Raziel:
Private and Verifiable Smart Contracts on Blockchains

David Cerezo Sánchez*
Calctopia*
david@calctopia.com*

(This paper is a first implementation of PCT/IB2015/055776)

December 19, 2017

Abstract
Raziel combines secure multi-party computation and proof-carrying code to provide privacy, correctness and verifiability guarantees for smart contracts on blockchains. Effectively solving DAO and Gyges attacks, this paper describes an implementation and presents examples to demonstrate its practical viability (e.g., private and verifiable crowdfunding and investment funds, double auctions for decentralized exchanges). Additionally, we show how to use Zero-Knowledge Proofs of Proofs (i.e., Proof-Carrying Code certificates) to prove the validity of smart contracts to third parties before their execution without revealing anything else. Finally, we show how miners could get rewarded for generating pre-processing data for secure multi-party computation.

*Corresponding author
1 Introduction

The growing demand for blockchain and smart contract technologies sets the challenge of protecting them from intellectual property theft and other attacks: security, confidentiality and privacy are the key issues holding back their adoption. As shown in this paper, the solution must be inter-disciplinary (i.e., cryptography and formal verification techniques): code from smart contracts cannot be formally-verified before its execution with cryptographic techniques and conversely, formal verification techniques keep track of information flows to guarantee confidentiality but they don’t provide privacy on their own.

The availability of the proposed technical solution and its broad adoption is ultimately a common good: it’s in the public interest to use smart contracts that respect the confidentiality and privacy of the processed data and that can be efficiently verified. Smart contracts have recently been heralded as “cryptocurrency’s killer app”, but to develop the next digital businesses based on the blockchain (e.g., the equivalents of Paypal, Visa, Western Union, NYSE) there is an urgent need for better protected smart contracts, a gap solved on this publication.

Contributions We propose a system for securely computing smart contracts guaranteeing their privacy, correctness and verifiability. Our main and novel contributions are:

- Practical formal verification of smart contracts: the proofs accompanying the smart contracts can be used to prove functional correctness of a computation as well as other properties including termination, security, pre-conditions and post-conditions, invariants and any other requirements for well-behaved code. A smart contract that has been fully formally verified protects against the subtle bugs such as the one that enabled millions to be stolen from the DAO. And when signed proofs conform to the specifications of a trusted organization, Raziel also prevents the execution of criminal smart contracts (i.e., Gyges attacks) solving this kind of attacks for the first time.

- A practical use of Non-Interactive Zero-Knowledge proofs of proofs/certifiable certificates is proposed (see section §5.3): the code producer can convince the executing party of the smart contract of the existence and validity of proofs about the code without revealing any actual information about the proofs themselves or the code of the smart contract. Although the concept of zero-knowledge proofs of proofs is not new, it can now be realised in practice for general properties of code.

- An outsourcing protocol for secure computation that allows offline parties and private parameter reuse is presented (see section §4.6): previous approaches don’t allow all the parties to be offline: previous approaches don’t allow all the parties to be offline: previous approaches don’t allow all the parties to be offline: previous approaches don’t allow all the parties to be offline: previous approaches don’t allow all the parties to be offline, or reusing encrypted values.
• We propose that miners should get rewarded for generating pre-processing data for secure multi-party computation (see section §4.7), in line with earlier attempts to replace wasteful PoWs [Kim13, MJS+14, BRSV17, ORP17].

Minimal set of functionalities We argue that the combined features here described are indeed the minimal set of functionalities that must be offered by a secure solution to protect computations on blockchains:

• A pervasive goal of blockchain technologies is the removal of trusted third parties: towards this end, the preferred solution in cryptography is secure multi-party computation, which covers much more than transactions. Moreover, public permissionless blockchains are executing smart contracts out in the open and any curious party is able to inspect the input parameters and detailed execution of any on-chain smart contract: again, MPC is the best cryptographic solution to protect the privacy of the computation of said smart contracts.

  – Since carrying out encrypted computations has a high cost, we introduce two improvements to reduce that cost: outsourcing for cloud-based blockchains (see section §4.6) and mining pre-processing data for secure multi-party computation (see section §4.7).

• Once encrypted smart contracts are being considered, a moral hazard arises: why should anyone execute a potentially-malicious encrypted smart contract from an anonymous party? Formal verification techniques such as proof-carrying code provide an answer to this dilemma: mathematical proofs about many desirable properties (termination, correctness, security, resource consumption, legal/regulatory, economic and functional, among others) can be offered before carrying out any encrypted execution.

  – To prevent that said proofs leak too much information about the smart contracts, a novel solution for zero-knowledge proofs of proofs is proposed (see section §5.3).

This paper describes an implementation discussing cryptographic and technical trade-offs.

2 Background

This section provides a brief introduction to the main technologies that underpin Raziel: blockchains, secure multi-party computation [Gol97] and formal verification.
**Blockchains**  A blockchain is a distributed ledger that stores a growing list of unmodifiable records called blocks that are linked to previous blocks. Blockchains can be used to make online secure transactions, authenticated by the collaboration of the P2P nodes allowing participants to verify and audit transactions. Blockchains can be classified according to their openness. Open, permissionless networks don’t have access controls (e.g., Bitcoin[Nak08] and Ethereum[But14a, Woo14]) and reach decentralized consensus through costly Proof-of-Work calculations over the most recently appended data by miners. Permissioned blockchains have identity systems to limit participation (e.g., Hyperledger Fabric[Cac16]) and do not depend on proofs-of-work. Blockchain-based smart contracts are computer programs executed by the nodes and implementing self-enforced contracts. They are usually executed by all or many nodes (**on-chain smart contracts**), thus their code must be designed to minimize execution costs. Lately, off-chain smart contracts frameworks are being developed that allow the execution of more complex computational processes.

**Secure Multi-Party Computation**  Protocols for secure multi-party computation (MPC) enable multiple parties to jointly compute a function over inputs without disclosing said inputs (i.e., secure distributed computation). MPC protocols usually aim to at least satisfy the conditions of inputs privacy (i.e., the only information that can be inferred about private inputs is whatever can be inferred from the output of the function alone) and correctness (adversarial parties should not be able to force honest parties to output an incorrect result). Multiple security models are available: semi-honest, where corrupted parties are passive adversaries that do not deviate from the protocol; covert, where adversaries may deviate arbitrarily from the protocol specification in an attempt to cheat, but do not wish to be “caught” doing so; and malicious security, where corrupted parties may arbitrarily deviate from the protocol. Multiple related cryptographic techniques (including secret sharing[Sha79], oblivious transfer[Rab85], garbled circuits, oblivious random access machines[Gol87]) and MPC protocols (e.g., Yao[Yao82, Yao86, LP04], GMW[GMW87], BMR[BMR90], BGW[BGW88] and others) have been developed since MPC was originally envisioned by Andrew Yao in the early 1980s.

**Formal verification**  Formal verification uses formal methods of mathematics on software to prove or disprove its correctness with respect to certain formal specifications. Deductive verification is the preferred approach: smart contracts are annotated to generate proof obligations that are proved using theorem provers or satisfiability modulo theories solvers. In the software industry, formal verification is hardly used, but in hardware the high costs of recalling defective products explain their greater use: analogously, it’s expected a higher use of formal verification methods applied to smart contracts compared to the general rate of use on the software industry given the losses in case of errors and exploitation[Dai16].
3 Model and Goals

Parties executing smart contracts need to protect their private financial information and obtain formal guarantees regarding their execution. The central goal for Raziel is to offer a programming framework to facilitate the development of formally-verified, privacy-preserving smart contracts with secure computation.

3.1 Threat Model and Assumptions

A conservative threat model assumes that parties wish to execute smart contracts but mutually distrust each another. Each party is potentially malicious and the smart contract is developed by one of the parties or externally developed. We assume that each party trusts its own environment and the blockchain; the rest of the system is untrusted. The threat model does not include side channel attacks or denial of service attacks.

3.2 Goals

A secure smart contract system should operate as follows: a restricted set of parties willing to execute a smart contract check the accompanying proofs/certificates to verify it before its execution. Then these parties send their private inputs to the nodes at the start of the execution of the smart contract; after that, the nodes run the smart contract carrying out the secure computation. Alternatively, the same parties may run the secure computation between themselves without the use of external executing nodes. Finally, the restricted set of parties obtain the results from the secure computation, which could be stored on the blockchain according to the rules of some consensus protocol.

4 Private Smart Contracts

Enabling smart contracts with secure computation techniques (e.g., secure multi-party computation, homomorphic encryption [RAD78], indistinguishability obfuscation [BV15]) is a key-step to the global adoption of blockchain technologies: encrypted transactions could be stored on the blockchain; secure computations could be carried out between distrustful parties; even the contract’s code on the blockchain could be kept private.

Although it would be very profitable to sell/acquire smart contracts based on the value of their secret algorithms (see Markets for Smart Contracts) using homomorphic encryption (bootstrapping being a costly operation that can only be minimized [PV16, BLMZ16] and not avoided) and indistinguishability obfuscation (polynomial-time computable, but with constant factors $\geq 2^{100}$), are both considered currently infeasible due to concrete efficiency issues. In spite of impressive progress towards making these techniques practical [LMA+16, CMR17, CGGI17], they appear to be a long way from suitability for our purposes (i.e., Obfustopia is still a very expensive place, Cryptomania is much more affordable).
Another possible approach, which is being adopted by some blockchains and related technologies, is to rely on a trusted execution environment (most notably Intel’s SGX[CD16]). Relying on trusted hardware is a risky bet and assumes a high level of trust in the hardware vendor. Several severe attacks have exposed vulnerabilities of SGX[BMD+17, SWG+17, MIE17, WKP16, XCP15, SLK17, LSG+16, BCLK17, Swa17, LJ1+17, Cor17, BWK+17, JLLK17, XLCZ17b, XLCZ17a, JVB17]: all the current proposed and existing blockchains whose security rest on SGX aren’t providing detailed explanations and proofs on how they are defending against these attacks. Unlike software bugs, new hardware would have to be deployed to fix these kinds of bugs, sometimes re-architecting the full solution.

Hence, our design employs secure multi-party computation. Secure multi-party computation is more mature than the fully homomorphic methods, and has a less trusting threat model than trusted execution approaches. MPC protocols have solid security proofs based on standard assumptions and efficient implementation. Current MPC technologies that can be used in production[ABPP15] include: secret sharing, garbled circuits, oblivious transfer and ORAMs. Secret sharing based schemes (i.e., many-round, dependent on the depth of the circuit) can be faster than garbled circuits/BMR (i.e., constant-round) in low-latency settings (LANs): when latency is large or unknown, it’s better to use constant-round protocols[SZ13, BELO16].

