Off-Chaining Approaches for Cost-Efficiency in Threshold-Based Elliptic Curve Systems over Blockchains

Visakh K. Vijayan, Maria Francis and Kotaro Kataoka
Department of Computer Science and Engineering, Indian Institute of Technology, Hyderabad, India

Keywords: Off-Chaining, Threshold-Based Anonymous Credentials, Blockchains.

Abstract: In this work, we propose an off-chaining technique – ***t**hreshold **o**ff-chain **c**omputation* (TOC) – to reduce the gas cost of **t**hreshold-based **e**lliptic curve cryptographic systems over **b**lockchains (TEB), while preserving the security guarantees. We use threshold-based anonymous credentials with opening (TACO) and without opening (TAC) as examples and instantiate them with a PoC implementation of a blockchain-based credential management system. These implementations are built for both Ganache and Sepolia. Based on the evaluation results, we propose a) selective off-chaining where functions are off-chained using the TOC approach solely for gas cost reduction, and b) empirical push-back off-chaining where operations within the off-chained functions are pushed back on-chain for a balance between gas cost reduction and execution time. We observe that selective off-chaining of the TACO system results in a significant reduction of gas cost – 32x and 29x w.r.t. to the on-chain system in Ganache and Sepolia, respectively, but with a degradation in execution time. The empirical push-back off-chaining of the TACO system results in gas costs that are 6x and 4x lower than the original system in Ganache and Sepolia, respectively with an improvement in execution time of 59% in Ganache and 23% in Sepolia.

1 INTRODUCTION

The properties of decentralization, immutability, and availability of blockchains make them an ideal choice for implementing systems that assume the threshold trust assumption, i.e. where at least a threshold number of honest participants must cooperate to perform the operation. Threshold-based cryptographic systems with elliptic curve operations over blockchains (TEB) are blockchain systems where the cryptographic functionalities are achieved using elliptic curve operations that run on-chain and follow the threshold trust assumption. However, they have high gas costs[1] because elliptic curve operations are computationally intensive to run on blockchain smart contracts. The execution times and gas costs for a few anonymous credentials based on elliptic curve operations and use blockchains are given in Table 1.

Anonymous credentials are privacy-preserving mechanisms where the credentials are randomized every time the user presents it to a service provider, making the user unlinkable across multiple credential shows, and preserves the anonymity of the user even if the service provider and the credential issuer collude. They are built using bilinear pairings over elliptic curve groups. To avoid having to trust a single credential issuer, threshold-based anonymous credential schemes proposed over blockchains such as Coconut (Sonnino et al., 2019), DTRAC (Naaz et al., 2022) rely on multiple credential issuers who follow the threshold trust assumption to issue a credential. They are, therefore, examples of threshold-based systems with elliptic curve operations over blockchains (TEB) and we use them as a running example in this paper. They require computationally intensive elliptic curve operations and pairings-based operations primarily for the construction and verification of zero-knowledge proofs (ZKPs), cryptographic commitments, signature verifications, etc., all of which lead to high gas costs. Most works that use anonymous credentials either remain theoretical (Hébant and Pointcheval, 2022; Fuchsbauer et al., 2018; Connolly et al., 2022; Sanders, 2020; Camenisch et al., 2015) or are limited to local blockchains such as Ganache (Naaz et al., 2022; Sonnino et al., 2019; Rathee et al., 2022; Yu et al., 2019; Muth et al., 2023) and only a very few have mainnet simulations like Goerli and Ropsten testnets (Buccafurri et al., 2022). Recent anonymous credentials that are blockchain-based – zk-creds (Rosenberg et al., 2023) and ZEBRA

[1] Gas cost is the cryptocurrency required to perform an operation in the blockchain and varies with network congestion, fluctuating gas prices, type of transaction, transaction prioritization by the miners, etc.

Vijayan, V., Francis, M. and Kataoka, K.
Off-Chaining Approaches for Cost-Efficiency in Threshold-Based Elliptic Curve Systems over Blockchains.
DOI: 10.5220/0012361600003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 411-422
ISBN: 978-989-758-683-5; ISSN: 2184-4356

(Rathee et al., 2022) – reduce gas costs and execution time by using zk-SNARKs, and batched verifications but they assume a single trusted authority for credential issuance and do not support threshold issuance. Also, credential verification in both zk-creds and ZEBRA are on-chain, primarily to enable efficient credential revocation. Thus credential verification, a frequently performed operation, has a large gas cost.

Table 1: Gas costs and execution times of credential verification in different anonymous credential systems.

Anonymous credentials	Avg. gas cost (M: million)	Avg. time (s: seconds)
Coconut (Sonnino et al., 2019)	2.8 M	15s
DTRAC (Naaz et al., 2022)	1 M	6s
BASS (Yu et al., 2019)	1.5 M	85s
ZEBRA (Rathee et al., 2022) [1]	0.3 M	-
TSCVAC (Muth et al., 2023) [1]	32 M	-

A possible solution to improve cost efficiency is to move inefficient and expensive on-chain operations to an off-chain entity. Off-chaining is a widely studied method to improve the performance and reduce the costs of blockchain smart contracts (Eberhardt and Heiss, 2018; Liu et al., 2021; Eberhardt and Tai, 2017; Molina-Jimenez et al., 2018; Eberhardt and Tai, 2018; Kalodner et al., 2018). However, it can also lead to centralization of trust, introduce security vulnerabilities and scalability issues. To the best of our knowledge, there are no off-chaining works that concretely study threshold-based systems with elliptic curve operations over blockchains or anonymous credential systems or any other threshold-based cryptographic systems. In this work, we study off-chaining approaches specifically tailored for TEB systems by leveraging the threshold trust assumption. The following are the key contributions of this work.

