionary tale about the **future of blockchains + AI**

The bigger picture

- We all worry about rogue AI
- Escape into real world via:
  - Autonomous weapons systems
  - Cyberphysical infrastructure (e.g., autonomous vehicles)
  - **Financial system?**

The bigger picture

- What to do about rogue AI accessing crypto assets?
- Oracles are gatekeepers
- **How can oracles help enforce AI safety?**

Opinion

AI Safety for Smart Contracts Is AI Safety for the World

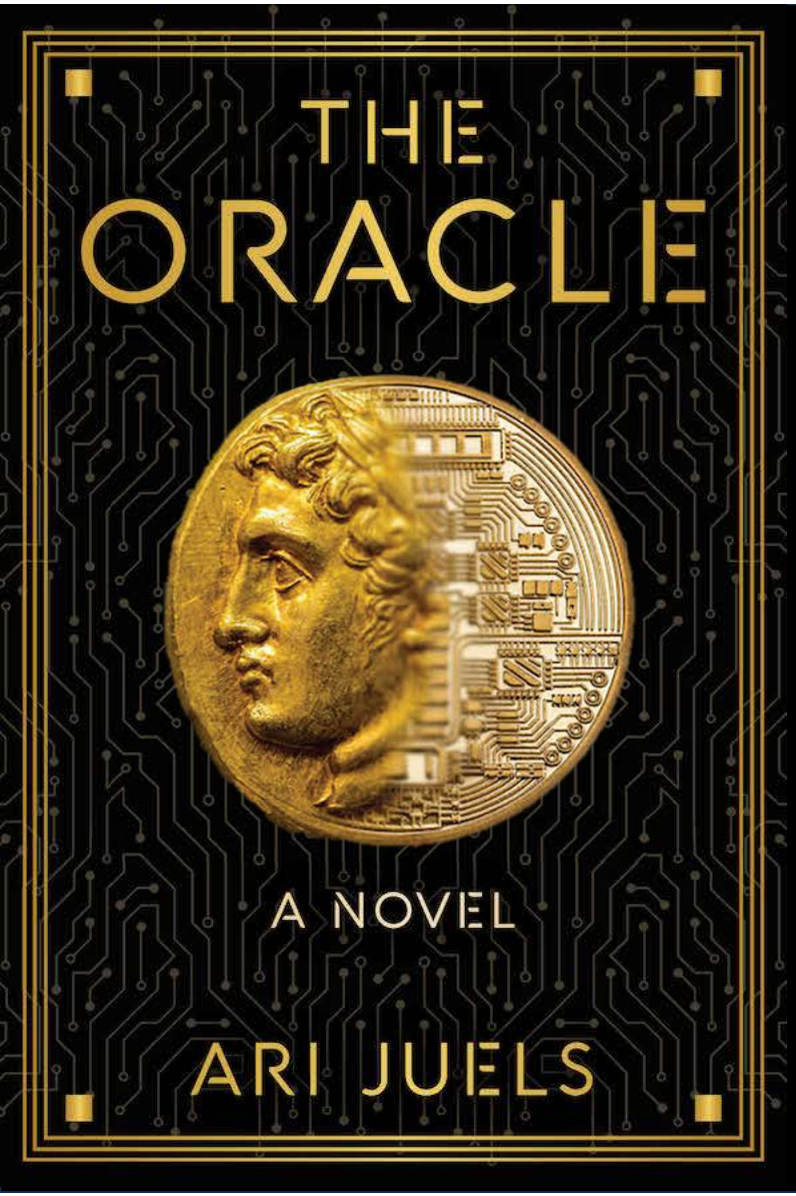
Web3 infrastructure can bring new safety and reliability tools to AI, a cycle that will make the intersection of AI and Web3 massively and mutually beneficial, Chainlink scientist Ari Juels and Google AI lead Laurence Moroney write.

