大阪大学
OSAKA UNIVERSITY

# Ethereum スマートコントラクトのセキュリティ研究

大阪大学
大学院情報科学研究科
セキュリティ工学講座

矢内直人

# 自己紹介

大阪大学
OSAKA UNIVERSITY

- **メインテーマ：情報セキュリティ**
  - 学位論文：暗号技術の設計と証明可能安全性を研究
  - 現職：セキュリティ技術の開発研究と安全性検証
- **2014：筑波大博士課程修了**
- **2014-2021/12：阪大・助教**
- **2021/12-：現職**
- **2016-2018/3：JST ACT-I**
  - サイバーセキュリティの安全性を証明する数理モデル
    - Web: https://github.com/naotoyanai/websecmodel
    - スマートコントラクト: https://github.com/naotoyanai/RA
- **2021-：CREST 主たる共同研究者**
  - 地域を支える知のデジタライゼーションと共有基盤

# 参考資料

ブロックチェーンの解説を国内雑誌 IEICE B-plusに寄稿 (2020年6月)

## スマートコントラクト
### ——ブロックチェーンからなるプログラミングプラットホーム——


知念祐一郎 Yuichiro Chinen 大阪大学
芦澤奈実 Nami Ashizawa 大阪大学
矢内直人 Naoto Yanai 大阪大学
クルーズ ジェイソン ポール Jason Paul Cruz 大阪大学


### 1 スマートコントラクトとは

2008年のビットコイン（Bitcoin）誕生から現在に至るまで多くのブロックチェーンが出現しているが，ブロックチェーンと聞くと暗号通貨を思い浮かべる人も多いだろう．しかし，その機能は単なる通貨の送受信以上の領域にまで広がっている．その最たるものがスマート

表1 スマートコントラクトと暗号通貨の違い

| | ブロックチェーン上の主な情報 | トランザクションの内容 |
|---|---|---|
| 暗号通貨 | ・通貨残高 | ・送金 |
| スマートコントラクト | ・コード<br>・変数 | ・コード実行<br>・コードの書込みと変数の初期化 |

シンボリック実行ツールの開発を国内論文誌 JIP に掲載 (2021年9月)

## RA: A Static Analysis Tool for Analyzing Re-Entrancy Attacks in Ethereum Smart Contracts


Yuichiro Chinen[1,a) ] Naoto Yanai[1,b)] Jason Paul Cruz[1,c)] Shingo Okamura[2,d)]



Received: November 11, 2020, Accepted: June 7, 2021



**Abstract:** Ethereum smart contracts are programs that are deployed and executed in a consensus-based blockchain managed by a peer-to-peer network. Several re-entrancy attacks that aim to steal Ether, the cryptocurrency used in Ethereum, stored in deployed smart contracts have been found in the recent years. A countermeasure to such attacks is based on dynamic analysis that executes the smart contracts themselves, but it requires the spending of Ether and knowledge of attack patterns for analysis in advance. In this paper, we present a static analysis tool named *RA* (*Re-entrancy Analyzer*), a combination of symbolic execution and equivalence checking by a satisfiability modulo theories solver to analyze vulnerability of smart contracts to re-entrancy attacks. In contrast to existing tools, RA supports analysis of inter-contract behaviors by using only the Ethereum Virtual Machine bytecodes of target smart contracts,


Ethereum 上でアクセス制御アプリの開発 (被引用数200越え)


IEEE Access
SPECIAL SECTION ON RESEARCH CHALLENGES AND OPPORTUNITIES IN SECURITY AND PRIVACY OF BLOCKCHAIN TECHNOLOGIES

Received January 10, 2018, accepted February 26, 2018, date of publication March 7, 2018, date of current version March 19, 2018.

*Digital Object Identifier 10.1109/ACCESS.2018.2812844*


## RBAC-SC: Role-Based Access Control Using Smart Contract


JASON PAUL CRUZ[1], (Member, IEEE), YUICHI KAJI[2], (Member, IEEE), AND NAOTO YANAI[1]
[1]Graduate School of Information Science and Technology, Osaka University, Suita 565-0871, Japan
[2]Information Strategy Office, Nagoya University, Nagoya 464-8601, Japan
Corresponding author: Jason Paul Cruz (jpmcruz@ymail.com)


Ethereum の脆弱性の機械学習検知技術の提案

## Eth2Vec: Learning Contract-Wide Code Representations for Vulnerability Detection on Ethereum Smart Contracts


Nami Ashizawa *Non-Member*, Naoto Yanai *Member, IEEE*, and Jason Paul Cruz *Member, IEEE*
Shingo Okamura *Member, IEEE*



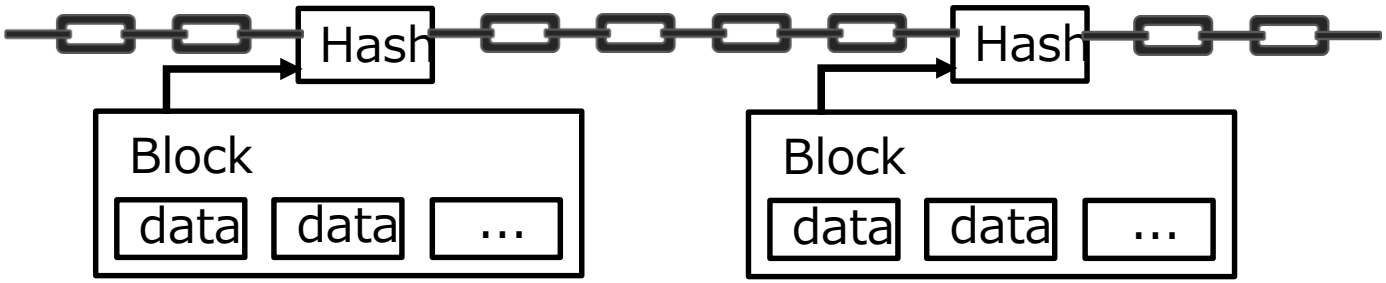
**Abstract**—Ethereum smart contracts are computer programs that are deployed and executed on the Ethereum blockchain to enforce agreements among untrusting parties. Being the most prominent platform that supports smart contracts, Ethereum has been targeted by many attacks and plagued by security incidents. Consequently, many smart contract vulnerabilities have been discovered in the past decade. To detect and prevent such vulnerabilities, different security analysis tools, including static and dynamic analysis tools, have been created but their performance decreases drastically when codes to be analyzed are constantly being rewritten. In this paper, we propose Eth2Vec, a machine-learning-based static analysis tool that detects smart contract vulnerabilities. Eth2Vec maintains its robustness against code rewrites, i.e., it can detect vulnerabilities even in rewritten codes. Other machine-learning-based static analysis tools require features, which analysts create manually, as inputs. In contrast, Eth2Vec uses a neural network for language processing to automatically learn features of vulnerable contracts. In doing so, Eth2Vec can detect vulnerabilities in smart contracts by comparing the similarities between the codes of a target contract and of the learned contracts. We performed experiments with existing