A preferred approach is to use modular secure computation frameworks: for security reasons, at least two secure computation frameworks should be available, offering different cryptographic and security assumptions; in case the security of one of them is compromised, there will be a second option.

4.1 Off-chain computation

Even when using the fastest available secure multi-party computation techniques, the overhead would be very significant if secure computations would have to be executed on every full node of a blockchain, as have been previously proposed[But14b]. In Ethereum, at current prices (380 $/ETH, 21 Gwei/gas, 30/August/2017), multiplying or dividing 2 plaintext integers 10 million times costs:

\[
\frac{5}{\text{Gas ops}} \cdot 10000000 \text{ ops} \cdot \frac{0.000000001}{\text{ETH Gwei}} \cdot 21 \text{ Gwei} \cdot \frac{380}{\text{ETH}} = \$399
\]

and to store 32768 words of 256 bits (i.e. 1 megabit), it costs:

\[
2000 \frac{\text{Gas SSTORE}}{\text{ops}} \cdot 32768 \text{ ops} \cdot \frac{0.000000001}{\text{ETH Gwei}} \cdot 21 \text{ Gwei} \cdot \frac{380}{\text{ETH}} = \$523
\]

However, multiplying 2 plaintext integers 10 million times on a modern computer takes 0.02 seconds: since it costs $0.004/hour (Amazon EC2 t2.nano 1-year Reserved Instance), the same multiplications cost

\[
\frac{\$0.004 \text{ hour}}{3600 \text{ seconds/hour}} \cdot 0.02 \text{ seconds} = \$0.000000022
\]
It’s order of magnitude more expensive, concretely

\[
\frac{399}{0.000000022} = 18136363636.3636364
\]

That is, more than 18 billions times more expensive: and as the price of Ether keeps rising, the costs of computation will also rise. On another note, current state-of-the-art secure computation executes 7 billion AND gates per second on a LAN setting [AFL+16], but an 8-core processor executes 316 GIPS at the Dhrystone Integer Native benchmark (Intel Core i7-5960X), an approximate slowdown of

\[
\frac{316 \text{ GIPS}}{7 \text{ Billion gates/second}} = 45.142857143 \times
\]

which must not be additionally imposed to the overhead/overcost of a public permissionless distributed ledger: on the hand, it also means that there are overheads/overcosts being accepted which are higher than those imposed by secure computation or verifiable computation (\(10^5 - 10^7\) for proving correctness of the execution [WB15]).

We address on-chain and off-chain secure computations separately:

- For on-chain secure computations, the validation of transactions happens through the replicated execution of the smart contract and given the fault assumption underlying the consensus algorithm. Because privacy-preserving smart contracts introduce a significant resource consumption overhead, it is important to prevent the execution of the same privacy-preserving smart contract on every node. We relax the full-replication requirement for PBFT consensus: a “query” command could be executed on a restricted set of nodes (large enough to provide consensus), and then an “invoke” store the result in the distributed ledger. Finally, achieving consensus is a completely deterministic procedure, with no possible way for differences.

- Regarding off-chain secure computations, simple oracle-like calls could be considered or other more complex protocols [HMP17, TR17, iEx17] for scalable off-chain computation.

4.1.1 Latency and its impact

As previously mentioned, MPC protocols can be roughly divided into two classes: constant-round protocols, ideal for high latency settings; and protocols with rounds dependent on the depth of the evaluated circuit, usually faster but only on very low latency settings. The present paper proposes the use of two protocol suites to get the maximum performance, independent of the latency:

- if all parties are on a low latency setting, they could use a very fast secret-shared protocol [AFL+16, BLW08]
• but if parties are on a high latency setting, they must use a constant-round protocol \[\text{[KRW17, WMK16a, BELO16, HSSV17, BELO17, BEO17]}\]. Alternatively, they could outsource the secure computation to a cloud setting (see section §A) to use a faster secret-shared protocol.

4.2 Blockchain Solutions

The guarantees of privacy, correctness and verifiability are designed for the more threatening setting of public permissionless blockchains, although the smart contracts can also be used on private permissioned blockchains: it’s also preferred that private blockchains keep their communications open to public blockchains to allow the use of smart contracts of public utility.

We considered two blockchains solutions:

• Hyperledger Fabric \[\text{[Cac16]}\] is a good fit for executing complex computational procedures like secure multi-party computation and formal verification techniques: including such complex procedures on its chaincodes (i.e. smart contracts) requires no special design considerations.

• Ethereum \[\text{[But14a]}\] is a public permissionless blockchain and integrating complex procedures on its smart contracts is much trickier: executed code consumes \textit{gas}, thus the general pursuit to minimize the number of executed instructions. For complex procedures, oracles are the best option (external data providers, not to be confused with random oracles in cryptography or oracle machines in complexity theory). The initial purpose of oracles is to provide data that didn’t belong in the blockchain (e.g., web pages) because decentralized applications that achieve consensus shouldn’t rely on off-chain sources of information. But the mechanism can also be used for off-chain execution of complex code. The steps to incorporate an oracle are:

1. Contract call to on-chain contract that executes complex computational procedures (e.g., secure multi-party computation). Said call must include enough \textit{gas} and the correct parameters:
   (a) Parameters should be encrypted to prevent that other participants of the blockchain inspect them: a public key should be available for this purpose; only the executing oracle should be able to decrypt the parameters using the corresponding private key. Said executing oracle must be implemented as a trusted server of the calling party; otherwise, a more complex protocol involving outsourced oblivious transfer must be used.
   (b) Contributed \textit{gas} is used to cover the costs of returning results to the calling contract.

2. The executing oracle receives the contract call, decrypts the data and proceeds to the off-chain execution of the complex computational procedure.
3. The executing oracle returns back the results to the calling contract address.

4. Calling contract obtains the results: if large results are expected (e.g., some few kilobytes) it’s better to store them on IPFS\cite{Ben14} to prevent gas costs, and what would be returned is a pointer to said results.

Regarding Bitcoin\cite{Nak08}, although it would be possible to use oracles\cite{Ori14} similar to the ones used for Ethereum, these are hardly used due to a combination of high transaction fees, high confirmation time and low transaction rate.

4.2.1 Alternative Protocols and Standards

Although this paper is focused on blockchains, it could be adopted to other financial standards such as:

- Financial Information eXchange\cite{Com16}: messaging standard for trade communication in the equity markets, with presence in the foreign exchange, fixed income and derivatives market.

- Financial Products Markup Language (FpML)\cite{SA17}: XML messaging standard for the Over-The-Counter derivatives industry.

4.3 Functionality and Protocol

The functionalities and protocols of this sub-section and section 6 constitute an open framework on which to instantiate different secure multi-party computation protocols, thus benefiting from upcoming research advances.

In this sub-section we present our secure protocol for private smart contracts, consisting of the following standard functionality:

<table>
<thead>
<tr>
<th>Functionality 4.1: Secure computation of smart contracts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parties:</strong> $E_1, ..., E_N$, set of nodes $N_i$ of a blockchain $B$</td>
</tr>
<tr>
<td><strong>Inputs:</strong> smart contract $SC$, private inputs from parties $E_1 : \overrightarrow{x}, E_2 : \overrightarrow{y}, ..., E_N : \overrightarrow{z}$</td>
</tr>
<tr>
<td><strong>The functionality:</strong></td>
</tr>
<tr>
<td>1. Secure computation of smart contract $SC$</td>
</tr>
<tr>
<td>2. Results are returned and/or saved on the blockchain $B$</td>
</tr>
<tr>
<td><strong>Output:</strong> results from the secure computation $E_1 : \overrightarrow{r_1}, E_2 : \overrightarrow{r_2}, ..., E_N : \overrightarrow{r_N}$</td>
</tr>
</tbody>
</table>

Functionality 4.1 (Secure computation of smart contracts) is implemented by the following protocol:
Protocol 4.2: Realising Functionality 4.1 (Secure computation of smart contracts)

- **Parties:** $E_1, ..., E_N$, set of nodes $N_i$ of a blockchain $B$
- **Inputs:** smart contract $SC$, private inputs from parties $E_1 : \vec{x}, E_2 : \vec{y}, ..., E_N : \vec{z}$
- **The protocol:**

  1. Parties $E_1, ..., E_N$ proceed to execute the smart contract $SC$:
     
     (a) The private inputs $\vec{x}, \vec{y}, ..., \vec{z}$ and non-private inputs are sent to nodes $N_i$:
        
        i. Technically, this could be a HTTPS/REST call or an oracle call to executing nodes $N_i$.
        
        ii. The number of executing nodes $N_i$ depends on the setting of the blockchain $B$ (public/private permissionless/permissioned): that is, it could range from every node of the blockchain $B$ to just a subset of nodes under PBFT consensus.
        
        iii. On permissioned blockchains, each executing node $N_i$ should be a server owned/operated by the corresponding calling party $E_i$ (i.e., the servers are assumed to be trusted and the adversary is on the network); but if the nodes are being run on a public cloud or any other server outside the full control of the corresponding calling party $E_i$, then a protocol for outsourcing secure computations must be used (see section §A).
     
     (b) The executing nodes $N_i$ proceed to execute the smart contract $SC$: the execution command from parties $E_1, E_2, ..., E_N$ contains the preferred secure computation engine to be used (i.e., there could be multiple execution engines with different protocols under various security assumptions; if the parties don’t agree, the secure computation will not be carried out).

  2. If consensus on the results of the previous computation is reached, then said results $\vec{r}_1, \vec{r}_2, ..., \vec{r}_N$ could be returned to executing parties $E_1, E_2, ..., E_N$ and/or written on the blockchain $B$.

- **Output:** results from the secure computation $E_1 : \vec{r}_1, E_2 : \vec{r}_2, ..., E_N : \vec{r}_N$.

The security of the protocol is proved on section §6.3

4.4 Experimental Results

Table 1 summarizes the execution cost for several example applications, chosen for their economic significance:
1. Millionaire’s Problem (i.e., determining who’s got the bigger number without revealing anything else)

2. Second-price auction: sealed-bid auction not revealing the bids between the participants and without an auctioneer. The highest bidder wins, but the price paid is the second-highest bid\cite{Vie61}.