1. We present a computation off-chaining solution, ***t**hreshold **o**ff-chain **c**omputation (TOC)* that uses the threshold trust assumption to ensure the same trust guarantees and computational correctness as the original on-chain system. It eliminates the need of introducing complex on-chain verifications for every off-chained computation as in (Rathee et al., 2022).
2. We use threshold anonymous credential systems over blockchains (TACO), as an instance of a TEB system, to implement the proposed off-chaining approach. From the evaluation of the off-chained system, we make a critical observation that is valid for any TEB system – despite significant improvement in gas costs, the execution time degrades. This happens when we off-chain pairings-based operations to nodes that are less powerful than the miner nodes. Pairings are resource-intensive elliptic curve operations that do not have many optimizations, both on-chain and off-chain. They are more in number – linear in the number of openers – in anonymous credentials that support opening of the credential. To reduce execution time, we push pairings-based operations back on-chain for just opening. We thus introduce two implementation approaches: 1) selective off-chaining, that off-chains all the on-chain elliptic curve operations and is ideal for threshold-based anonymous credentials that do not have opening (TAC), and 2) empirical push-back off-chaining for those that support opening (TACO), where the pairings-based operations are retained on-chain. We benchmark the system under multiple evaluation setups. The TAC system exhibits a gas cost reduction of 13x in Ganache and 11x in Sepolia after selective off-chaining. For a TACO system, threshold off-chain computation with selective off-chaining results in a gas cost reduction of 32x and 29x on Ganache and Sepolia respectively, but with a degradation in the execution time. The empirical push-back off-chaining of TACO results in a 6x and 4x lower gas cost than the original system in Ganache and Sepolia, respectively with improved execution times.
3. This work gives a comprehensive set of steps – the first of its kind – for off-chaining a TEB system using the TOC approach.

2 RELATED WORKS

Elliptic curve cryptography (Miller, 1986; Koblitz, 1987) is immensely popular because parameter values are typically shorter than other classical cryptographic primitives. Bilinear pairings using elliptic curves were first used in cryptography to build an identity-based encryption scheme (Boneh and Franklin, 2001), the first instantiation of such a scheme. Since then, pairings have been the go-to framework to build privacy preserving mechanisms such as anonymous credentials, group signatures, etc. Anonymous credentials (Chaum, 1985) were

[1] The systems do not provide execution time for credential verification.

first instantiated using CL-signatures (Camenisch and Lysyanskaya, 2001). Based on a general distributed ledger, (Garman et al., 2014) proposed the first decentralized anonymous credential, which did not require a trusted credential issuer. Coconut (Sonnino et al., 2019), the state-of-the-art threshold-based anonymous credential scheme, modifies PS-signatures (Pointcheval and Sanders, 2016), to enable a distributed set of credential issuers to issue partial credentials and requires at least a threshold number of partial credentials to construct a valid credential. DTRAC (Naaz et al., 2022) extends Coconut to include threshold opening where at least a threshold number of openers come together to open the credential and reveal the identity. Nevertheless, both Coconut and DTRAC are far from being practical primarily due to their high gas cost. ZEBRA (Rathee et al., 2022) provides accumulator-based revocable anonymous credentials over blockchains, and here, the credential verification happens on-chain. It maintains a list of revoked credentials in an on-chain accumulator and a non-membership ZKP is verified on-chain each time a credential is verified. Another recent work that is also accumulator-based is zk-creds (Rosenberg et al., 2023), where credential verification happens off-chain but the hash of the credential needs to be looked up on-chain. This is relatively a cheap operation in terms of gas cost but still will incur a few hundred to a few thousand gas units for every credential verification. In zk-creds, blockchains are used to store the list of issued credentials which is updated if any credential is revoked. So, when a service provider verifies a credential, it has to check if the credential belongs to the on-chain accumulator. Thus, to ensure revocation and accountability, ZEBRA and zk-creds use the blockchain for credential verification. In the off-chained DTRAC, since there is no revocation and only opening, the credential verification does not use blockchains and thus has zero gas cost.

Initial works studied off-chaining by focusing on applications (Eberhardt and Tai, 2017). For a good overview of various off-chaining approaches one can refer to (Eberhardt and Heiss, 2018) but these approaches do not analyze security and trust trade-offs. Research has focused on automatically generating FSM (Finite State Machine) and HSM (Hierarchical State Machine) models to decide which processes should go off-chain (Liu et al., 2021, 2022) but they are not applicable to smart contracts with cryptographic operations. Some works explores off-chaining as a solution to improve the security of smart contracts such as Cloak (Ren et al., 2022), which uses verifiable off-chaining multiparty computations, and Zokrates (Eberhardt and Tai, 2018), which uses verifiable computations, but they are not applicable to TEB systems as we show in Section 3.3.

3 PRELIMINARIES

3.1 Pairing-Based Operations

Elliptic curve cryptography (ECC) builds cryptographic primitives that exploit the algebraic structure of elliptic curves over finite fields. It provides the same level of security with shorter key lengths compared to classical primitives like RSA. However, they are computationally expensive for they do operations on large inputs with multiple iterations. These operations include elliptic curve point addition, point doubling, point negation, scalar multiplication and bilinear pairings. A bilinear pairing (Boneh et al., 2004) maps two elements g_1 and g_2, from two cyclic pairing-friendly elliptic curve groups $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, to a third element g_T from a subgroup $\mathbb{G}_T$ of a finite field. They are efficiently computable maps that satisfy the properties of bilinearity and non-degeneracy. They have enabled the construction of many cryptographic systems that, previously, had no feasible implementations such as identity-based encryption (Boneh and Franklin, 2001), anonymous credentials (Sonnino et al., 2019), attribute-based encryption (Goyal et al., 2006), etc. PS signatures (Pointcheval and Sanders, 2016) are short randomizable pairings-based signatures that allow for the signing of committed messages where the user can prove the knowledge of the signature efficiently, without revealing the message. They are randomizable, i.e. the user can generate fresh valid signatures from a given signature for the same message. This helps make the credential generated from a PS signature, unlinkable. Coconut (Sonnino et al., 2019) is a threshold-based anonymous credential system that uses a modified PS signature scheme to support threshold credential issuance, where a distributed set of issuers issues partial credentials and a threshold number of such credentials are required for the user to be able to generate a valid credential.