# スマートコントラクト

- **ブロックチェーン上のプログラムの実行環境**
  - 暗号通貨は通貨残高を記録
  - スマートコントラクトは実行コード / 変数も記録

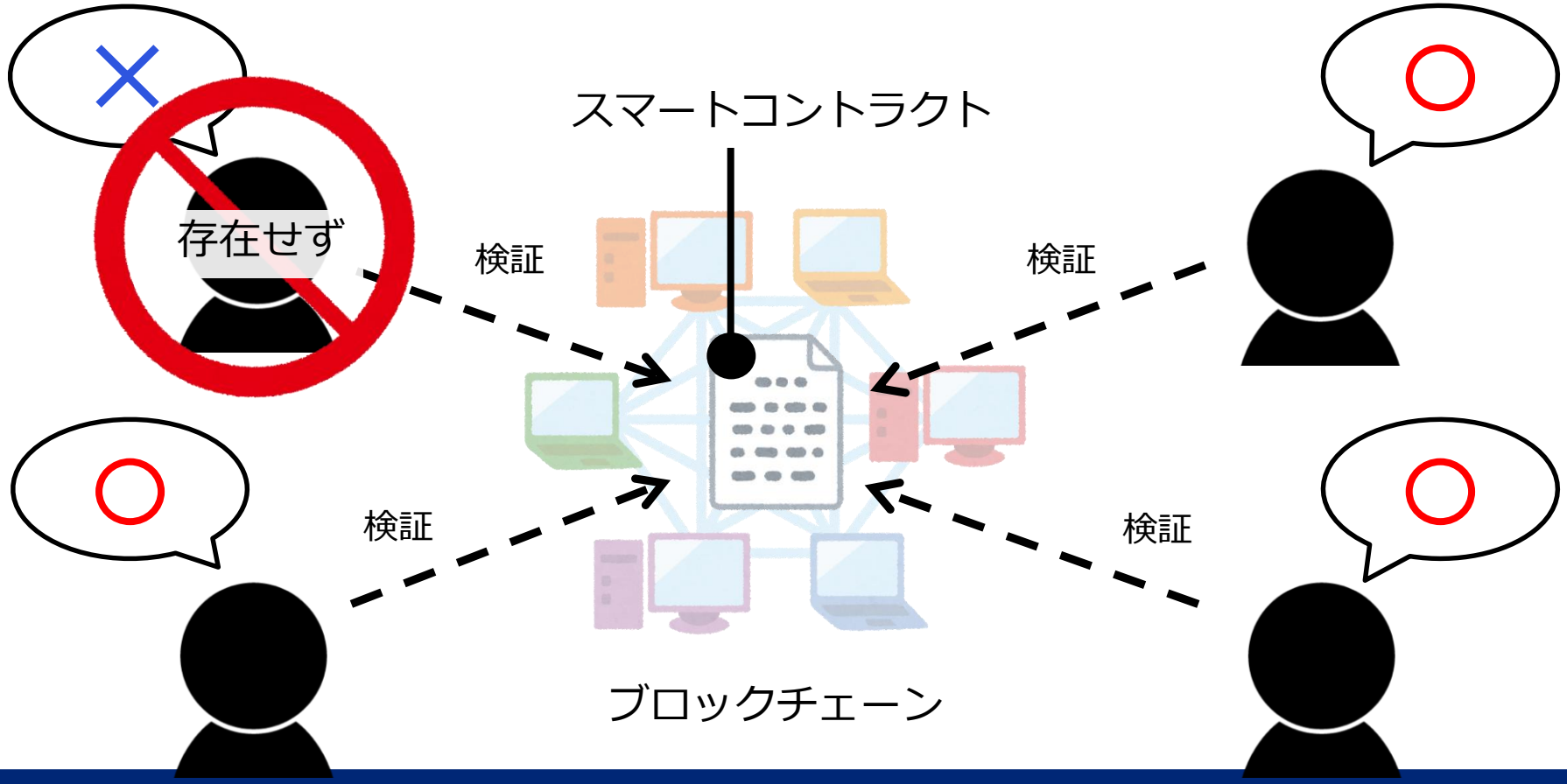
## ブロックチェーン

- **非中央集権型のプラットフォーム**
- **全ての情報をハッシュ関数に入力・連結させることで、データの改ざん耐性・透明性を実現**



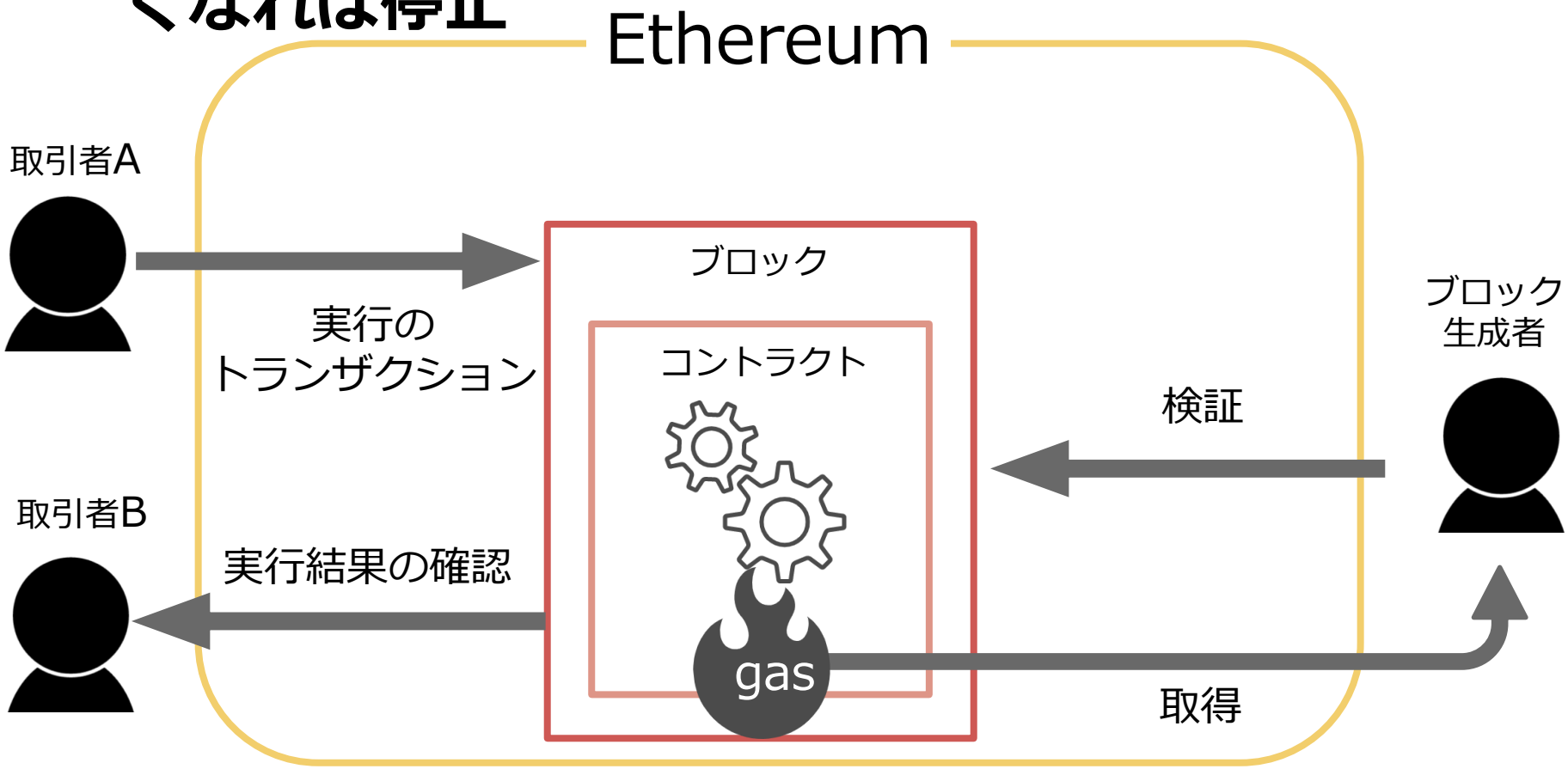
# スマートコントラクトの原理

- ブロックチェーンのノード上にプログラム公開
- 誰が実行しても同じ結果 → 結果の公開検証が可能



# Ethereum の場合

- Ethereum 上のブロックにプログラムをデプロイ
- 燃料（gas） を消費することで実行 → gas がなくなれば停止



# 従来のプログラムとEthereum の違い

攻撃者の優位性

解析し易く、永遠に残る

バイトコードの公開

解析できる

01100001 01110010
01100010 01101001
01110010 01111001
01001001 00100000
01110000 01100101