3. European Exchange Options: valuation of an option (the right, but not the obligation) using Margrabe’s formula\cite{Mar78} to exchange one risky asset for another risky asset at the time of maturity; this example is useful to hedge private portfolios of volatile crypto-tokens of physical assets. Suppose two risky assets with prices $S_1(t)$ and $S_2(t)$ at time $t$ and each with a constant dividend yield $q_i$: we calculate the option to exchange asset 2 for asset 1 has a payoff $\max (0, S_1(t) - S_2(t))$,

\[
\text{Price option } = S_1e^{-q_1 t}N(d_1) - S_2e^{-q_2 t}N(d_2)
\]

\[
\sigma = \sqrt{\sigma_1^2 + \sigma_2^2 - 2\rho \sigma_1 \sigma_2}
\]

\[
d_1 = \frac{\ln \left( \frac{S_1}{S_2} \right) + \left( q_2 - q_1 + \frac{\sigma_2^2}{2} \right) t}{\sigma \sqrt{t}}
\]

\[
d_2 = d_1 - \sigma \sqrt{t}
\]

where $\rho$ is the Pearson’s correlation coefficient of the Brownian motion of $S_i$ and $\sigma_i$ are the volatilities of $S_i$. Private inputs are $\sigma_i$, $S_i$ and $q_i$.

4. Currency Exchange Options: valuation of an option (the right, but not the obligation) using the model of Garman-Kohlhagen\cite{GK83} to exchange one currency for another at a fixed price; this example is useful to hedge private portfolios of volatile crypto-currencies. Suppose two risky currencies with different interest rates but constant exchange rate: we calculate the calls and puts with the following equations,

\[
\text{Call } = S_0e^{-\rho t}N(d_1) - X^{-r t}N(d_2)
\]

\[
\text{Put } = Xe^{-r t}N(-d_2) - S_0e^{-\rho t}N(-d_1)
\]

\[
d_1 = \frac{\ln \left( \frac{S_0}{X} \right) + \left( r - \rho + \frac{\sigma^2}{2} \right) t}{\sigma \sqrt{t}}
\]

\[
d_2 = d_1 - \sigma \sqrt{t}
\]

where $r$ is the continuously compounded domestic interest rate, $\rho$ is the continuously compounded foreign interest rate, $S_0$ is the spot rate, $X$ is the strike price, $t$ is the time to maturity and $\sigma$ is the foreign exchange rate volatility. Private inputs are $r$, $\rho$ and $S_0$ (with constant exchange rate).

5. Crowdfunding smart contract: a simple crowdfunding smart contract is considered, that checks if the minimum contribution target is reached and
then returns the raised amount, or 0 otherwise.

**Algorithm 1** Crowdfunding smart contract

```c
int crowdfund(int inputX, int inputY) {
    int ret;
    int sum = inputX + inputY;
    int minimum = 1000;
    if ( sum >= minimum ) ret = sum; else ret = 0;
    return ret;
}
```

6. DAO-like Investment Fund: a simple emulation of an investment fund is considered, that check if the minimum contribution target is reached and then returns the principal compounded after a number of years.

**Algorithm 2** DAO-like Investment Fund

```c
float daoInvestFund(int inputX, int inputY) {
    float ret;
    int sum = inputX + inputY;
    int minimum = 1000;
    if ( sum >= minimum ) ret = sum * (1 + (0.04/4))^(4*5); else ret = 0;
    return ret;
}
```

7. Double auction for decentralized exchanges: the secrecy of the prices and quantities is maintained during the off-chain secure computation and the settlement is finally done on-chain. Secure computation is very useful in these settings because it enables secret order books, increasing liquidity and price discovery under specially designed mechanisms [Int15].
Table 1: Execution times for application experiments. The times shown are the wall clock time in millisecond to complete the secure multi-party computation (i.e., from the initial oblivious transfers to the final reveling of the results) for various secure multi-party computation engines (A: semi-honest; B: malicious security; C: secret-sharing (Sharemind[BLW08] estimation)).

<table>
<thead>
<tr>
<th>Example</th>
<th>AND Gates</th>
<th>Time A</th>
<th>Time B</th>
<th>Time C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Millionaire (int)</td>
<td>96</td>
<td>1</td>
<td>1</td>
<td>0.485</td>
</tr>
<tr>
<td>Second-price Auction (int)</td>
<td>192</td>
<td>1.1</td>
<td>1</td>
<td>0.862</td>
</tr>
<tr>
<td>European Exchange Options (float)</td>
<td>267507</td>
<td>810</td>
<td>1273.8</td>
<td>1185.49</td>
</tr>
<tr>
<td>Currency Call Options (float)</td>
<td>323529</td>
<td>979.6</td>
<td>1540.6</td>
<td>957.77</td>
</tr>
<tr>
<td>Crowdfunding smart contract (int)</td>
<td>128</td>
<td>1</td>
<td>1</td>
<td>0.458</td>
</tr>
<tr>
<td>DAO-like Investment Fund (int)</td>
<td>2144</td>
<td>6.5</td>
<td>10.2</td>
<td>0.458</td>
</tr>
<tr>
<td>Double auction (int)</td>
<td>567829</td>
<td>1419</td>
<td>2552.2</td>
<td>2137.2</td>
</tr>
</tbody>
</table>

4.5 Modes of Interaction

Secure computation can be carried on the nodes of the blockchain or on the parties themselves. Additionally, said secure computations can be outsourced...
to the cloud (see section §4.6) or use mined pre-processing data for secure multi-party computation (see section §4.7).

4.6 Outsourcing Secure Computations for Cloud-based Blockchains

The following scheme makes use of a multi-party non-interactive key exchange\cite{BZ13,MZ17} to establish a shared secret between the computing parties and the executing nodes of the blockchain: replacing the NIKE protocol would require a PKI infrastructure between the computing parties and the executing nodes that will be used to establish shared secrets between them; it’s viable but also more cumbersome within the context of public permissionless ledgers. A multiparty non-interactive key exchange (NIKE) scheme consists of the following algorithms:

- **Setup**(\(M, N, \lambda\)): this algorithm outputs public parameters \(\text{params}\), taking as input \(M\), the maximum number of parties that can derive a shared key, \(N\), the maximum number of parties in the scheme, and the security parameter \(\lambda\).

- **Publish**(\(\text{params}, i\)): this algorithm outputs the party’s secret key \(\text{sk}_i\), and a public key \(\text{pk}_i\) which the party publishes; inputs are public parameters \(\text{params}\) and the party’s index \(i\).

- **KeyGen**(\(\text{params}, i, \text{sk}_i, S, \{\text{pk}_j\}_{j \in S}\)): this algorithm outputs a shared key \(k_S\); inputs are public parameters \(\text{params}\), the party’s index \(i\), the set \(S \subseteq [N]\) of size at most \(M\) and the set of public keys \(\{\text{pk}_j\}_{j \in S}\) of the parties in \(S\).

As specified below, the functionality for outsourcing secure computations satisfies the following requirements:

- **offline parties**: no parties need to be involved when the outsourced secure computation is executed.

- **private parameters reuse**: parties don’t need to re-upload their private parameters.

- **restricted collusion**: an adversary may corrupt a subset of the parties or the nodes of the blockchain, but not both\cite{KMR11}.
Functionality B.1: Outsourcing for Cloud-based Blockchains

- **Parties:** \(E_1, E_2, ..., E_N\), set of nodes \(N_i\) of a blockchain \(B\) (\(N_G\) being the garbling node and \(N_E\) being the evaluator node)

- **Inputs:** smart contract \(SC\), private inputs from parties \(E_1 : x_1, E_2 : x_2, ..., E_N : x_N\)

- **The functionality:**

1. **KeyExchange:** run a multi-party NIKE between parties \(E_1, E_2, ..., E_N\) and nodes \(N_i\) and publish their public keys \(pk_i\); from said public keys, a secret key \(k_S\) is derived.

2. **SendPrivateParameters\((E_i)\):** send \((SendPrivateParameters, E_i)\) to \(N_E\).

3. **SECCOMP\((SC)\):** upon the reception of a computation request from party \(E_k\) for a function in smart contract \(SC\), compute \(y = SC(x_k, \{x_j | \forall j \in N : E_j\})\); send \((result, y)\) to \(E_k\) and \((SECCOMP, SC, E_k)\) to \(N_E\).

Let \(Enc\) be a symmetric-key encryption algorithm secure against Chosen-Plaintext Attacks. The following protocol uses a pivot table during the secure computation, allowing the evaluator node to obliviously map the encoded inputs by the parties to the encoding expected by the circuit created by the garbling node. To implement Functionality B.1 (Outsourcing for Cloud-based Blockchains), the following protocol is proposed:
Protocol B.2: Realising Functionality B.1 (Outsourcing for Cloud-based Blockchains)

- **Parties:** $E_1, E_2, ..., E_N$, set of nodes $N_i$ of a blockchain $B$ ($N_G$ being the garbling node and $N_E$ being the evaluator node)

- **Inputs:** smart contract $SC$, private inputs from parties $E_1: \overrightarrow{x_i}, E_2: \overrightarrow{x_i}, ..., E_N: \overrightarrow{x_i}$

- **The protocol:**

1. *KeyExchange*: run a multi-party NIKE between parties $E_1, E_2, ..., E_N$ and nodes $N_i$ and publish their public keys $pk_i$; from said public keys, a secret key $k_S$ is derived.

   (a) The setup phase is executed: $\text{params} := \text{Setup}(M, N, \lambda)$

   (b) Each party $i$ runs $\text{pk}_i, \text{sk}_i := \text{Publish}(\text{params}, i)$ and publish $\text{pk}_i$

   (c) Each party $i$ runs $k_S := \text{KeyGen}(\text{params}, i, \text{sk}_i, S, \{\text{pk}_j\}_{j \in S})$ to obtain the shared secret key

2. *SendPrivateParameters($E_i: \overrightarrow{x_i}, k_S$)*: party $E_i$ chooses nonce $n_i$ and for every bit of $\overrightarrow{x_i}$ computes $X_{\overrightarrow{x_i}[l]} = \text{PRF}_{k_S} (\overrightarrow{x_i}[l], n_i)$; then, party $E_i$ sends these to $N_E$ and also sends $n_i$. $N_E$ stores $((X_{\overrightarrow{x_i}[1]}, ..., X_{\overrightarrow{x_i}[l]}), n_i)$.

3. *SECCOMP ($SC$)*:

   (a) Secure computation at node $N_G$: the garbling node $N_G$ compiles and garbles smart contract $SC$ into the garbled circuit $GC_{SC}$. Then, for each party $E_j$ and index $l$ of the length of $\overrightarrow{x_i}$:

   i. Compute pivot keys: generate $s^{0}_{jl} = \text{PRF}_{k_S} (0, l, n_j), s^{1}_{jl} = \text{PRF}_{k_S} (1, l, n_j)$.

   ii. Compute and save garbled inputs: using the pivot keys, encrypt $\text{Enc}_{s^{0}_{jl}} (w^{0}_{jl})$ and $\text{Enc}_{s^{1}_{jl}} (w^{1}_{jl})$; then save them into pivot table $P_q[j, l]$ in random order.