Bilinear pairings are computationally more intensive than other ECC operations. They require multiple elliptic curve point operations that need to combine points from different elliptic curve groups. In Ethereum, the Ethereum Virtual Machine (EVM) is stack-based which means that all the data must be first pushed onto the stack before it can be operated on. Pairings-based operations require a large number of intermediate values which leads to a significant growth in stack size, which, in turn, results in high gas costs. The elliptic curve operations that are not pairings-based require relatively less gas. However, they are generally more in number than pairings (refer Table 2) and thus collectively result in large gas costs. For ECC operations there are several optimizations and some of them are available on-chain too. But optimizations for pairings-based operations, on the other hand, are not very efficient whether it is for off-chain or for on-chain systems.

3.2 Threshold Anonymous Credentials with Opening (TACO)

A threshold anonymous credential system (TAC) has a set of (possibly malicious) distributed issuers who issue partial credentials over a blockchain and at least a threshold number of them are required to construct the final credential. A TAC system that supports threshold opening after consensus from at least a threshold number of credential openers is referred to as a TACO system. Coconut (Sonnino et al., 2019) is a TAC system and DTRAC (Naaz et al., 2022) extends Coconut to enable opening, i.e. a TACO system. We describe a generic TACO system, modelled along the lines of Coconut and DTRAC, as shown in Figure 1. The stakeholders of the system are a) the user, who requires an anonymous credential that attests to her attributes – without revealing them – to avail a service, b) certifiers, who attest the attributes of the user and sign on the attribute commitments to generate verifiable certificates, c) credential issuers (CI), who are distributed entities that generate partial credentials – a threshold number of which are required to construct the final credential – after verifying the certificates issued by the certifier, d) service provider (SP), who verifies the anonymous credential of the user and grants the service, and e) credential openers (CO) who are distributed entities with partial opening information that can open/deanonymize the user if at least a threshold number of them come together.

A threshold anonymous credential with opening (TACO) can be described in four phases: *1) Registration Phase,* where the user obtains verifiable certificates on the attributes from the certifiers. *2) Issuance Phase,* where the user sends these certificates along with the commitments to her attributes, the opening shares and the corresponding ZKPs to the credential issuers via the blockchain, who issue the partial credentials after verification. Then the openers are provided with their individual opening (deanonymizing) information called partial opening shares. The entire process is referred to as credential request verification, $Credreq_{ver}$ (Step 4, Figure1). A TAC system has no openers, and therefore $Credreq_{ver}$ does not have to verify the ZKP for the correctness of the opening shares. Once the user receives a threshold number of partial credentials, she aggregates them to obtain the final anonymous credential. *3) Verification Phase,* where the user randomizes the credential and presents it to the service provider who verifies the proofs on-chain. We refer to this as credential verification, $Cred_{ver}$ (Step 10, Figure 1). *4) Opening Phase,* which is initiated if deemed necessary to deanonymize the user. Once a credential opener receives a threshold number of opening shares from the other openers, it can deanonymize the user.

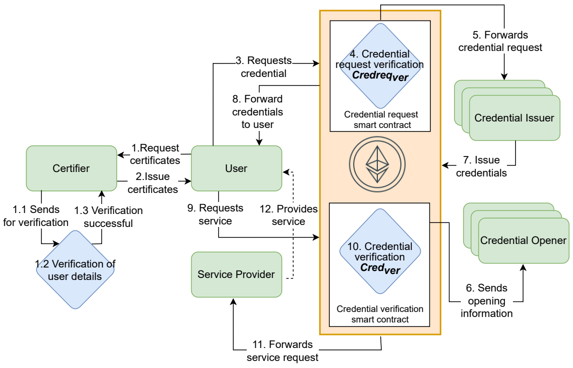
5. Forwards credential request
3. Requests credential
4. Credential request verification Credreqver
Credential request smart contract
8. Forward credentials to user
Credential Issuer
1.Request certificates
2.Issue certificates
Certifier
User
7. Issue credentials
1.1 Sends for verification
1.3 Verification successful
9. Requests service
12. Provides service
1.2 Verification of user details
10. Credential verification Credver
Credential Opener
Service Provider
Credential verification smart contract
6. Sends opening information
11. Forwards service request

Figure 1: Overview of TACO over blockchains for credential management.

The credential request verification $Credreq_{ver}$ and credential verification $Cred_{ver}$ are the only on-chain functions where cryptographic operations are performed. $Credreq_{ver}$ is run once per credential issuance and $Cred_{ver}$ is run every time a service is availed. They perform several ECC operations including pairings on-chain for the verification of ZKPs which is the main reason for high gas costs.

3.3 Off-Chaining

Off-chaining (Smith and Doe, 2022) takes smart contract computations outside the blockchain node reducing transaction/gas costs. The off-chain nodes that execute the computation are called solver nodes. Even though off-chaining reduces transaction costs, it has its limitations. The system may become more complex as off-chaining can add additional stakeholders and communication links to realize all the original functionalities. Off-chain solutions typically require additional infrastructure, maintenance and operational costs. The security will have to be analyzed again because the off-chain data and processes lack the consensus mechanisms and immutability properties of the blockchain which can lead to new attacks and collusion of various entities. It can also create interoperability challenges.