01101111 01110101

金銭的処理

リターンが巨大

攻撃を誘引しやすい

スマート
コントラクト


ユーザが抱える困難

挙動が従来の環境と異なる
（動作が想像しにくい）

gasの取り扱い

特有の要素

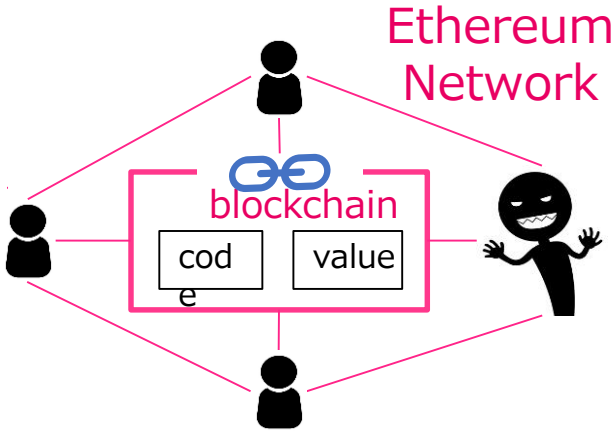
知見の不足

若すぎる技術

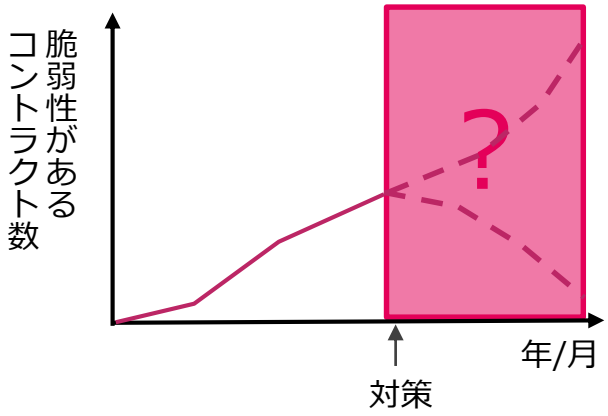
# Ethereumスマートコントラクトの脆弱性

大阪大学
OSAKA UNIVERSITY

- **ネットワーク上で実行コードを公開**
  - Ethereumネットワーク上でプログラムが実行可能
  - 攻撃者によるコードの閲覧，解析が容易[CAYC20]




- **脆弱性への対策**
  - 記述言語のコンパイラ更新
  - 脆弱性の解析ツール開発




*[CAYC20]* 知念ら, “スマートコントラクト ーブロックチェーンからなるプログラミングプラットホームー”, 信学会, *b-plus, 2020.*

# Ethereumスマートコントラクトの脆弱性調査

大阪大学
OSAKA UNIVERSITY

脆弱性に関する実態調査[DFAC20]