   (b) Secure computation at node $N_E$: for every bit of $x_j$ and using the encoding $X_{x_j[l]}$, decrypt the correct garbled values of each $E_j$ from $P_q$; evaluate the garbled circuit $GC_{SC}$ and send the output to $N_G$.

   (c) Result at $N_G$: decode the output to obtain the results $\overrightarrow{r_1}, \overrightarrow{r_2}, ..., \overrightarrow{r_N}$.

- **Output:** results from the secure computation $E_1 : \overrightarrow{r_1}, E_2 : \overrightarrow{r_2}, ..., E_N : \overrightarrow{r_N}$.

Theorem 1. (Outsourcing for Cloud-Based Blockchains). Assuming secure channels between the parties $E_1, E_2, ..., E_N$ and the nodes $N_i$ of the blockchain $B$, Protocol B.2 securely realises Functionality B.1 against static corruptions.
in the semi-honest security model with the garbling scheme satisfying privacy, obliviousness and correctness.

Proof. See Appendix A.

4.7 Mining pre-processing data for Secure Multi-Party Computation

The Proof-of-Work of crypto-currencies consumes great amounts of computational power and electricity: 14TWh for Bitcoin\cite{Dig17a} and 4.25TWh for Ethereum\cite{Dig17b} just calculating hash functions. Miners could create pre-processing data for secure multi-party computation and be incentivised with crypto-tokens: 50-80% of total execution time is spent on pre-processing depending on the function/protocol, thus they would be profiting from "renting" their computational power to save significant amounts of computational time.

A recent paper considers the case of outsourcing MPC-Preprocessing\cite{SSW17} to third parties and then computing parties reusing the pre-processed data (i.e., SPDZ-style authenticated shares) in the online phase: it’s especially efficient if there is a subset of parties trusted by all the computing parties which can do all of the pre-processing and then distribute it to the computing parties. It’s based on the re-sharing technique of \cite{BGW88}, but without using zero-knowledge proofs: it also fits into another recent protocol for secure multi-party computation\cite{KRW17,WMK16a} that is much more efficient for WAN networks than SPDZ derivatives, except that \cite{KRW17} uses BDOZ-style authenticated shares instead of SPDZ-style authenticated shares:

- BDOZ-style\cite{BDOZ10} authenticated shares: for each secret bit $x$, each party holds a share of $x$; for each ordered pair of parties $(P_i, P_j)$, $P_i$ authenticates its own share to $P_j$. Specifically, when party $P_i$ holds a bit $x$ authenticated by $P_j$, this means that $P_j$ is given a random key $K_j [x] \in \{0, 1\}^k$ and $P_i$ is given the MAC tag $M_j [x] := K_j [x] \oplus x \Delta_j$, where $\Delta_j \in \{0, 1\}^k$ is a global MAC key held by each party. Let $[x]_i$ denote an authenticated bit where the value of $x$ is known to $P_i$ and is authenticated to all other parties: that is, $(x, \{M_k [x]\}_{k \neq i})$ is given to $P_i$ and $K_j [x]$ is given to $P_j$ for $j \neq i$. An authenticated shared bit $x$ is generated by XOR-sharing $x$ and then distributing the authenticated bits $\{ [x]_i \}$: let $(x) := (x, \{M_j [x], K_i [x]\}_{j \neq i})$ denote the collection of these authenticated shares for $x$.

- SPDZ-style\cite{DPSZ11} authenticated shares: each party holds a share of a global MAC key; for a secret bit $x$, each party holds a share $x$ and a share of the MAC on $x$. Specifically, a value $x \in \mathbb{F}_q$ is secret shared among parties $P$ by sampling $(x_i)_{i \in P} \leftarrow \mathbb{F}_q^{|P|}$ subject to $x = \sum_{i \in P} x_i$ with a party $i$ holding the value $x_i$; the MAC is obtained by sampling $(\gamma (x))_{i \in P} \leftarrow \mathbb{F}_q^{|P|}$ subject to $\sum_{i \in P} \gamma (x)_i = \alpha \cdot x$ and party $i$ holding the share $\gamma (x)_i$: let
$$\langle x \rangle := ((x_i)_{i \in P}, (\gamma(x)_i)_{i \in P})$$

to denote that $x$ is an authenticated secret share value, where party $i \in P$ holds $x_i$ and $\gamma(x)_i$, under a global MAC key $\alpha = \sum_{i \in P} \alpha_i$. It’s straightforward to adapt the protocol $\Pi_{\text{Prep}}^{R \rightarrow Q}$ from [SSW17] to process BDOZ-style authenticated shares instead of SPdz-style authenticated shares: thus, the authenticated shares generated by the offline pre-processing parties would be reshared amongst the computing parties as required before executing any secure multi-party computation and the pre-processing parties would be incentivised with crypto-tokens. Another recent paper [ZHC17] concurrently considered the generation of a pool of garbled gates to provide on-demand secure computation services between two parties, a similar concept except that it doesn’t include outsourcing from third parties.

4.7.1 Security setting

Let $E$ denote the set of $n_E$ parties who are to run the online phase and $O$ the set of $n_O$ outsourcing parties that run the pre-preprocessing for the executing parties $E$ (respectively $Q$ and $R$ in [SSW17]). Adversaries can corrupt a majority of parties in $E$ and in $O$, but not all parties in $E$ nor all parties in $O$: that is, each honest party in $E$ believes that there is at least one honest party in $O$, but they may not know which one is honest. Let $t_E$ denote the number of parties in $E$ that are corrupt (resp. $t_O$ in $O$): the associated ratios are denoted by $\epsilon_E = t_E/n_E$ and $\epsilon_O = t_O/n_O$. The executing parties $E$ are divided into subsets $\{E_i\}_{i \in O}$ forming a cover, with a party in $O$ associated with each subset: a cover is defined to be secure if at least one honest party in $O$ is associated to one honest party in $E$.

In public permissionless blockchains, it’s expected that there is no prior trust relation between parties in $E$ and $O$: an efficient algorithm is offered in [SSW17] for assigning a cover to the network of parties so that the adversary can only win with negligible probability in the security parameter $\lambda$ in the case where the covers are randomly assigned, and working out the associated probability of obtaining a secure cover. It assumes that each party in $O$ sends to the same number of parties $l \geq \lceil n_E/n_O \rceil$ in $E$. The high-level idea of the algorithm is the following:

1. For each party in $E$, we assign a random party in $O$, until each party in $O$ has $\lceil n_E/n_O \rceil$ parties in $O$ assigned to it

2. For each party in $O$, we assign random parties in $E$ until each party in $O$ has $l$ total parties which it sends to.

The probability to obtain a secure cover is given by

$$1 - \frac{t_E! \cdot (n_E - (n_O - t_O - 1) \lceil n_E/n_O \rceil)!}{n_E! \cdot (t_E - (n_O - t_O - 1) \lceil n_E/n_O \rceil)!} \cdot \left( \frac{t_E - \lceil n_E/n_O \rceil}{l - \lceil n_E/n_O \rceil} \right)^{n_O - t_O - 1}$$
In case where all but one party is corrupt in each $E$ and $O$, then the probability to obtain a secure cover is given by $l/n_E$.

4.7.2 Preventing Sybil attacks

In the context of blockchains, Sybil attacks in which an attacker creates a large number of pseudonymous identities can easily be prevented: before running secure computations, any party could be required to deposit some arbitrarily high amount of money on a smart contract that would be confiscated in case any abnormal behaviour is detected (e.g., selective failure attacks, aborts, ...). Note that this simple technique maintains the anonymity of the parties and prevents that the computed pre-processing data gets intentionally wasted.

4.8 Other Applications

Applications of this technology can be found on many commercial/financial settings. Some of the most noteworthy are as follows:

- the most immediate application of secure multi-party computation is the removal of third parties and the financial industry has plenty of them: market makers, escrows, custodians, brokers, even banks themselves are intermediaries between savers and borrowers.

- crypto-banks: all the financial information contained within bank’s databases could be encrypted with secure computation techniques. Users could make deposits, take loans and trade financial instruments without ever revealing their financial positions/transactions to inquiring third-parties.

Other applications mentioned in literature:

- economic/financial applications: financial exposures could be shared between mutually distrusting parties without revealing any confidential information to better control financial risks [EAA11], credit scoring [DDN’15, Lie13]; facilitate the work of financial supervisors [FKOS13] without compromising confidentiality; protect the privacy of data in online marketplaces [CHK’11]; re-implement the stock market [Jut12] without a trusted auctioneer and no party learning the order book; remove escrows [Kum16] with claim-or-refund transactions and secure computation.

- game theory/mechanism design: remove trusted third-parties in tâtonnement algorithms [WCT11] for one-time markets, allowing to privately share the utility function of the involved parties without revealing it and obtaining an incentive compatible protocol in the process; privacy-preserving auctions [AACM16, AV17]; more generally, implement mechanisms respecting privacy to obtain incentive-compatibility (e.g., auctions [NPS99, EL03] or that incentivise data-driven collaboration among competing parties [AGP15].
• statistics: benchmark the performance of companies within the same sector \cite{BTW11}; establish correlation and causation \cite{BKK+15} between confidential datasets.

5 Verifiable Smart Contracts

After the DAO attack, there has been some work \cite{Hir17, BDLF+16, Fro16, PE16, HSR+17} to include formal methods in the development of smart contracts: unfortunately, current solutions are very complex and cumbersome \cite{Hir17, BDLF+16, PE16, HSR+17}, almost equivalent to formally verifying assembly code. Only very high-level languages should be used to write smart contracts, not assembly-like ones (EVM); even the C language should be considered too low-level for these purposes because the required proofs must contain all kind of details about memory management and pointers.

Not all smart contracts need to be formally verified, and not even every part of their code should be. On permissioned blockchains, non-verified smart contracts will be much more accepted than on public permissionless blockchains.