We assume that the TEB system does not have 1) any inter-smart contract dependencies, 2) any time-sensitive data requirements, 3) any intermediate inter-stakeholder communications, 4) any interoperarability requirements, and 5) any verifiable on-chain computations. Existing off-chaining approaches such as those discussed in (Eberhardt and Heiss, 2018) are not suitable for TEB systems. Verifiable off-chaining computation (eg. (Miers et al., 2013), (Sasson et al., 2014)) requires that the function being off-chained is a verifiable function but TEB systems do not necessitate having any. Secure multiparty computation-based off-chaining (eg. (Zhu et al., 2018)) performs computations on private inputs, which are split as shares across the solver nodes, who generate outputs that are aggregated for the final result. However, this cannot be generalized for all TEB systems – for e.g. in TACO, the blockchain verifications do not use private inputs and the output of each threshold entity is independent. Enclave-based off-chain computations require the system to place trust in external hardware which compromises the strong privacy guarantees of TEB systems. Incentive-driven off-chain computations (eg. (Teutsch and Reitwießner, 2019)) are used typically when the execution traces are short. In a TEB system, if we have to maintain traces for all the cryptographic operations off-chain and run the traces that differ, on-chain, for every dispute, then there will be considerable memory and computation overhead, which is undesirable.

4 SOLUTION OVERVIEW

All elliptic curve operations, especially pairings, are computationally expensive as we saw in Section 3.1. Over blockchains, such computations incur huge gas costs. We propose a new off-chaining technique – *threshold **o**ff-chain **c**omputation (TOC)* – for **t**hreshold-based **e**lliptic curve cryptographic systems over **b**lockchains (TEB). The key idea here is to leverage the threshold trust assumption – i.e. at least a threshold number of entities are not malicious – to off-chain elliptic curve cryptographic computations to solver nodes while ensuring the same security and privacy guarantees as long as they follow the threshold assumption. The solver nodes can be motivated by incentives. The immutability and trust guarantees of the blockchain are replaced by the threshold trust assumption. The system does not trust individual solvers and assumes that the off-chained code is public. It uses only public inputs and generates only public outputs. We use **t**hreshold **a**nonymous **c**redential system with **o**pening (TACO) and without opening (TAC) as examples of TEB systems.

We make an important non-intuitive observation that the execution time of the overall system does not benefit from the off-chaining, but rather shows a degradation. The reason for this is that blockchains including Ethereum have in-built pre-compiled contracts optimized for elliptic curve pairings which are executed on dedicated mining hardware when run on-chain. The same operations on solver nodes, do not have access to such optimizations and have implementations typically running on general-purpose hardware, thus resulting in longer execution times. Given the threshold assumption as well as the drawback mentioned above, we use two different implementation approaches to reinforce the threshold off-chain computation: 1) selective off-chaining for TAC, and 2) empirical push-back off-chaining for TACO. In selective off-chaining, we off-chain all the functions we identify as resource-intensive, whereas in the empirical push-back approach, we make use of both on-chain and off-chain optimizations to achieve a balance between gas costs and execution time.

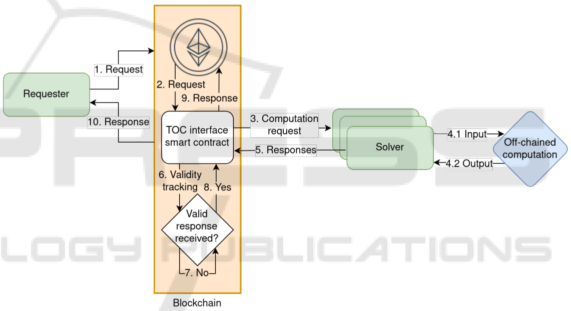

Figure 2: Overview of threshold off-chain computation.

We introduce an *on-chain **t**hreshold **o**ff-chain **c**omputation (TOC) interface smart contract* as an interface to facilitate communication between the on-chain components and the solver nodes. Figure 2 depicts the workflow. When a requester makes a request to the blockchain for a function to be off-chained (Step 1), the request is forwarded to the TOC interface smart contract (Step 2). The interface ensures access control, integrity, data synchronization, formatting and processing, error handling of the input and output data between the original system and the off-chain nodes as per specific requirements of the system. After the request is validated, it is forwarded to the solver nodes (Step 3) who independently execute the required functions for the same set of inputs (Step 4.1) and generate the outputs (Step 4.2). The solvers send the responses to the interface (Step 5) and it checks whether the responses are valid (Step 6). The computation is deemed valid (Step 8) only if at least a threshold number of them responds. The outputs from the solvers are sent to the on-chain system by the interface for further computations (Step 9). The interface can also track incentives by recording the addresses of the off-chain nodes that respond. Figure 3 provides a high-level view of data propagation and data reception in the proposed TOC approach.

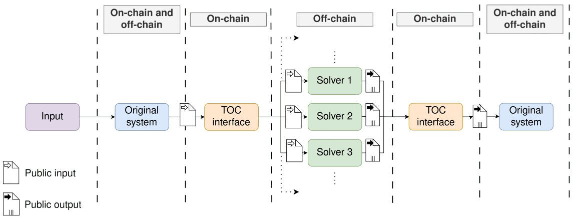

Figure 3: Input-output data flow diagram of threshold off-chain computation.