- 2019年までの47,587件のコントラクトの脆弱性を調査
- 脆弱性の傾向変化の要因については未調査

脆弱性解析ツールの性能評価[PDCS18]

- 既存のオープンソース解析ツールに対する性能評価
- 性能の高いツール：SmartCheck[TVI+18]

開発者のセキュリティに関する意識調査[WXL+21]

- 開発時のセキュリティ対策についてのヒアリング調査
- 多くの開発者が使用するコンパイラは安定した古いバージョン

*[DFAC20] T. Durieux, et al., "Empirical Review of Automated Analysis Tools on 47,587 Ethereum Smart Contracts", ICSE 2020.*
*[PDCS18] R. Parizi, et al., "Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains", CASCON2018*
*[TVI+18] S. Tikhomirov, et al., "SmartCheck: Static Analysis of Ethereum Smart Contracts", WETSEB 2018.*
*[WXL+21] Z. Wan, et al., "Smart Contract Security: a Practitioners' Perspective", ICSE2021*

# 実際の被害

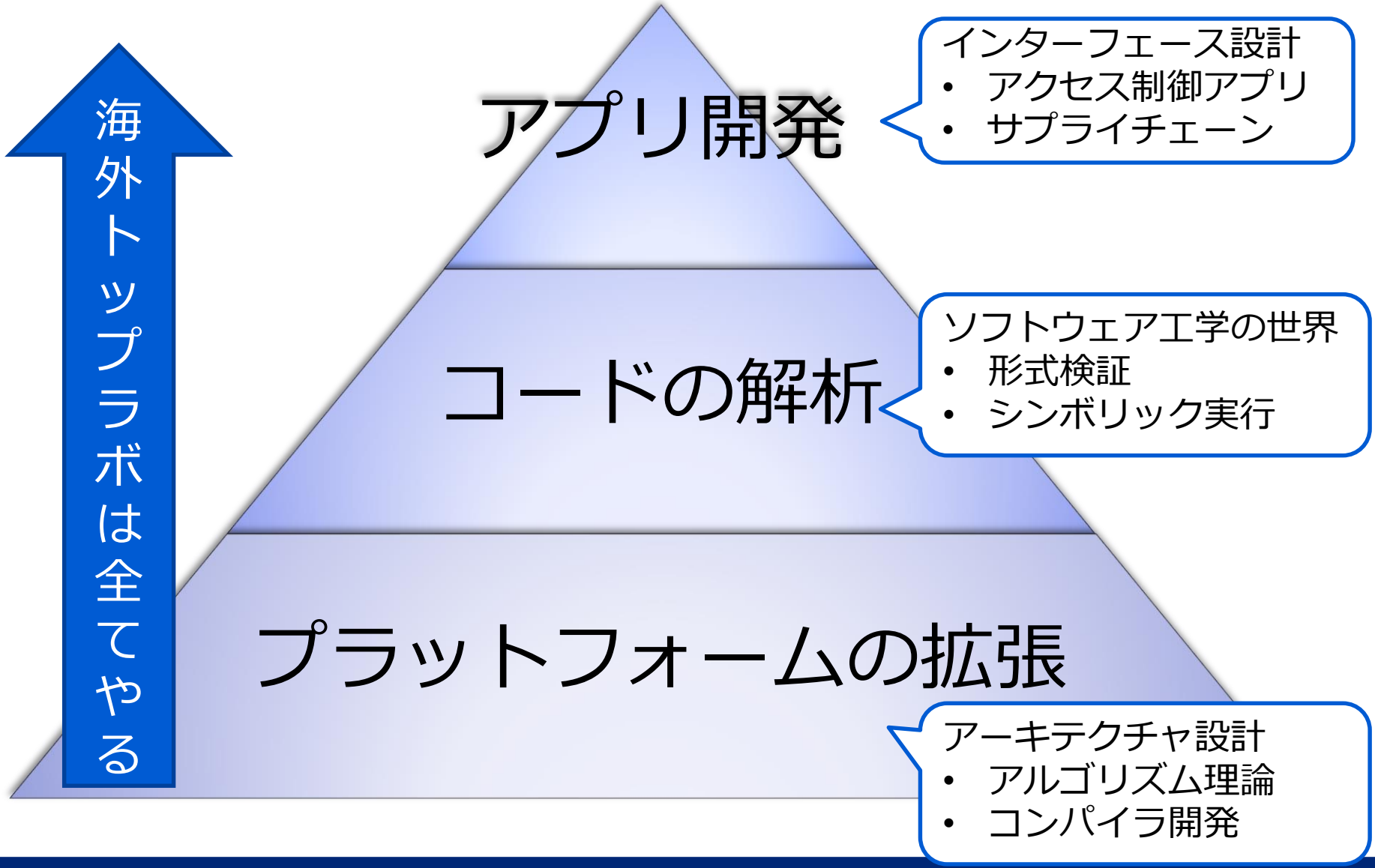
- **パリティ多重署名ウォレット攻撃**
  - 2017年に発生
  - Locked Moneyが発見された事件
  - 約1億5000万USドルの被害

- **The DAO**
  - 2016年に発生
  - Reentrancyを起点とした攻撃
  - 約6000万USドルの被害

1 https://techcrunch.com/2017/11/07/a-major-vulnerability-has-frozen-hundreds-of-millions-of-dollars-of-ethereum/
2 https://www.gemini.com/cryptopedia/the-dao-hack-makerdao

# スマートコントラクトにおける研究領域

大阪大学
OSAKA UNIVERSITY



# 日本の立ち位置はどうか？

- **サイバーセキュリティ分野では国際的プレゼンスがものすごく低い…**
  - セキュリティトップ会議にブロックチェーン論文は日本からほとんど通らず
- **一個一個の論文の規模として**
  - 海外トップラボはすべてやる（ETH Zurich や INRIA、TU Wien などがすごく強い）
  - 国内では、「どれか一層」