Unlike other works that only consider the correctness of the computed output and resort to resource-consuming zero-knowledge proofs \cite{BCG+14}, the mathematical proofs considered here are multi-purpose: invariants, pre- and post-conditions, termination, correctness, security, resource consumption, legal/regulatory (e.g., self-enforcement), economic (e.g., fairness, double-entry consistency, equity), functional and any other desirable property that can be mathematically expressed.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{proof-carrying-code-infrastructure.png}
\caption{Proof-Carrying Code infrastructure}
\end{figure}

The solution of how to execute untrusted code from potentially malicious sources is not new, said problem was already considered for mobile code: Proof-Carrying Code \cite{NL98b} prescribes accompanying the untrusted code with proofs (certifiable certificates) that can be checked before execution to verify their validity and compare the conclusions of the proofs to the security policy of the code consumer to determine whether the untrusted code is safe to execute. On
the positive side, no trust is required on the code producer and there is no runtime overhead during execution, but the code must be annotated (e.g., see pseudo-code annotation of the Program Listing below) and detailed proofs generated, a process which can be complex and costly. A novel variant combining PCC with Non-Interactive Zero-Knowledge proofs is proposed in the next sub-section 5.3.

Algorithm 3 Example pseudo-code with annotations

```
class Account {
    int balance; // invariant balance >= 0;
    // requires amt >= 0
    // ensures balance == amount
    Account(int amount) { balance = amount; }

    // ensures balance == acc.balance
    Account(Account _account) { balance = _account.balance(); }

    // requires amount > 0 && amount <= _account.balance()
    // ensures balance == \old(balance) + amount
    // && _account.balance == \old(_account.balance - amount);
    transfer(int amount, Account _account) {
        _account.withdraw(amount);
        deposit(amount);
    }

    // requires amount > 0 && amount <= balance
    // ensures balance == \old(balance) - amount
    void withdraw(int amount) { balance -= amount; }

    // requires amount > 0;
    // ensures balance == \old(balance) + amount
    void deposit(int amount) { balance += amount; }

    // ensures \result == balance
    int balance() { return balance; }
}
```

The verification of a program typically requires many annotations, at least a 1:1 ratio of lines of code against specifications: tools have been developed to automatically generate said annotations and are very useful in this setting. In case of using an interactive theorem prover, an extensive library of tactics must help to handle complex cases. Smart contracts must be written with the specific purpose of verification in mind, otherwise it becomes extremely complex to generate complete proofs\cite{WSC07}; regarding the size, effort and duration of the verification process, there is a strong linear relationship between effort and proof size\cite{SJA14} and a quadratic relationship between the size of the formal statement and the final size of its formal proof\cite{MMA15}.

The most cost-effective option in some settings (e.g., permissioned blockchains)
could be the publication of the annotated smart contracts to the blockchain and not using some of the more advanced options like the PCC toolchain or any kind of theorem prover, reversing the burden of proof to code consumers but in some sense helping them with the provided annotations. Therefore, there is a scale of Verification Levels when publishing smart contracts on blockchains:

1. Annotated smart contracts
2. Annotated smart contracts automatically tested using heuristics/concolic execution
3. Annotated smart contracts with full/partial proofs
4. Annotated smart contracts with certifiable certificates (Proof Carrying Code)

Ultimately, as an example of their applicability, the use of the proposed annotated smart contracts in combination with the zero-knowledge proofs of section §5.3 allows for an alternative way to implement the proofs of assets, liabilities and solvency of exchanges of [DBB +15].

5.1 Case Study

Algorithm 4

```java
class Crowdfunding {
    int minimum = 1000;
    // requires 0 < n
    // ensures \result >= minimum
    public int crowdfund(int n, int[] inputs) {
        int sum = 0;
        // invariant 0 <= i && i <= n
        for (int i = 0; i < n; i++) {
            sum += inputs[i];
        }
        return sum;
    }
}
```

Proofs are written in Coq: the following execution statistics of the PCC toolchain are reported,

- Proof-generation time overhead: directly correlated to the size of the compiled program being analysed. It follows approximately the following formula on a modern laptop (Intel® Core™ i7-7500U 2.7Ghz):

\[
\text{time} = 1.5 + \left( \frac{bs}{1500} \right) \text{secs}
\]
• Proof-verification time overhead: (less) correlated to the size of the compiled program being analysed. It follows approximately the following formula on a modern laptop (Intel® Core™ i7-7500U 2.7Ghz):

\[
time(\text{bytecode size } bs) = 0.25 + \left( \frac{bs}{6000} \right) \text{ secs}
\]

• Certificate size overhead: 30%

![Spreadsheet Screenshot]

Figure 5.2: Secure spreadsheet[Cal17] enabled for privacy-preserving computation displaying the result of private and verifiable smart contracts (e.g., cryptographically secure financial instruments and their derivatives)

Not much thought has been given to the rather practical question of what user interface should smart contracts use: calculations will be done on the returned values of smart contracts, even encrypted ones; and nested calculations on their inputs/outputs is also required. A spreadsheet enabled for secure computation fits all the given requirements, especially given that it’s well accepted on the financial industry and many are trained on its use.

5.2 On the Size of Certifiable Certificates

Since the invention of Proof Carrying Code[Nec97], the question of how to efficiently represent and validate proofs[NL98a] has been a focus of much research. Different techniques are considered in this work to reduce the size of certificates:
1. The reflection technique\textsuperscript{ACHA90}. This technique decreases the size of the proof using the reduction offered by a proof assistant: multiple explicit rewriting steps are replaced by implicit reductions. In other words, implicit computation replaces explicit deduction, achieving a reduction of proof size of orders of magnitude.

2. Deep embedding of the verification condition generator reduces the size of proof terms due to the use of reflective tactics with the subsequent reduction in the time needed to check the proofs.

3. Using hybrid methods that include static analysis: using the information provided by type systems to eliminate unreachable paths reduces the number of proof obligations. For example, null-pointer analysis is used to prove that most accesses are safe and this information is then employed to reduce the number of proof obligations.

4. Partitioning the certificate to reduce the memory required to check it by running an interactive protocol between the code consumer and producer.

5. Abstract interpretation is used to verify safety policies that reduce the control flow graph. A fixed-point abstract model accompanies the code whose validity implies compliance with safety policies: then, the code consumer checks its validity in a single pass. Note that there’s an inherent tradeoff between certificate size and checking time: in order to reduce the size of the certificate, the code consumer could generate the fixpoint but that would also increase the checking time. Thus, it’s important to send the smallest subset of the abstract model while maintaining an efficient single-pass check: that is, to only store the information that the code consumer is not able to reproduce by itself.

6. The size of certificates using proofs in sequent calculus is reduced since it can be reconstructed from the used lemmas (i.e., using the cut-inference rule). Proofs are represented in tables that a proof engine will check\textsuperscript{LM07}: in order to reduce the size of the table, some atomic formulas can be omitted if the code consumer will be able to easily reprove them.

Other approaches that could be considered in order to reduce the size of the proof include transmitting a proof generator\textsuperscript{PDH10} to the code consumer instead of the proof itself, and executing the proof generator on the consumer side to re-generate the proof using a virtual machine.

5.3 Zero-Knowledge Proofs of Proofs

Although it’s possible to obfuscate certifiable certificates in such a way that de-obfuscation wouldn’t be any easier\textsuperscript{Dup08} while keeping the certifiable certificate sound and complete, this level of security isn’t acceptable in a formal cryptographic model. When smart contracts are fully encrypted with homomorphic encryption/IO, certifiable certificates reveal too much information about the
code and additional cryptographic protection is absolutely necessary: it’s possible to generate zero-knowledge proofs of proofs [Blu87] (or certifiable certificates, which are shorter), in such a way that the code producer can convince the code consumer of the existence and validity of proofs about the code without revealing any actual information about the proofs themselves or the code of the smart contract.

Classically, this would require to come by an interactive proof system [GMR85] were the code consumer is convinced, with overwhelming probability, of the existence and validity of proofs of the code through interaction with a code producer; then, a zero-knowledge proof system will be obtained using the methods of [ROGG+90] [LY88]; for a more detailed description on how to prove a theorem in zero-knowledge, see [Pop94]. Lately, advances in verifiable computation have produced advanced zero-knowledge proof systems to prove correctness of remote execution; although many of these results could theoretically be extended to prove general assertions about the code, the slowdowns for proving would be higher than the current $10^5 - 10^7$ for the very optimized case of proving correctness of executions [WB15].

Until the advent of methods to obtain zero-knowledge proofs from garbled circuits [JKO13] (i.e., general purpose ZK), zero-knowledge proofs have been difficult to come by. ZKBoo [GMO16], a later development of [JKO13], creates non-interactive zero-knowledge proofs for boolean circuits: this line of work is the preferred choice to obtain NIZK-proofs of the validity of certifiable certificates of smart contracts, because zk-SNARKs [BCCT12] would be very succinct, but with setup assumptions and much slower to proof (e.g., the circuit $C_{FOUR}$ from Zerocash [BCG+14] has 4,109,330 gates and a reported execution time of 2 min). Lately, ZKB++ [CDG+17] provides proofs that are less than half the size than ZKBoo and Ligero [AHIV17] four time shorter than ZKB++.

Using ZKBoo, the statement to be proved would be “I know a certifiable certificate such that $\phi(certificate) = true$” for a certificate validation circuit $\phi$ and $L_0$, the language $\{true \mid \exists certificate.s.t. \phi(certificate) = true\}$ with soundness error $2^{-80}$; minimizing the certificate validation circuit $\phi$ as much as possible would be the most important optimization.

**Proof-Carrying Data** A conceptually related technique to Proof-Carrying Code is Proof-Carrying Data [CT10]: in a distributed computation setting, PCD allows messages to be accompanied by proofs that said messages and the history leading to them follow a compliance predicate, in such a way that verifiers can be convinced that the compliance predicate held throughout the computation, even in the presence of malicious parties. PCC and PCD are complimentary since PCD can enforce properties expressed via PCC: interestingly, PCD could enable zero-knowledge privacy for PCC [CTV13], but at a greater efficiency cost.
6 Functionalities and Protocols

6.1 General Overview

Figure 6.1: General overview of the functionalities (top) and realised protocols (bottom) described in this paper

6.2 Detailed Description

In this section we present our secure protocol for private and verifiable smart contracts, specified in the Functionality below:

**Functionality 6.1: Private and Verifiable Smart Contracts**

- **Parties:** $E_1, ..., E_N$, set of nodes $N_i$ of a blockchain $B$
- **Inputs:** smart contract $SC$, private inputs from parties $E_1 : \overrightarrow{x}, E_2 : \overrightarrow{y}, ..., E_N : \overrightarrow{z}$
- **The functionality:**
  1. Parties $E_1, ..., E_N$ verify the smart contract $SC$
  2. Parties $E_1, ..., E_N$ securely execute the smart contract $SC$ on nodes $N_i$
- **Outputs:** results from the secure computation $E_1 : \overrightarrow{r_1}, E_2 : \overrightarrow{r_2}, ..., E_N : \overrightarrow{r_N}$.