5 IMPLEMENTATION

This work applies the **t**hreshold **o**ff-chain **c**omputation (TOC) approach to a **t**hreshold-based **e**lliptic curve cryptographic system over **b**lockchains (TEB). For an instance of a TEB system, this work chooses **t**hreshold **a**nonymous **c**redential system with **o**pening (TACO) as it has multiple on-chain elliptic curve operations. As TEB systems using TAC and TACO, Coconut (Sonnino et al., 2019) and DTRAC (Naaz et al., 2022) can be considered as the base systems, respectively. DTRAC (Naaz et al., 2022) is used as a reference implementation of a TACO scheme since it can be modified to operate in both TAC and TACO modes. The major difference between TAC and TACO is in the issuance phase which executes the credential request verification function $Credreq_{ver}$ – the credential issuers must verify the correctness of the opening shares in a TACO system, which they do not have to do in a TAC system. In the TACO system, TOC is applied to credential request verification, $Credreq_{ver}$ and credential verification, $Cred_{ver}$ as they use several pairings and non-pairings based elliptic curve operations, and therefore, are resource-intensive. The off-chaining of a TEB system with TOC happens in five phases: 1) the *assessment phase*, to decide whether a TEB system is feasible for threshold off-chaining, 2) the *classification phase*, to classify the functions to be off-chained, 3) the *design phase*, to formulate a new system with the identified functions running on the solver nodes, 4) the *security analysis phase*, to verify the security and consistency of the new system, and 5) the *implementation and evaluation phase*, to execute the new system on an instantiation of a TEB system.

5.1 Off-Chaining Approaches for TAC and TACO

The asymptotic analysis for the number of elliptic curve cryptographic operations for DTRAC is given in Table 2. Bilinear pairings-based elliptic curve cryptographic operations are more complex and have high gas usage than other elliptic curve operations (Section 3.1). However, non-pairings-based operations still incur a similar gas cost because they are more in number. Therefore, both pairings-based and non-pairings-based elliptic curve operations are potential candidates for off-chaining to reduce gas costs. Another important observation in Table 2 is that for the opening functionality, the number of pairings increases linearly with the number of openers, whereas for all the other functionalities, it remains constant. As noted before, since pairings have very limited optimizations both on-chain and off-chain, off-chaining these operations to less powerful solver nodes can lead to increased execution times. This will impact TACO systems more than TAC systems since the number of pairings increases linearly with the number of openers. To accommodate these differences, we introduce two off-chain implementation approaches: 1) Selective off-chaining for TAC systems and 2) Empirical push-back off-chaining for TACO systems.

Selective off-chaining approach for TAC. In this approach, we identify the two resource-intensive functions that use elliptic curve operations – credential request verification, $Credreq_{ver}$ and credential verification function, $Cred_{ver}$ – to off-chain.

Empirical push-back off-chaining approach for TACO. Here also, $Credreq_{ver}$ and $Cred_{ver}$ are identified as functions to be off-chained for a TACO system. However, even though it reduces the gas costs as shown in Figure 7, a performance degradation is observed as shown in Figure 11, due to pairings-based operations that grow linearly in the number of openers. The Ethereum Virtual Machine (EVM) uses built-in pre-compiled contracts for all elliptic curve operations including addition (alt_bn128), scalar multiplication (EIP-196) and pairings (EIP-197). All these contracts are optimized to fit within the block gas limit. However, the gas costs incurred by pairings are still large due to their complex and non-trivial nature. Also, the nature of the bilinear pairing operation, which combines elements from two different groups, limits its flexibility to be optimized in general. However, this is not the case with standard elliptic curve operations, which can utilize compiler optimizations and parallelizations run off-chain on a solver node. The empirical data relating to execution time (Figure 11) indicates that, if off-chaining is limited to

Table 2: Asymptotics of elliptic curve operations for on-chain verification operations in DTRAC.

Elliptic curve operation		$\mathbb{G}_1$ point negation	Scalar multiplication	Pairing	$\mathbb{G}_1$ Point addition	Modular exponentiation	$\mathbb{G}_2$ point addition
Gas cost per unit operation		100	6000	$34000 \times k + 45000$	150	200	28474
Verification operation	Credential verification	$O(n_{attr})$	$O(n_{attr})$	$O(1)$	$O(1)$		$O(1)$
	Correctness of opening shares	$O(n_{CO})$	$O(n_{CO} \times n_{priv.attr} \times t_{CO})$	$O(n_{CO})$	$O(n_{CO} \times n_{priv.attr})$		$O(n_{CO})$
	Signature on certificate		$O(n_{certs})$		$O(n_{certs})$	$O(n_{certs})$	
	Correctness of attributes		$O(n^2_{attr})$		$O(n^2_{attr})$		

k is the no. of points on which pairing is done, n_{attr} is the total number of attributes, n_{CO} is the total number of credential openers, $n_{priv.attr}$ is the number of private attributes, t_{CO} is the threshold value for credential openers and n_{certs} is the total number of certificates.

non-pairing based elliptic curve cryptographic operations and pairings-based functions are pushed back on-chain, the execution time improves. The pairings-based operations benefit from running on the miner nodes. This enables us to achieve the best of both worlds at a slightly higher gas cost.

Using Table 2 as a reference, we off-chain the non-pairing elliptic curve operations of $Credreq_{ver}$ in the TACO system, while keeping the pairing operations on-chain. That is, the verification of ZKPoKs that proves the correctness of the commitments of the user attributes and the signature verification of the certificates issued by the certifiers are off-chained. However, the verification of the ZKPoK that proves the correctness of the encrypted opening shares is pushed back on-chain. The execution time of the off-chained $Cred_{ver}$ is lesser than the average block time of Ethereum because it has only very few (constant number) pairings-based operations. It is therefore off-chained as per the selective off-chaining approach.

5.2 Instantiation of TAC and TACO

DTRAC is a threshold anonymous credential system over blockchains that extends Coconut to enable threshold opening of the credential. To instantiate the TACO system, we use DTRAC as-is, and to instantiate the TAC system we disable the opening functionality. Using DTRAC for both TAC and TACO systems ensures consistency in our comparisons of the performances over various benchmarks. Note that in DTRAC, credential issuers of the TACO system are referred to as validators and credential openers are referred to as openers. The $Credreq_{ver}$ operation includes both Verify Vcerts and Verify proofs functions of DTRAC and $Cred_{ver}$ is the same as VerifyCred in DTRAC.