（個人的に必要と思ってること）
「個人型」から「チーム型」研究への移行・
チーム内で層ごとの分担と連携（一人で全てやるのは無理）

# Blocklab Meeting （in December’19）

大阪大学
OSAKA UNIVERSITY

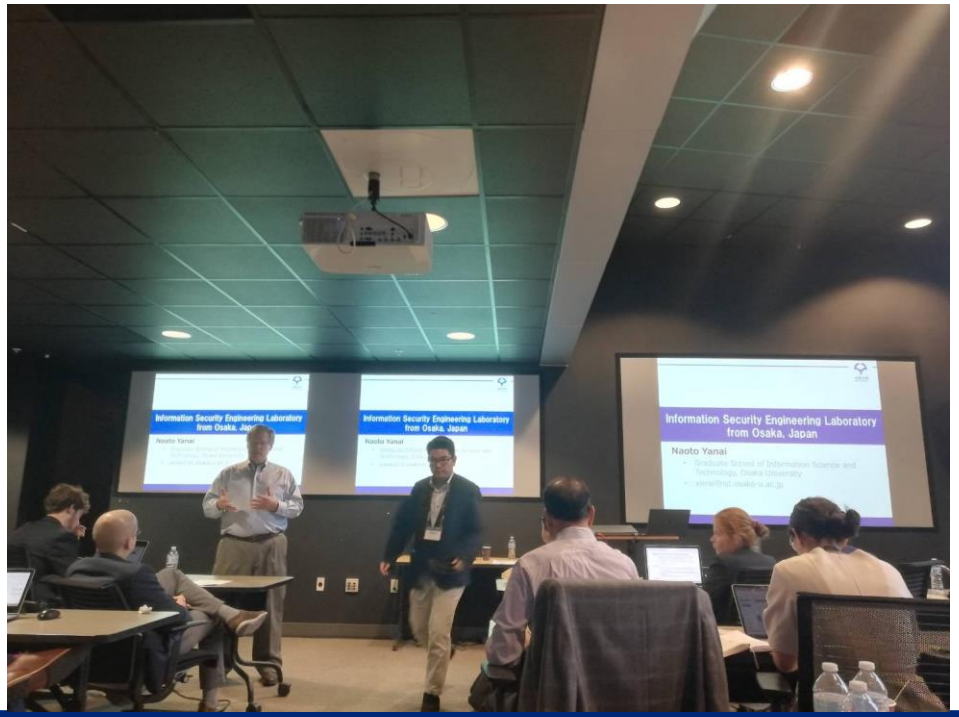
AGENDA VERSION 1.5 (12-11-2019) PLEASE DO NOT DISTRIBUTE


**SDSC Annual Winter BlockLAB Sponsors Board and Research Meeting**
**Date & Venue: Dec 12, 2019, Synthesis Center, San Diego Supercomputer Center, UC San Diego**
**Attendees: BlockLAB Founding Sponsors, LAB Principals and Invited Guests (est. 25-30 participants)**
**Chairs: Pieter De Leenheer (Collibra), Jim Short (SDSC)**

**THURSDAY, DECEMBER 12, 9:00 – 4:00 PM**

**MORNING AGENDA: SPONSORS BOARD MEETING**
**(closed meeting for sponsors, LAB principals and researchers)**

| | |
|---|---|
| **9:00 AM** | **MEETING START** |
| 9:00 – 9:15 | Welcome, Overview, Goals (P. De Leenheer, J. Short)<br>Around the Room<br>Agenda: Additions, Changes |
| **DIRECTORS REPORT** | |
| 9:15 – 10:00 | LAB Themes and Overall Goals 2019-2020<br>Project Portfolio and Publications 2019<br>LAB Financial Report 2019 |



# ブロックチェーンを使った面白い取り組み

大阪大学 OSAKA UNIVERSITY

OPEN SCIENCE CHAIN

HOME ABOUT RESOURCES PORTAL (BETA)

UCSD が開発してる科学データ管理基盤（Hyperledger Fabric ベースで、実験データの再現性を保存・保証）

**Protecting Integrity and Provenance of Research Data.**

Open Science Chain utilizes distributed ledger technology (consortium blockchain) to securely store information about scientific data including its provenance to enable independent verification of its authenticity to establish trust in the research community.

**Open Science Chain Blockchain Platform**

**Proof of Existence**

Provide immutable proof of existence of research datasets at a given point in time by storing unique identifiers of the data and ownership information on the blockchain.

**Provenance Tracking**

Promote transparency and traceability of research data by tracking and storing all changes made to data on the blockchain.

**Open Science Chain Portal**

**Data Verification & Validation**

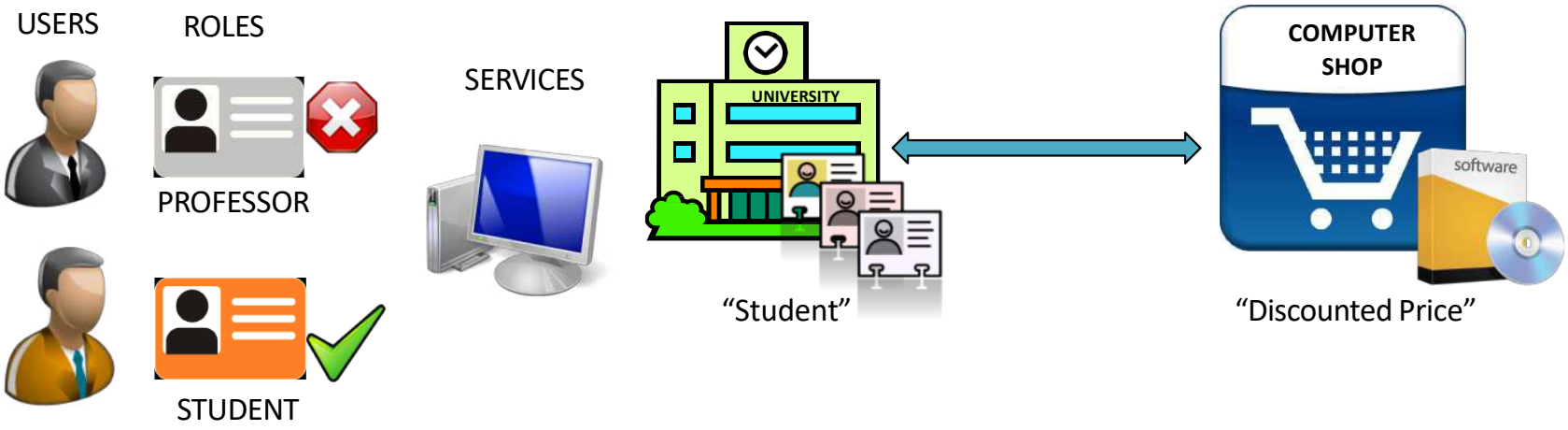
Independent verification of the authenticity of scientific data using information stored in the OSC blockchain. Search, view and validate scientific datasets including lineage information.

