Smart-Contract Protocols: Theory for Applications

(PROCONTRA)

STEFAN DZIEMBOWSKI

UNIVERSITY OF WARSAW

General goal of this project

Transfigure a new discipline called

smart-contract protocols

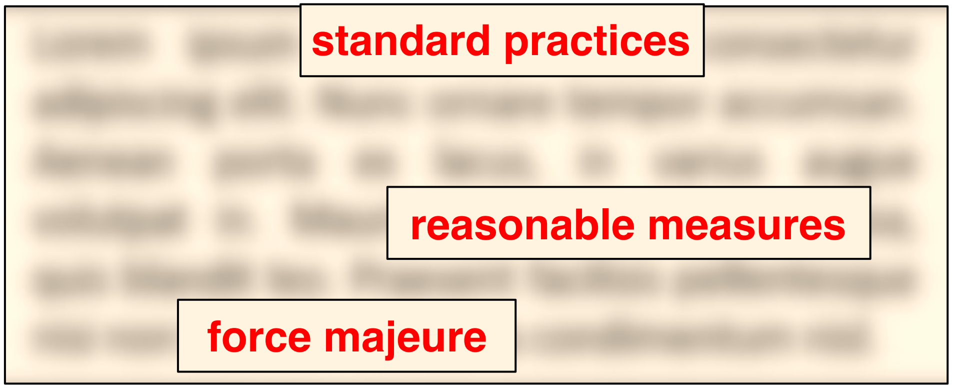
into a **mature science**.

This will be done by:

1. establishing **its foundations**, and
2. proposing **new constructions** in it.

Contracts

Legal contracts – **ambigous**:



Natural idea:
Instead of using natural language – use the lang
of **maths** or **computer science**.

```
function withdraw(uint withdrawAmount)
          public returns (uint remainingBal) {
          if (withdrawAmount <=
balances[msg.sender]) {
          balances[msg.sender] -= withdrawAmount;
          msg.sender.transfer(withdrawAmount); }
          return balances[msg.sender]; }
```

“**smart contracts**” – contracts **written in a programming language** and **executed automatically** [Nick Szabo, 1990s]

Can it be used for anything?

Lawyers: “smart-contracts are not very useful in law”

answer:

smart contracts are meant for **algorithm-to-algorithm** interaction

But then: where to write smart contracts down? Who should execute them?

recent idea:

this will be done by **blockchain**!

a **distributed trusted “public computer”** (often with its own “**virtual currency**”)

first proposed for Bitcoin in 2019 (now used in several other variants)

Huge interest

“blockchain community”

ethereum DFINITY CARDANO

industry

IBM HYPERLEDGER BOSCH

libra

“industry 4.0”

academia

smart contract research at world’s leading universities (Stanford, Berkeley, Princeton, ETH Zurich, …)

Different aspects of smart contracts can be studied.

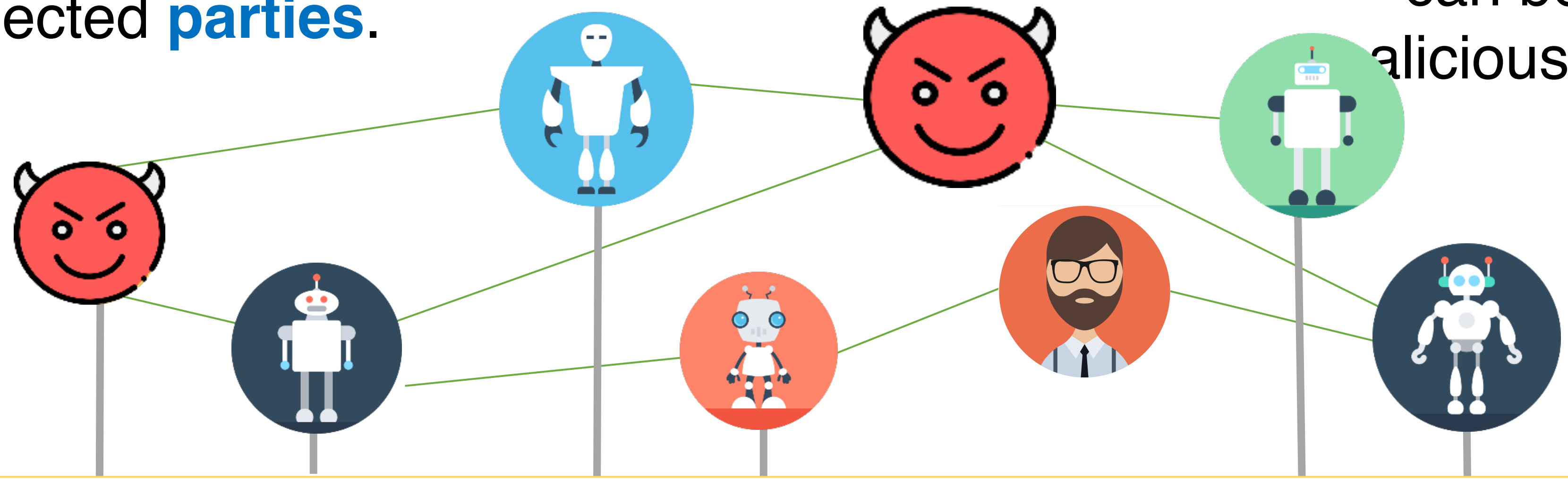
Focus of **PROCONTRA**: “smart-contract **protocols**”

Smart-contract **protocols**

Group of connected **parties**.

algorithms or humans

Some parties can be alicious!



algorithms have **access to "smart contract platform"**

≈ "**public computer**" that

- can have its own **"currency"**
- is **trusted**, but
- **slow**, and **expensive** to use

Examples of such protocols

One of the first papers on this topic was published by me and my students at **IEEE S&P 2014** **(Best Paper Award)** [301 citations].

probably **the most prestigious annual conference in data security**

contingent payments

“plasma”

decentralized exchanges

state channels

“truebit”

“arbitrum”

games

payment channels

rollups

Many of them **developed over the last 2-3 years** (often by practitioners in so-called “white papers”).

Goals of this project

The first **main goal of this project**

Build foundations of this area, using **methods of theoretical computer science** and **cryptography**:

- formal definitions
- security proofs
- impossibility results

“provable

de facto standard in cryptography

(proofs are needed since there is no “experimental evidence” of security)

Second main goal

Improve existing protocols and **propose new ones** using tools from **theoretical cryptography**.

The proposal lists **9 new ideas** for this.

Multiparty scriptless scripts

Adding privacy to channel protocols

Dealing with non-uniquely attributable faults

Adding privacy to Plasma-like schemes

MPCs with state channel networks

Watchtowers for off-chain protocols

. . .

More likely to be discovered during execution of the project.

Icons made by Freepik, Linector, monkik, Chanut, and Vectors Market.