By Ari Juels, Laurence Moroney Apr 23, 2024 at 1:04 p.m. EDT

Updated Apr 23, 2024 at 1:07 p.m. EDT CONSENSUS MAGAZINE

Other forward-looking DeFi stuff in the book

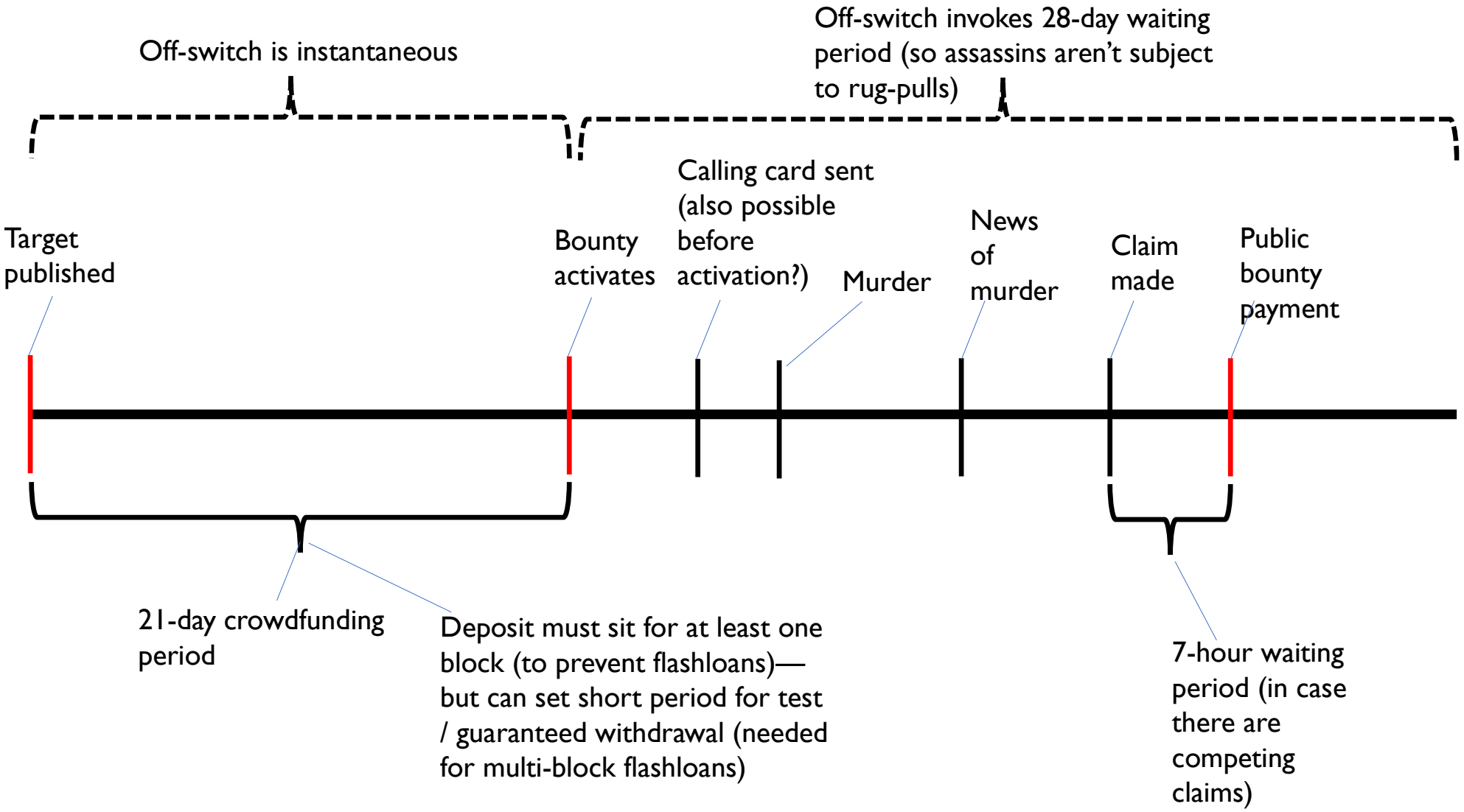
- Trusted hardware (a.k.a. TEEs / secure enclaves)
  - Hardening approaches and breaks
- Multi-block flash loans



OracleNovel.com

Thank you!

Now for a fireside chat with Dawn…


Off-switch is instantaneous
Off-switch invokes 28-day waiting period (so assassins aren't subject to rug-pulls)
Target published
Bounty activates
Calling card sent (also possible before activation?)
Murder
News of murder
Claim made
Public bounty payment
21-day crowdfunding period
Deposit must sit for at least one block (to prevent flashloans)—but can set short period for test / guaranteed withdrawal (needed for multi-block flashloans)
7-hour waiting period (in case there are competing claims)