Assessment Phase. The bottleneck estimation of DTRAC (Table 3) reveals that the two on-chain processes 1) Verify Vcerts and Verify proofs ($Credreq_{ver}$) executed by the validators in the issuance phase ((Naaz et al., 2022, Figure 4)) and 2) VerifyCred ($Cred_{ver}$) executed by the service provider in the verification phase ((Naaz et al., 2022, Figure 5)) take up 94% of the gas cost and 80% of the execution time, respectively. The elliptic curve cryptographic computations in these smart contracts are the cause of the performance bottleneck and since they are contained in specific smart contracts with no architecture or ecosystem-related dependency, off-chaining is a viable option.

Classification Phase. The credential request verification $Credreq_{ver}$ (Step 4) and the credential verification $Cred_{ver}$ (Step 10) functions do not incur any major communication overhead because they only have data inputs typically in the range of tens of bytes and the output of a verification function is either true or false. These functions do not produce output data that needs to be shared with other stakeholder nodes, and thus they have minimal immutability requirements. The functions $Credreq_{ver}$ and $Cred_{ver}$ do not use any private code and thus can be shared with untrusted entities for execution. The inputs to the function are public parameters shared on-chain, and the output are public values as they are verification functions outputting either true or false. We thus conclude that

Table 3: Bottleneck Estimation of DTRAC.

Method	Avg. gas cost	Avg. time
	(in million)	(in sec)
Verify Vcerts and Verify proofs ($Credreq_{ver}$)	6	35.2
VerifyCred ($Cred_{ver}$)	1	5.3
Others	0.4	10.3
Total	7.4	50.8

$Credreq_{ver}$ and $Cred_{ver}$ are viable candidates to be off-chained.

Design Phase. Threshold off-chain computation (TOC) is applied to $Credreq_{ver}$ and direct off-chaining – which can be described as the TOC approach with the threshold value set to 1 – is applied to off-chain $Cred_{ver}$. The reason for the TOC approach is that the on-chain $Credreq_{ver}$ function is performed by issuers that follow the threshold trust assumption. In the off-chain system, the issuers are extended to additionally perform the role of the solver nodes. The threshold trust assumption ensures the same trust guarantees in the off-chain system. In $Cred_{ver}$, the choice of providing the service or not is solely up to the service provider regardless of it being performed on-chain or off-chain. This is the case even if the credential is valid. Thus, the trust guarantee solely relies on the service provider, and therefore, having the service provider perform the function off-chain will still ensure the same trust guarantees and computational availability. Figure 4 describes a TACO system after off-chaining and the modified entities and functionalities are marked with the ”Extended” prefix. The two timeline charts compare and contrast the chronological sequence of events in a threshold anonymous credential system before (Figure 5) and after off-chaining (Figure 6).

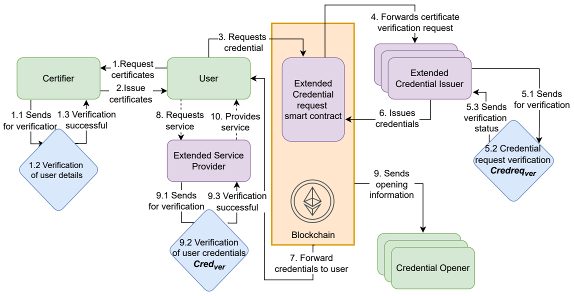
Certifier
User
1.Request certificates
2.Issue certificates
3. Requests credential
1.1 Sends for verificatior
1.3 Verification successful
1.2 Verification of user details
8. Requests service
10. Provides service
Extended Service Provider
9.1 Sends for verification
9.3 Verification successful
9.2 Verification of user credentials $Cred_{ver}$
Extended Credential request smart contract
Blockchain
7. Forward credentials to user
4. Forwards certificate verification request
Extended Credential Issuer
6. Issues credentials
5.1 Sends for verification
5.3 Sends verification status
5.2 Credential request verification $Credreq_{ver}$
9. Sends opening information
Credential Opener

Figure 4: Threshold anonymous credentials after off-chaining.

Security Analysis Phase. Here, checks are made to determine if the security requirements of the on-chain system are met off-chain. The off-chained TEB system has no/minimal data immutability requirements and uses on-chain storage which ensures data availability as blockchains are a highly available platform. The privacy and trust guarantees of the system are preserved as discussed in the design phases. The TOC interface smart contract ensures access control.

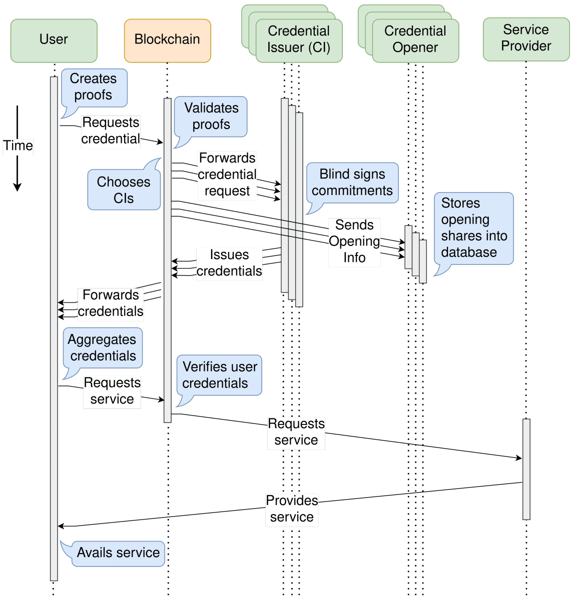

Figure 5: Timeline of credential issuance and availing a service before off-chaining.