**Research Workflows**

Create "research workflows" linking one or more entries in the OSC blockchain, documenting an auditable record of the data workflow process behind the research hypothesis.

# 役割ベースアクセス制御(RBAC)

- RBAC はユーザとサービス間のアクセス制御関係を反映する技術
- とくにブロックチェーンを使って組織間向け推移的役割ベースアクセス制御を構成
  - (Torans-Organizational Roll-based Access Control: TO-RBAC)
-



# RBAC における認証機構の必要性

- 役割の誤った利用はセキュリティ上の懸念
  → 対策としての認証機構の導入
- しかしながら、電子的な証明書の導入は管理コストが大きい
- また、メリットがないと企業の参画を促せない

infrastructure (PKI).

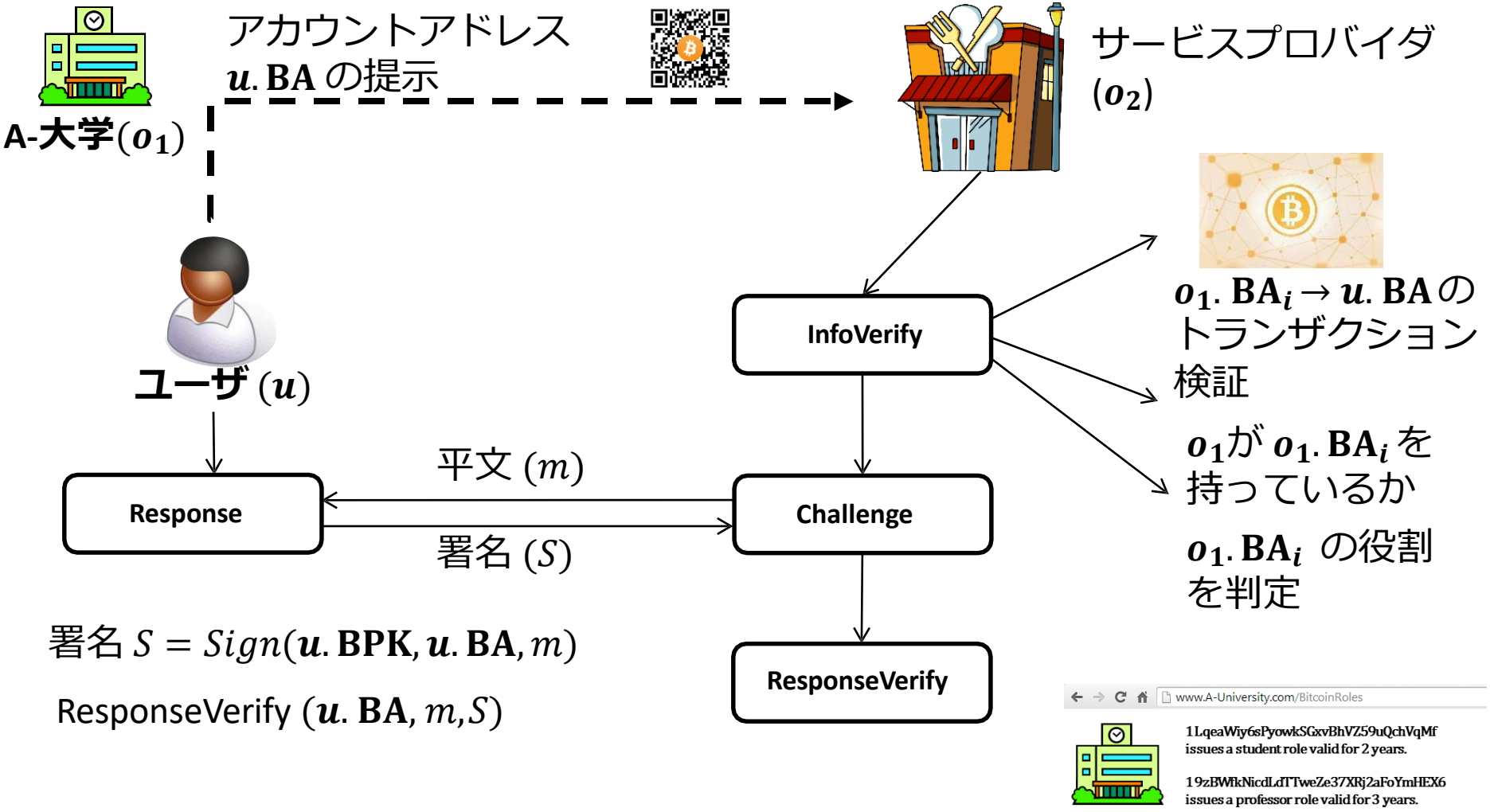

スマートコントラクトを使ったら、簡単に構成可能

# 組織間向け役割ベースアクセス制御（RBAC-SC）

大阪大学
OSAKA UNIVERSITY

- **ブロックチェーンをベース技術として利用し、各組織・ユーザごとの役割(role）間の関係をチェーンで反映**
  - 組織所属のユーザにコインを配布 → 外での利用
  - 様々な権利管理を可能にする(取引の個人化と承認)
  - タイムスタンプ機能を、役割の有効期限として利活用

# RBAC-SC の詳細


A-大学$(o_1)$
アカウントアドレス
$u.\mathbf{BA}$の提示
サービスプロバイダ
$(o_2)$
ユーザ $(u)$
InfoVerify
$o_1.\mathbf{BA}_i \rightarrow u.\mathbf{BA}$の
トランザクション
検証
$o_1$が$o_1.\mathbf{BA}_i$を
持っているか
$o_1.\mathbf{BA}_i$ の役割
を判定
平文 $(m)$
署名 $(S)$
Response
Challenge
ResponseVerify
署名 $S = Sign(u.\mathbf{BPK}, u.\mathbf{BA}, m)$
ResponseVerify $(u.\mathbf{BA}, m, S)$
www.A-University.com/BitcoinRoles
1LqeaWiy6sPyowkSGxvBhVZ59uQchVqMf
issues a student role valid for 2 years.
19zBWfkNicdLdTTweZe37XRj2aFoYmHEX6
issues a professor role valid for 3 years.