Our protocols for realising Functionality 6.1 consists of a standard verification functionality and a secure computation functionality (Functionality 4.1):
Functionality 6.2: Standard verification of smart contracts

- **Parties:** $E_1, ..., E_N$
- **Inputs:** smart contract $SC$
- **The functionality:**

1. Parties $E_1, ..., E_N$ obtain the annotations/proofs/certificates of smart contract $SC$
2. Verify the annotations, proofs and/or certificates available on the smart contract $SC$
3. Check if the verified annotations, proofs and/or certificates are sufficient for the smart contract $SC$ to be declared correct, according to the local policies of each party

- **Output:** true if the verification was correct, false otherwise.

To implement Functionality 6.2 (Standard verification of smart contracts), the following protocol is used:

Protocol 6.3: Realising Functionality 6.2 (Standard verification of smart contracts)

- **Parties:** $E_1, ..., E_N$
- **Inputs:** smart contract $SC$
- **The protocol:**

1. Parties $E_1, ..., E_N$ download the annotations/proofs/certificates of smart contract $SC$ and check their digital signatures.
   
   (a) If annotated smart contracts do not contain any kind of proofs or certificates, the annotations of the smart contract are automatically tested using an heuristic/concolic execution engine.
   
   (b) If annotated smart contracts contain full/partial proofs, they are locally regenerated and compared to the embedded ones.
   
   (c) If annotated smart contracts contain certifiable certificates, said certificates are checked.

2. This step could be computationally expensive, so it only needs to be done the first time if the smart contract $SC$ is not modified.

3. Check if the verified annotations, proofs and/or certificates are sufficient for the smart contract $SC$ to be declared correct, according to the local policies of each party

- **Output:** true if the verification was correct, false otherwise.
The previous protocols are combined in the following general execution protocol for private and verifiable smart contracts:

<table>
<thead>
<tr>
<th>Protocol 6.4: Realising Functionality 6.1 (Private and Verifiable Smart Contracts)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parties:</strong> $E_1, E_2, \ldots, E_N$, set of nodes $N_i$ of a blockchain $B$</td>
</tr>
<tr>
<td><strong>Inputs:</strong> smart contract $SC$, private inputs from parties $E_1 : \overrightarrow{x}, E_2 : \overrightarrow{y}, \ldots, E_N : \overrightarrow{z}$</td>
</tr>
<tr>
<td><strong>The protocol:</strong></td>
</tr>
<tr>
<td>1. The parties invoke Functionality 6.2 (Standard verification of smart contracts), implemented using Protocol 6.3, and obtain the verification status of the smart contract $SC$.</td>
</tr>
<tr>
<td>2. The parties invoke Functionality 4.1 (Secure computation of smart contracts), implemented using Protocol 4.2 where party $E_1$ inputs $\overrightarrow{x}$, party $E_2$ inputs $\overrightarrow{y}$ and the rest of parties $E_N$ their corresponding inputs. Parties receive results $E_1 : \overrightarrow{r_1}, E_2 : \overrightarrow{r_2}$ and the rest of parties their corresponding outputs $E_N : \overrightarrow{r_N}$.</td>
</tr>
<tr>
<td><strong>Outputs:</strong> results from the secure computation $E_1 : \overrightarrow{r_1}, E_2 : \overrightarrow{r_2}, \ldots, E_N : \overrightarrow{r_N}$.</td>
</tr>
</tbody>
</table>

### 6.3 Security Analysis

The security analysis follows the standard definition of static semi-honest security in the standalone setting [Gol04] and assumes semi-honest security of basic building blocks: Yao’s protocol [LP04] and oblivious transfer accelerated with OT-extension [ALSZ13, IKNP03], implying the security for the Protocol 4.2 realising Functionality 4.1. Additionally, ORAMs [Gol87] could also be used to speed up dynamic memory accesses: also note that when the number of parties is huge, communication locality plays a central role and may be better achieved with ORAMs [BCP14, LO15]. The following theorem proves the general protocol 6.3:

**Theorem 2.** (General Protocol). Protocol 6.4 realises Functionality 6.1 against static corruptions in the semi-honest security model augmented with verifiability of the code.

**Proof.** Correctness and privacy of Protocol 4.2 (1.b) follows from Yao’s protocol [LP04] and oblivious transfer accelerated with OT-extension [ALSZ13, IKNP03]; in case of a multi-party setting, correctness and privacy follows from one of the multi-party protocols (GMW [GMW87], BMR [BMR90], BGW [BGW88, AL11]); when using ORAMs, the security proof comes from the specific security proof of the chosen ORAM scheme (Circuit ORAM [WCS14]; Square-Root ORAM [ZWR+16, GO96]); when using TLS, we make use of the composability of the security.
proofs of said protocols \cite{GMP+08,KMO+14,BFK+14}. Regarding verifiability, it follows from Protocol 6.3 realising Functionality 6.2.

### 6.4 Extended verification of smart contracts

Trusted third parties (e.g., governments, central banks, regulating bodies) may provide specifications against which proofs must be generated. Thus, Gyges attacks \cite{JKS16} can be prevented if parties and executing nodes require that all the executed smart contracts must adhere to said specifications and be digitally signed by trusted third parties: that is, prevent them from malicious hackers and others engaged in unlawful business practices while being compliant with certain regulations and laws (e.g., anti-money laundering laws). Comparing the next two diagrams provides a better understanding of the introduced differences:

![Diagram](image)

**Figure 6.2:** Standard verification of smart contracts
To formalize this concept, the following Functionality 6.5 is introduced:

**Functionality 6.5: Extended verification of smart contracts**

- **Parties:** $E_1, E_2, \ldots, E_N$, trusted third parties $T_i$
- **Inputs:** smart contract $SC$
- **The functionality:**

1. Parties $E_1, E_2, \ldots, E_N$ obtain the annotations/proofs/certificates of smart contract $SC$
2. Check digital signatures from trusted third parties $T_i$ and verify conformance to their specifications: verify annotations, proofs and/or certificates available on the smart contract $SC$
3. Check if the verified annotations, proofs and/or certificates are sufficient for the smart contract $SC$ to be declared correct, according to the local policies of each party

- **Output:** true if the verification was correct, false otherwise.

The following Protocol 6.6 implements Functionality 6.5:
Protocol 6.6: Realising Functionality 6.5 (Extended verification of smart contracts)

- **Parties:** $E_1, E_2, \ldots, E_N$, trusted third parties $T_i$
- **Inputs:** smart contract $SC$
- **The protocol:**
  
  1. Parties $E_1, E_2, \ldots, E_N$ download the annotations/proofs/certificates of smart contract $SC$ and check their digital signatures. Digital signatures from trusted third parties $T_i$ are checked and conformance to specifications from said third parties $T_i$ is tested: every party $E_i$ has a security profile that specifies the mandatory/optional trusted signing parties and specifications that every smart contract must adhere to.

     (a) If annotated smart contracts do not contain any kind of proofs or certificates, the annotations of the smart contract are automatically tested using an heuristic/concolic execution engine. At least, it should be digitally signed by a trusted third party.

     (b) If annotated smart contracts contain full/partial proofs, they are locally regenerated and compared to the embedded ones. Some of said proofs must conform to specifications from third parties.

     (c) If annotated smart contracts contain certifiable certificates, said certificates are checked. Some of said certifiable certificates must conform to specifications from third parties.

  2. This step could be computationally expensive, so it only needs to be done the first time if the smart contract $SC$ is not modified.

  3. Check if the verified annotations, proofs and/or certificates are sufficient for the smart contract $SC$ to be declared correct, according to the local policies of each party.

- **Output:** $true$ if the verification was correct, $false$ otherwise.

Finally, the general Protocol 6.4 is reviewed with the new Protocol 6.6 for the extended verification of smart contracts:
Protocol 6.7: Realising Functionality 6.1 (Private and Extended Verifiable Smart Contracts)

- **Parties**: $E_1, E_2, ..., E_N$, set of nodes $N_i$ of a blockchain $B$, trusted third parties $T_i$
- **Inputs**: smart contract $SC$, private inputs from parties $E_1 : x, E_2 : y, ..., E_N : z$
- **The protocol**:
  1. The parties invoke Functionality 6.5 (Extended verification of smart contracts), implemented using Protocol 6.6, and obtain the extended verification status of the smart contract $SC$.
  2. The parties invoke Functionality 4.1 (Secure computation of smart contracts), implemented using Protocol 4.2 where party $E_1$ inputs $x$, party $E_2$ inputs $y$ and the rest of parties $E_N$ their corresponding inputs. Parties receive results $E_1 : r_1, E_2 : r_2, ..., E_N : r_N$.
- **Outputs**: results from the secure computation $E_1 : r_1, E_2 : r_2, ..., E_N : r_N$.

The following theorem finally proves the extended general protocol 6.7:

**Theorem 3.** *(Extended General Protocol)*. Protocol 6.7 realises Functionality 6.1 against static corruptions in the semi-honest security model augmented with extended verifiability of the code.

**Proof.** Correctness and privacy of Protocol 4.2 (1.b) follows from Yao’s protocol [LP04] and oblivious transfer accelerated with OT-extension [ALSZ13, IKNP03]; in case of a multi-party setting, correctness and privacy follows from one of the multi-party protocols (GMW [GMW87], BMR [BMR90], BGW [BGW88, AL11]); when using ORAMs, the security proof comes from the specific security proof of the chosen ORAM scheme (Circuit ORAM [WCST14], Square-Root ORAM [ZWR+16, GO96]); when using TLS, we make use of the composability of the security proofs of said protocols [GMP+08, KMO+14, BFK+14]. Regarding verifiability against Gyges attacks [JKS16], it follows from Protocol 6.6 realising Functionality 6.5.

6.5 Malicious security

Smart contracts are compiled to efficient Boolean circuits that could be executed on multiple secure computation frameworks with the added benefit of obtaining malicious security [WMK16b, WRK17, KRW17, WMK16a, HSSV17]: protocols and theorems above can trivially be updated with their security definitions and proofs. In case of using ORAMs, security against malicious adversaries comes from specialized versions of said protocols [AHMR14, Min10, HY16].

32
6.6 Private Function Evaluation

In this setting, the smart contract itself is kept secret: that is, only one of the parties knows the function $f(x)$ computed by the smart contract, whereas other parties provide the input to the private function without learning about $f$ besides the size of the circuit defining the function and the number of inputs and outputs. Private function evaluation can be implemented using secure function evaluation\[AF90, KS08\] by securely evaluating a Universal Circuit\[Val76\] that is programmed by the party knowing the function $f(x)$ to evaluate it on the other parties’ inputs: the security follows from that of the secure function evaluation protocol that is used to evaluate the Universal Circuit.