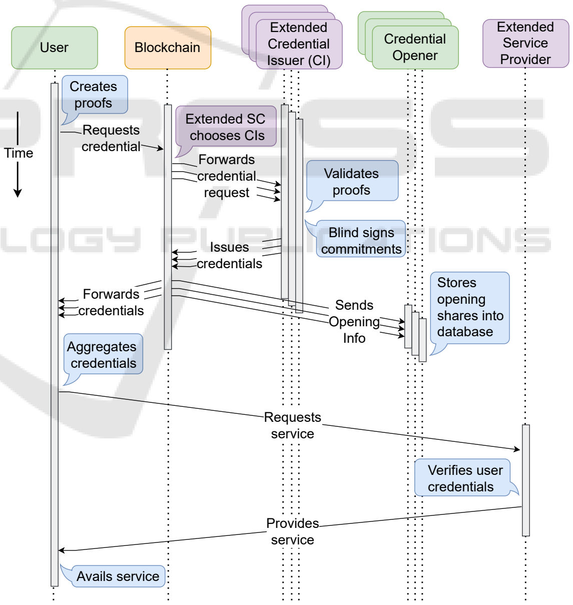

Figure 6: Timeline of credential issuance and availing a service after off-chaining.

Implementation and Evaluation Phase. TOC and direct off-chaining approaches are implemented for both TACO and TAC as per the design we finalized. This is implemented on the same DTRAC system by enabling and disabling the opening functionality.

6 EVALUATION

We present the evaluation of the off-chained DTRAC after implementing selective off-chaining for DTRAC with and without opening, and empirical pushback off-chaining for DTRAC with opening.

6.1 Experimental Setup

The specifications of the computation environment and the number of entities are given in Table 5 and Table 6, respectively. The experiments were performed on a 64-bit Ubuntu 22.04.2 LTS with AMD Ryzen 5 5600H CPU (6 core and 12 threads at 4.2 GHz) and 16 GB RAM. The implementation was built using Python for the codebase and Solidity for the smart contracts. The smart contracts were deployed on the local blockchain, Ganache and to accurately reflect the real-world execution time of a blockchain, we also deploy the smart contracts on the public testnet, Sepolia. We consider several combinations of the evaluation setup which are summarized in Table 4.

6.2 Gas Costs

For selective off-chaining for TAC (Figure 8), the gas cost for $Credreq_{ver}$ improves by 5.65x and 5.15x for Ganache and Sepolia, respectively. When using selective off-chaining in TACO (Figure 7), the gas cost reduces significantly for $Credreq_{ver}$ – 25x in Ganache and 23x in Sepolia. However, the execution time degrades (refer Section 5.1 and Figure 11) and therefore to balance that, we do empirical push-back for TACO (Figure 9) where the gas cost for $Credreq_{ver}$ still improves by 4.75x and 3.61x for Ganache and Sepolia, respectively. This is as expected as less on-chain computations result in lower gas costs. The gas cost for the credential verification function, $Cred_{ver}$ is zero for both TAC and TACO systems since we bypass the blockchain completely.

6.3 Execution Time

Figure 10 depicts the execution time for TAC after applying selective off-chaining to the $Credreq_{ver}$ and $Cred_{ver}$ functions. In Ganache, the execution time reduces drastically for $Credreq_{ver}$ when off-chained. However, in Sepolia, the off-chained $Credreq_{ver}$ waits for the data to be published on the blockchain to initiate the verification computations, making the execution time comparable with the on-chain case. The execution time for the off-chain $Cred_{ver}$ for both Ganache and Sepolia resulted in comparable outcomes to the on-chain case. This is because 1) the optimizations for pairings provided by pre-compiled on-chain contracts and the optimizations for non-pairing operations offered by the off-chain nodes offset each other, and 2) $Cred_{ver}$ performs fewer elliptic curve operations, including pairings, compared to $Credreq_{ver}$ (Table 2).

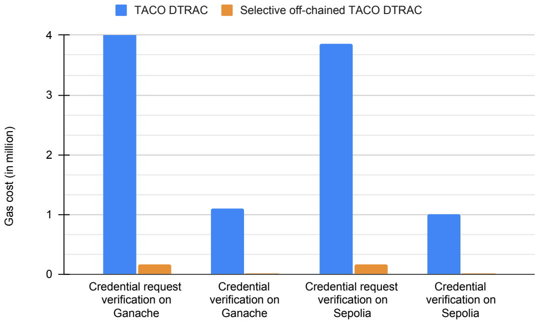

Figure 7: Gas costs of threshold anonymous credentials with opening (TACO) using selective off-chaining.

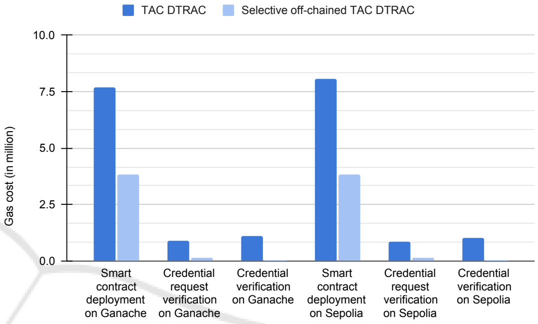

Figure 8: Gas costs of threshold anonymous credentials without opening (TAC) using selective off-chaining.

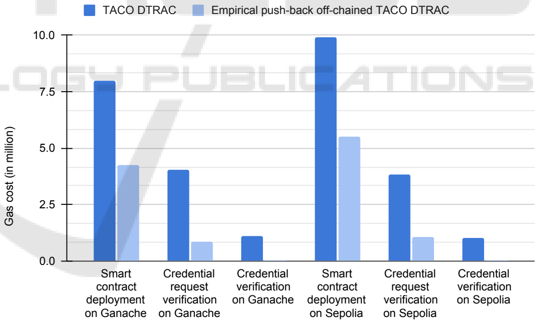

Figure 9: Gas costs of threshold anonymous credentials with opening (TACO) using empirical push-back off-chaining.