# 機械学習 × 静的解析 × スマートコントラクト

- **機械学習×静的解析：ソフトウェアの特徴量をモデルに与えて、任意のソフトウェアを分類**

解析時間の短縮

新規の脆弱性に対応

×

スマートコントラクト

- スマートコントラクトのコードリリースは時間勝負
- 解析時間の短縮と解析精度の向上が重要

# スマートコントラクトの脆弱性

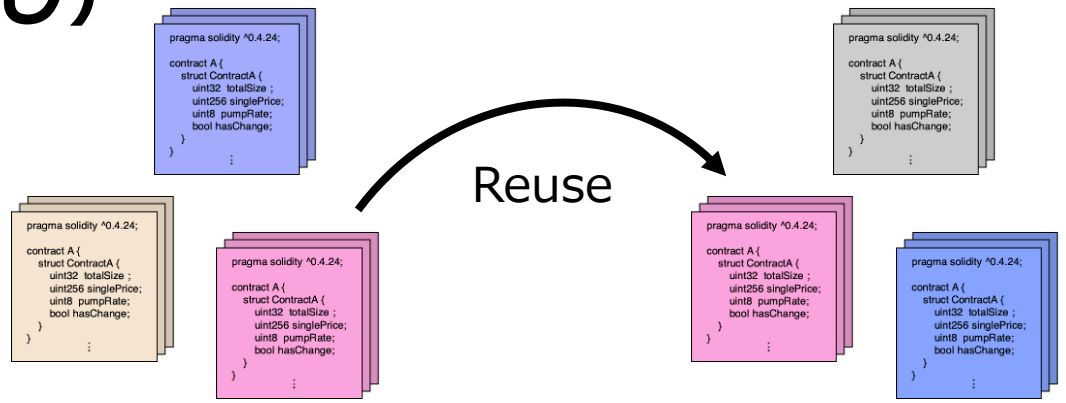
大阪大学
OSAKA UNIVERSITY

## 脆弱性に基づくインシデントの多発

- The DAO ハック: $60百万 Ethers の盗み出し

## 脆弱なコードの再利用による拡散

- **コントラクトが再利用されたなら、その中の脆弱性も利用される**
- **多くの類似コードが発見（最新バージョンでは約8割が使いまわし）**



# 静的解析

## プログラムの一般的な解析手法

- 脆弱性の発見
- マルウェア解析

```
pragma solidity ^0.4.24;

contract A {
    struct ContractA {
        uint32  totalSize ;
        uint256 singlePrice;
        uint8  pumpRate;
        bool hasChange;
```

高級言語

```
PUSH  EBP
MOV   EBP,ESP
AND   ESP,0x214
SUB   ESP,0x214
```

アセンブリ

```
01110010
01101001
01111001
00100000
01100101
01110101
```

バイトコード

## 静的解析への機械学習への利用

- プログラムの特徴量を機械学習モデルに与えることで高速な解析を実現

解析時間の短縮

新規の脆弱性の発見

# 問い: 特徴量の抽出

- とくにコードが書き換えられたときに脆弱性の検知精度が劣化

```
1 function ObsidianSmartPay(){
2     balances[msg.sender] = totalSupply;
3 }
```

```
1 function Bam() public {
2     owner = msg.sender;
3     balances[owner] = totalSupply;
4 }
```

最適な特徴量抽出は非自明 [ZL+19]