Recently, Valiant’s Universal Circuit has been implemented and proven practical\[KS16, GKS17\]; its optimal size was proven to be $\Omega(k \log k)$\[Val76\] and its recent implementation further improved it by (at least) $2k$. Although it’s a considerable blowup in size, late MPC protocols provide very efficient pre-processing phases that could ameliorate execution times: online times are only 1-4% of the total execution time in the WAN setting\[KRW17, WMK16a, BELO16\], and 2-5% in the LAN setting\[HSSV17, BEO17\]. Since the generated universal circuit description $UC_{u,v,k^*}$ is public to all parties\[KS16, GKS17\], both function-dependent and function-independent pre-processing\[KRW17, WMK16a, BELO16, HSSV17, BELO17, BEO17\] could be used in the setting of private function evaluation for maximum speedup.

7 Economic Impact and Legal Analysis

Previous legal analysis\[Dam16\] has considered how secure computation fits current legal frameworks, although it’s much more interesting to evaluate how it could alter legal frameworks and its economic impact.

7.1 Data Privacy as Quasi-Property

Quasi-property interests\[Alg12\] refer to situations in which the law seeks to simulate the functioning of property’s exclusionary apparatus, through a relational entitlement mechanism, by focusing on the nature and circumstances of the interaction in question, which is thought to merit a highly circumscribed form of exclusion. The term first appeared in a SCOTUS decision in International News Service v. Associated Press\[SCO18\], in which Justice Pitney recognized the right of an information gatherer to prevent a competitor from free riding on the original gatherer’s labor for a limited period of time: more specifically, it’s limited in that it would only ever exist between the two parties in question and never in the abstract against the world at large.

Quasi-property allows to effectively treat data privacy as a property right\[Sch12\] and it’s the closest analogue in American law that grants individuals a property right in their personal data, as privacy has always been considered in the privacy-preserving literature in cryptography: in fact, the quasi-property view of privacy-preserving computation has stronger grounding than European database...
rights[RS97]. This approach provides a common framework that underlies all of the privacy torts, while avoiding the need to define privacy in such a way that it describes every injury that the law recognizes as an invasion of privacy and that can be generally categorized in four harms: (1) information collection; (2) information processing; (3) information dissemination, and (4) invasion.

7.2 A Solution to Arrow’s Paradox

Arrow’s Paradox[Arr62] states that “there is a fundamental paradox in the determination of demand for information; its value for the purchaser is not known until he knows the information, but then he has in effect acquired it without cost”. Ex-ante, the purchaser cannot value the original information since it can only be known after it has been revealed; ex-post, the purchaser could not compensate the seller and disseminate it for free. Due to the inherent properties of information (non-excludable, non-rivalrous), markets for information cannot exist in the absence of intellectual property rights[GS03] because the original producer/inventor of any information loses the monopoly on it after the information is revealed; regarding financial information, the finance literature generally agrees in that the troubles in informational trading explain financial intermediation[LP77, RT84, All90, AP90].

Secure computation techniques offer a practical solution to Arrow’s Paradox: distrustful third-parties can compute on private information without disclosing it, allowing its valuation while preventing intellectual property theft; this is significantly better than previously known methods based on partial the revelation of information[AY94, AY02, AY05]. More generally, secure computation techniques make information excludable while maintaining its non-rivalrousness: that is, the original producer/inventor of the information retains market power over it while maintaining its costless resale (i.e., the marginal cost of an additional digital copy is zero), theoretically allowing for digital goods of infinite value that bypass Coase conjecture[Coa72] since it’s also possible to prevent that first time purchasers resell the information they have queried/acquired[Mut90, NQ91], although in practice having to account for the costs of the slowdown introduced by secure computation techniques.

7.3 Expansion of Trade Secrecy

While software copyright and patentability protection have been weakened, trade secrecy stands firm. As defined in the United States’ Uniform Trade Secrets Act[Com85]: “Trade secret means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy”. The definition on the European Union’s Trade Secrets Directive[Com85] implicitly
includes computer programs, financial innovations, lists of customers, business statistics and many other types of secret information.

There is no definitional uncertainty in trade secret law: unlike copyright, there is no exclusion for functionality; unlike patents, there is no exclusion for abstract ideas. There isn’t any uncertainty about the exact contours of their extension either, such as in the debate of the mutual exclusivity of copyright and patents protections. In some cases, widely distributed software may remain a trade secret if the license agreement requires confidentiality and return upon non-use (see Data Gen. Corp. v. Grumman Systems Support Corp.).

Although software might be reverse engineered (i.e., an acceptable way to discover a trade secret that prevents its general use for protecting software), secure computation techniques effectively hinder and/or completely forbid reverse engineering. Trade secrets can be justified as a form, not of traditional property, but of intellectual property in which secrecy is central and may serve the purposes of IP law better than more traditional IP rights. Stronger trade secrecy law increases R&D in high technology industries: similar effects are expected from the utilisation of the technologies described in the present publication.

### 7.4 Verifiability and Self-Enforcement

The term *Lex Cryptographia* designates a new body/subset of law, containing rules administered through smart contracts and decentralized autonomous organizations: this concept is inspired on *Lex Mercatoria*, an old subset of customs that became recognized as a customary body of law for international commerce. Smart contracts are just software programs with very specialized functionalities intended to replace paper contracts: the practice of law could thus follow the path of software, with smart contract programming languages becoming more powerful and easier to develop, transforming the legal profession with more technical lawyers. By design, smart contract cannot be breached: once contracting parties have agreed to be bound by a particular clause, the code’s immutability binds them to that clause without leaving them the possibility of a breach; that is, the code defines its own interpretation and enforces the defined rules contained on it without the need of third parties (i.e., self-enforcement). The only way to escape from contractual obligations that the parties no longer want to honor is by including legal provisions into smart contract’s code. Over time, law and code may converge, so that infringing the law will be effectively breaking the code: that is, *Lex Cryptographia* is stronger than *Lex Posita* and will become more prevalent.

The strictness of self-enforcement has been much criticized: it could be misused and turned against the contracting parties and it doesn’t represent the realities of real-world enforcement of contracts. Adding verifiability to smart contracts as proposed in this work prevents all these problems as it allows to check conformity to the specifications from third parties (e.g., governments, regulating bodies, standards). In sum, contracting parties are
private lawmakers\cite{Sur12} in control of both the substance and the form of their contractual obligations (i.e., \textit{pacta sunt servanda}), but third parties could intervene to regulate said private agreements by redacting specifications that smart contracts must formally verify against.

7.5 Markets for Smart Contracts

Paradoxically, smart contracts are hardly bought/sold: the inexistence of strong property rights hampers the development of markets on smart contracts; actually, not even companies developing and operating them are being acquired/merged based on the value of their smart contracts since they can easily be reverse engineered and cloned.

Private smart contracts provide strong property rights based on cryptographic techniques which allow for the emergence of markets to trade them. Depending on the cryptographic techniques employed, the following advantageous situations could be considered:

1. The algorithms contained within smart contracts could be traded without disclosing their details when using private function evaluation, homomorphic encryption and/or indistinguishability obfuscation.

2. More practically, when using garbled circuits or secret sharing techniques the source of value will reside on encrypted data processed by the algorithms of private smart contracts, these cryptographic techniques being much more efficient than homomorphic encryption/IO; said encrypted data could be stored on the blockchain, easing the transfer of property of the smart contract.

Traditionally, binary compilation and obfuscation have been used to safeguard the value of software: secure computation techniques offer a provably-secure way to protect the value of even purely open-source software. Furthermore, the ability to safely trade private smart contracts will justify their higher development costs.

7.6 Effects on Currency Competition

Latest analysis on the monetary policy of cryptocurrencies\cite{FVS17} provide insights on the effects of currency competition:

- Monetary equilibrium between private cryptocurrencies will not deliver price stability: profit-maximizing entrepreneurs issuing cryptocurrencies do not have real incentives to provide stable currencies, only to maximise their seigniorage.

- Monetary systems consisting of only private cryptocurrencies in the equilibrium with stable prices do not provide the socially optimum quantity of money: competition between cryptocurrencies is not enough to provide optimal outcomes since entrepreneurs do not internalise the pecuniary externalities by minting additional tokens.
• Unlike private money, government money has fiscal backing because it can tax agents in the economy. But in competition with people willing to hold cryptocurrencies, the implementation of monetary policy in deflationary settings will be significantly impaired since profit-maximizing entrepreneurs will be unwilling to retire their private currencies and instead choose to increase their issued money.

• Government money could co-exist without intervention in a unique equilibrium with cryptocurrencies if the minted cryptocurrency growths following a predetermined algorithm (e.g., Bitcoin) and the proceedings are used to buy/finance sufficiently productive capital.

Additionally, social efficiency may also be achieved with different cryptocurrencies featuring diverse functionalities that provide market power to their issuers and users: particularly, this is the case of the private and verifiable smart contracts of this paper, since they could be used to provide natural monopolies on the encrypted programs stored on them.

7.7 Token vs. Account-based Cryptocurrencies

Most cryptocurrencies are based on the model of issuing and transacting tokens, using some form of distributed ledger to keep track of the ownership of said tokens (e.g., Bitcoin, Ethereum and Zcash): they’re the digital equivalents of cash.

Another unexplored model of cryptocurrency is that of holding funds in accounts at the central bank or in depository institutions, resembling debit cards: in fact, users of Digital Currency Exchanges maintain accounts holding substantial amounts of wealth, but in the form of token-based cryptocurrencies. There are many efficiency gains to be expected from account-based cryptocurrencies: latest macroeconomic models show that they would permanently raise GDP by as much a 3% in the USA due to lower bank funding costs, lower monetary transaction costs and lower distortionary taxes; additionally, they would introduce new tools for the central bank to stabilise the business cycle.

The technology required to implement account-based cryptocurrencies is different and more complex than the required for token-based cryptocurrencies: the smart contracts proposed in this paper are a perfect fit for this task, due to their ability to maintain privacy and guarantee their perfect functionality through formal verification techniques.

7.8 Impact on Market Structures

Although disintermediation will be one of the first consequences of the application of cryptographic smart contracts to financial markets, as happened in the past with the introduction of the Internet, bank and fund concentrations may also increase: information asymmetry is associated with more concentration and information production and its hiding is a valuable activity of banks, that is, opacity has value in itself. Ceteris paribus,
it’s difficult to estimate the resulting equilibria of the impact of this technology on the level of concentration in the financial industry, given the high number of inter-related variables; nonetheless it’s easier to predict that practices like shadow banking [PAAB13] will increase, as new financial technology accounts for 35% of their growth [BMPST17].