# 研究の技術的課題と講演者の活動

大阪大学
OSAKA UNIVERSITY

**技術的課題**

- **特徴量抽出の最適化**
- **コードの書き換えに対するロバスト性**
- **高速な解析**

## 講演者の活動

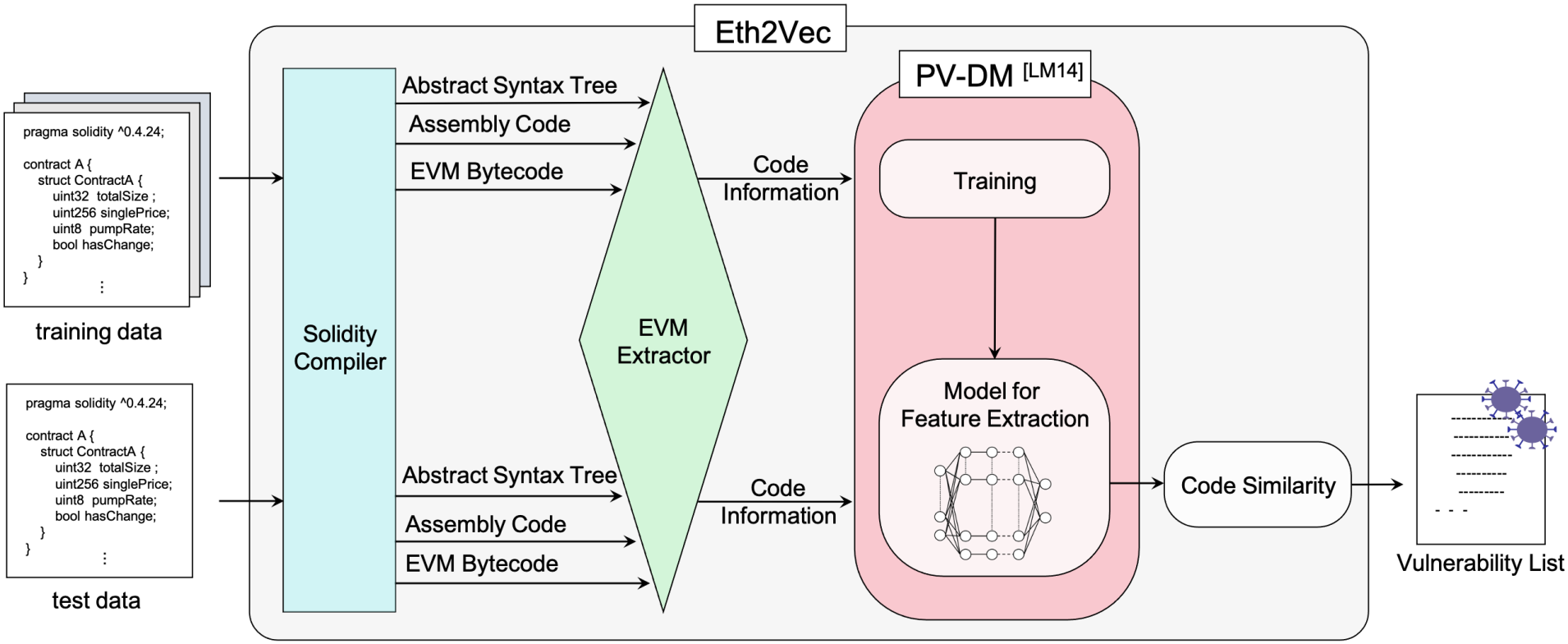
- **自然言語処理技術を活用した検知技術の設計**

自然言語処理技術の活用により、
コードの書き換えに対してもロバストな検知技術の提案

# Eth2Vec の設計

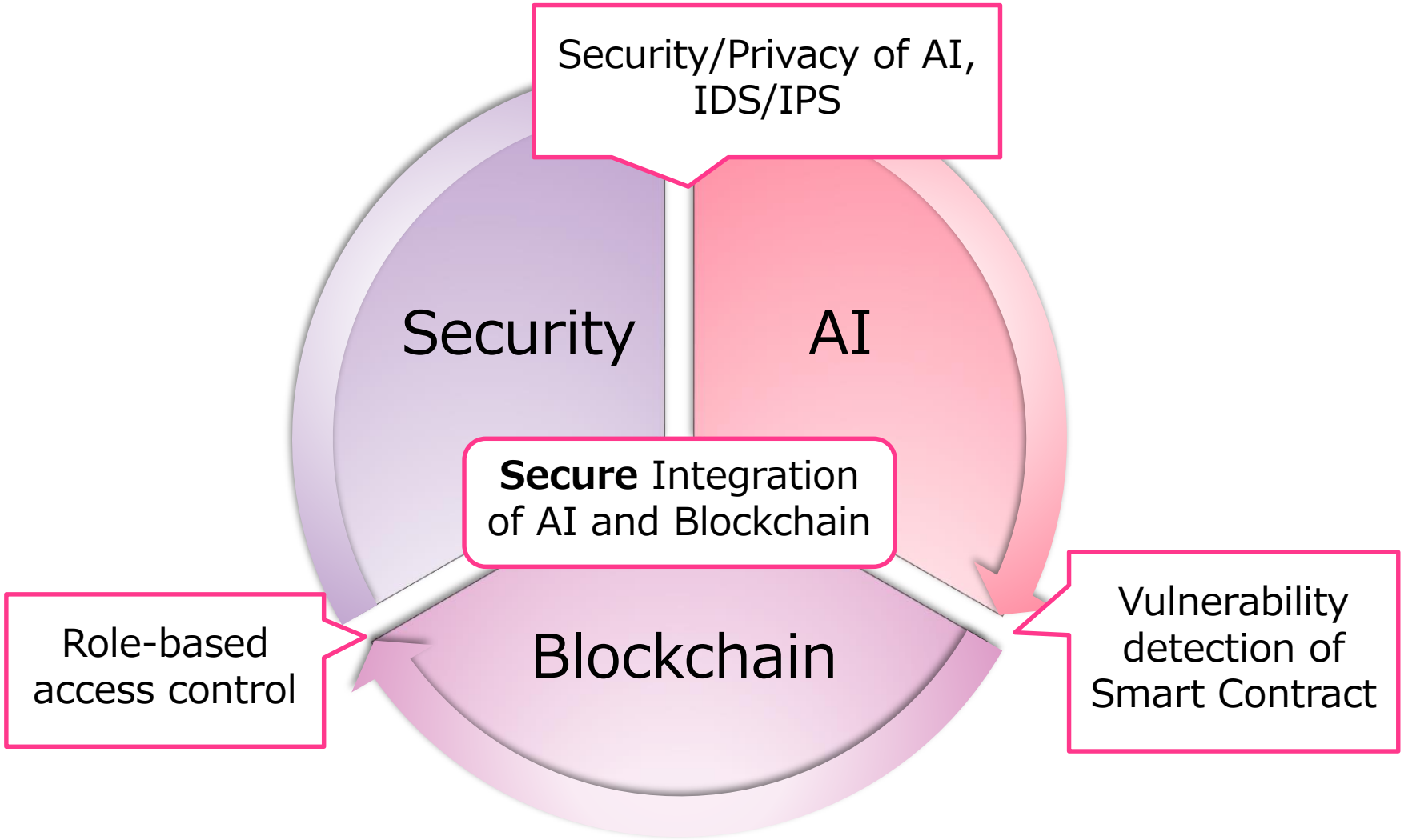
- 目的関数

$$\sum_{C_i}^{Dict\,\mathcal{U}(C_i)} \sum_{f_s}^{\mathcal{S}(f_s)} \sum_{seq_i}^{\mathcal{I}(seq_i)} \sum_{in_j}^{\mathcal{T}(in_j)} \sum_{t_c} \left\{ \log\left(\sigma(X)\right) + \sum_{i=1}^{k} \mathbb{E}_{t_d \sim P_n(t_c)} \left( [\![ t_d \neq t_c ]\!] \log\left(\sigma(X)\right) \right) \right\}$$



# セキュリティ・AI・ブロックチェーンの連携

大阪大学
OSAKA UNIVERSITY



# ブロックチェーンとセキュリティのこれから

大阪大学
OSAKA UNIVERSITY

- **1st step: 融合領域の更なる模索**
  - 機械学習との融合
  - ソフトウェア工学との融合も重要
  - セキュリティ/AI/ブロックチェーンの融合がこれからを支える
- **2nd step: “ユーザ”自体の意識向上**
  - セキュリティ/AI/ブロックチェーンの教材を開発・導入
  - 技術的課題によらない教育的課題

**Naoto Yanai: yanai@ist.osaka-u.ac.jp**