8 Related work

A number of related works using cryptographic techniques are as follows:

- Enigma [ZNPI15, Zys16] is coded in Python, a language lacking verification libraries/toolkits and formal semantics so it can’t be used for proof-carrying code; its cryptographic protocols are not constant-round, thus settings with some latency will be it excruciatingly slow (i.e., Internet); finally, the only supported distributed ledger is Bitcoin. Later developments show that Enigma is pivoting to a decentralized data marketplace using deterministic and order-preserving encryption [Pro17].

- WYS* [Ras16] offers an elegant solution for verifiable and secure multi-party computation based on the dependently typed feature of the F* language. Unfortunately, the use of said research language also compromises its real-world adoption; additionally, it’s not integrated on any blockchain and does not offer proof-carrying code. Another similar work [ABB+14] uses EasyCrypt to verify Yao’s garbled circuits.

- Hawk [KMS+15] focuses on protecting the privacy of transactions using zk-SNARKs: later works like [Solidus CZJ+17, Confidential Transactions Gib16, Bolt GM16] provide secure transactions at the protocol level with more efficient techniques. It only mentions secure multi-party computation as a tentative way to replace the trusted auction manager, rejecting it as impractical.

- Chainspace [ABSB+17] is a sharded smart contract platform that includes some examples of private smart contracts based on the PETLib library using homomorphic encryption, and zero-knowledge proofs only after the execution of the smart contract.

- ZeroCash [BCG+14] and Monero [Noe15] provide security for transactions, not smart contracts. Note that secure transactions on blockchains are just a special restricted case of smart contracts enabled with cryptography, but not the other way around.

- Oyente [LCO+16], a symbolic execution tool to formally verify Ethereum smart contracts (EVM).

- Accountable algorithms [KHB+16] propose a commit-and-prove protocol with zk-SNARKs to provide accountability proofs of compliance to legal standards without revealing key attributes of computerized decisions after
said decisions have been taken, but not before their execution as is done in the present paper.

- Previous works on combining MPC with Bitcoin [ADMM13b, ADMM13a] use it as support to obtain fairness in MPC, and not better smart contracts.
- Previous projects [MEK+12, ABB+10] designed high-level languages for Zero-Knowledge Proofs of Knowledge but not for Zero-Knowledge Proofs of Proofs, and their languages were restricted and not general purpose.

9 Conclusions, subsequent and future work

The present paper has tackled and successfully solved the problem of improving the privacy, correctness and verifiability of smart contracts, resolving the DAO and Gyges attacks. Examples have been shown to demonstrate its practical viability.

9.1 Subsequent work

The ability to save the state of garbled circuits and restore them at later times is a major improvement, bringing them closer to secret sharing techniques:

- partial garbled circuits [MGBF14]: for each wire value, the generator sends two values to the evaluator, transforming the wire labels of the evaluator to another garbled circuit; depending on its point and permute bit, the value from a previous garbled circuit computation is mapped to a valid wire label in the next computation.
- reactive garbled circuits [NR15]: a generalization of garbled circuits which allows for partial evaluation and dynamic input selection based on partial outputs.
- reusable garbled circuits [GKP+12, Agr16] allow for token-based obfuscation where the code producer provides tokens to code consumers representing rights to execute garbled smart contracts: later constructions [Wan17] improve their concrete efficiency.

Raziel is ongoing development and subject to improvements.

9.2 Future work

Some encrypted smart contracts will be perpetual (e.g., consols): if they ever store any kind of encrypted secure computation (e.g., secret shares, garbled circuits, homomorphic encryptions, IO) eventually there will be the need to update their encrypted contents to upgrade their security level, a concept that has already been considered [LCL+13, ACJ16, GRY17].

MPC and SGX are not mutually exclusive and they will be used jointly to obtain better performance [BBB+16, GMF+16, PST16]. On the other hand,
it’s difficult to derive realistic threat models and abstractions \cite{BPSW16, PST16, SSL+17} that withstand the latest attacks against SGX \cite{BMD+17, SWG+17, MIE17, WKPK16, XCPT+15, SLKP17, LSG+16, BCLK17, Swa17, LIJ+17, Cor17, BWK+17, JLLK17, XLCZ17b, XLCZ17a, JVBS17}.

Acknowledgments

I would like to thank David Evans and Jonathan Katz for helpful comments on the paper.

References


\cite{AF90} Martín Abadi and Joan Feigenbaum. Secure Circuit Evaluation, 1990. \url{http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.43.1130&rep=rep1&type=pdf}


A Outsourcing Secure Computations for Cloud-based Blockchains

Theorem 4. (Outsourcing for Cloud-Based Blockchains). Assuming secure channels between the parties $E_1, E_2, \ldots, E_N$ and the nodes $N_i$ of the blockchain $B$, Protocol B.2 securely realises Functionality B.1 against static corruptions in the semi-honest security model with the garbling scheme satisfying privacy, obliviousness and correctness.

Proof. Two cases must be analyzed: corruption at the node $N_E$ executing the secure computation and corruption of the parties.

Corruption at node $N_E$. The simulator $\text{Simul}_{N_E} (1^\lambda, \text{result}_{N_E})$, where $\text{result}_{N_E}$ stores the $\text{KeyExchange}$, $\text{SendPrivateParameters}$ and $\text{SECCOMP}$ run by each party $E_1, E_2, \ldots, E_N$:

- $\text{KeyExchange} (E_i (1^\lambda), N_E)$: sample a public key $pk_i$ for party $E_i$.
- $\text{SendPrivateParameters} (E_i, N_E)$: sample a vector of random values $c_i = \left( X_{x_i[1]}^{m_1}, \ldots, X_{x_i[l]}^{m_l}, n_i \right)$.
- $\text{SECCOMP} (E_k, N_E) (SC)$: a simulated garbled circuit and garbled values are computed. Then, the simulator computes one entry of the pivot tables by encrypting random values and the other entry by encrypting each garbled value with the random values generated in the $\text{SendPrivateParameters}$ phase:
  - A simulator of garbled circuits generates a simulated garbled circuit $GC_{SC}$ and garbled values $w_{jl}$ for each party $E_j$ and index $l$ of the length of $x_j$.
  - Compute $\text{Enc}_{s_{jl}} (0)$ with random key $s_{jl}$ and $\text{Enc}_{X_{x_{jl}[l]}^{m_j}} (w_{jl})$ and save them into pivot table $P_q [j, l]$ in random order.
  - Return the pivot tables $P_q$ for each $E_j$, the garbled circuit $GC_{SC}$ and values $w_{jl}$.

54
We prove using hybrid arguments that the view generated by $\text{Simul}_{N_E}$ is indistinguishable from the view obtained by $N_E$ in the real world:

$H_0$. The real world view is computed using the real inputs of the parties and according to the original protocol.

$H_1^i$. What is different between $H_1^i$ and $H_1^{i+1}$ is that for each $E_i$ in $H_1^i$ the inputs are encoded using random values: that is, $X_{il}^i = \text{rand}_{il}$. It would be possible to obtain a distinguisher for the pseudorandomness of PRF assuming a distinguisher between $H_1^i$ and $H_1^{i+1}$. The values $X_{il}^i$ will be computed with an oracle by the reduction: the view will be distributed as in game $H_1^i$ if the oracle is using a random function; otherwise, it will be distributed as in game $H_1^{i+1}$ if the oracle is a pseudo-random function. Thus, a contradiction will be reached since any adversary distinguishing $H_1^i$ from $H_1^{i+1}$ with non-negligible probability will be able to break the pseudo-randomness with the same probability.

The sequence of hybrid games starts with $H_1^1$ where random values encode inputs of party $E_i$, to $H_n^n$ where random values from parties $E_1\ldots E_N$ encode inputs of the parties.

Finally, note that the hybrid $H_0 = H_0^0$ corresponds to the case where all inputs are pseudo-random values, while the last game $H_1^n$ corresponds to the case in which random values encode all inputs.

$H_2^{1,j,l}$. In this hybrid, the call $\text{SECCOMP}$ by party $E_i$ computes the pivot table $P_{q[j,l]} = \text{Enc}_{s_{j[l]}}(0), \text{Enc}_{s_{j[l]}}(w_{j[l]}^x)$, that is, only one garbled value per wire is encrypted: therefore, a contradiction will be reached since an adversary distinguishing between $H_2^{1,j,l}$ and $H_2^{1,j,l+1}$ with non-negligible probability can be reduced to a distinguisher for the indistinguishability under chosen-plaintext attacks (IND-CPA) of the encryption scheme.

The sequence of hybrid games starts with $H_2^{1,1,l}$ where the pivot table of party $E_i$ is encoded with only one garbled value per wire, to $H_2^{n,n,l}$ where all pivot tables of parties $E_1\ldots E_N$ are encoded with only one garbled value per wire.

$H_3^j$. The simulator $\text{Simul}_{N_E}$ computes the pivot tables and a simulator of garbled circuits is used instead of the real garbling scheme. It would be possible to obtain a distinguisher for garbled circuits assuming a distinguisher between $H_2^{n,n,l}$ and $H_3^j$: the inputs to the garbled circuits circuit will be computed by an oracle by the reduction as in $H_3^{n,n,l}$, to get garbled values and garbled circuits.

Finally, we reach the ideal world with hybrid $H_3^3$, finishing the proof that started with the real world game $H_0$.

**Corruption of the parties.** Assuming a single party $E_i$ is corrupted and secure channels between the parties and $N_E$, the simulator $\text{Simul}_{E_i}$ is defined as:

- $\text{KeyExchange}(E_i(1^\lambda), N_E)$: a public key $pk_i$ is chosen by party $U_i$. 

55
• *SendPrivateParameters* $(E_i, N_E)$: using the honest version for $\bar{x}_i^3$, honestly compute values $X^{\bar{x}_i^3} = \text{PRF}_{k^S}(\bar{x}_i, l, n_i)$.

• *SECCOMP* $(E_k, N_E) (SC)$: honestly compute garbled circuit and pivot tables. For the result, select the garbled values according to Functionality B.1 called with value $x_i$.

Note that the method to compute the result is the only difference in computing the view of $E_i$: while the evaluation of the garbled circuit is required in the real world, in the ideal world the correct resulting garbled values are chosen by the simulator $\text{Simul}_{E_i}$ using the result of Functionality B.1. Therefore, the indistinguishability of the view of $E_i$ is due to the secure channels: the case for more corrupted parties trivially follows from this argument.

\[\square\]