Table 4: Evaluation setup summarized.

Mode of system	Blockchain platform	On-chain (original)	Selective off-chaining	Empirical push-back off-chaining
TAC	Ganache	Considered in all evaluation items	Gas cost (Figure 8), Execution time (Figure 10)	N/A
	Sepolia			
TACO	Ganache		Gas cost (Figure 7), Execution time (Figure 11)	Gas cost (Figure 9), Execution time (Figure 12)
	Sepolia			

Table 5: Specifications of the computation environment.

Components	Specification	Version
Blockchain	Ethereum	1
Ethereum emulator	Ganache	2.5.4
	Sepolia	0x90000069
Smart contracts	Solidity	0.8.19
Cryptographic library	py_ecc	6.0.0

Table 6: Number of Entities.

Type	No of entities
Certifiers	2
Validators (total, threshold)	(3,2)
Openers (total, threshold)	(3,2)

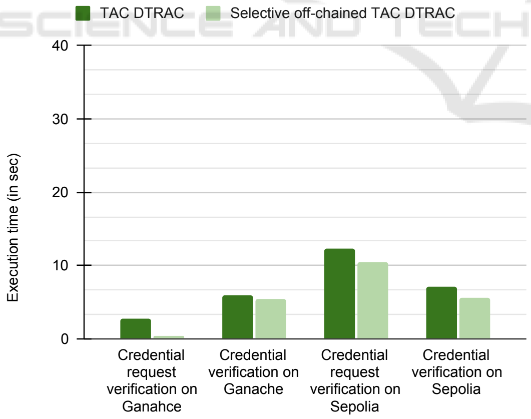

Figure 10: Execution times of threshold anonymous credentials without opening (TAC) using selective off-chaining.

For a TACO system, Figure 11 depicts the execution time with selective off-chaining and Figure 12 depicts the execution time with empirical push-back off-chaining. A significant degradation of the execution time for $Credreq_{ver}$ is observed with selective off-chaining, despite the substantial reduction of gas cost (Figure 7), for both Ganache and Sepolia. As discussed in Section 5.1, a solution to this is empirical push-back off-chaining, which improves the execution time at the cost of slightly increased gas cost. After the empirical push-back of TACO, the improvement in execution time of $Credreq_{ver}$ is significant for Ganache, as shown in Figure 12. However, in Sepolia, the execution time remains comparable to the on-chain case. This is because the system waits one block time for the on-chain verification of the correctness of the opening shares and only after that do the off-chain nodes fetch the data from the blockchain and perform the efficient off-chain operations. The off-chaining of $Cred_{ver}$ in TACO is similar to that of TAC because

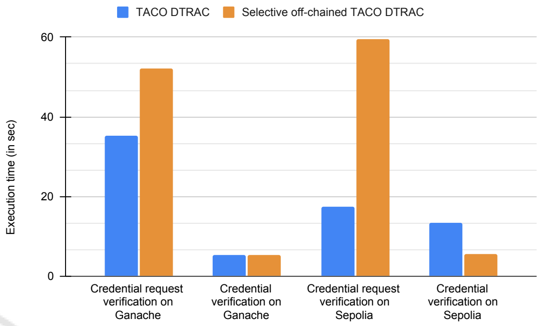

Figure 11: Execution time of threshold anonymous credentials with opening (TACO) using selective off-chaining.

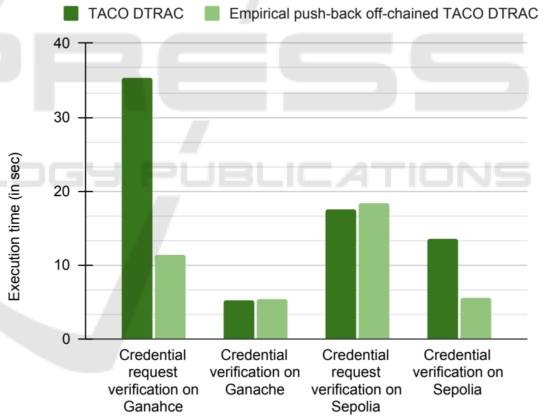

Figure 12: Execution times of threshold anonymous credentials with opening (TACO) using empirical push-back off-chaining.

it has no opening operations, and therefore the observations and justifications are the same as that of TAC, for both Ganache and Sepolia. The empirical push-back off-chaining approach reduces the overall gas costs while maintaining or improving the execution times as summarized in Figure 12.

7 CONCLUSION AND FUTURE WORK

This work addressed the problem of high gas consumption of smart contracts when they are used in threshold-based elliptic curve cryptographic systems (TEB) such as anonymous credential systems over blockchains. A new approach, threshold off-chain computation (TOC), was introduced which offloads on-chain functions from smart contracts to off-chain solver nodes, that follow the threshold trust assumption, thus reducing gas costs. The off-chained functions preserve the trust guarantees and computation correctness as long as at least a threshold number of solver nodes are honest. This paper first described a threshold-based anonymous credential system a) with opening (TACO) and b) without opening (TAC) over a blockchain as a base TEB system to illustrate the proposed TOC approach. Both TACO and TAC were instantiated using DTRAC. Two different TOC approaches were adopted: 1) selective off-chaining for TAC and 2) empirical push-back off-chaining for TACO, based on the asymptotic analysis of the number of pairings to be off-chained. The performance evaluation of both gas consumption and execution time demonstrated the effectiveness of the solution.

A possible future direction is to explore whether the non-interactive zero-knowledge proofs used in these TACO systems can be replaced with the shorter zk-SNARKS such Groth16 (Groth, 2016). This may allow selective off-chaining for TACO without any performance degradation. This will also allow the batching of off-chain verifications, which will make the system scalable. Rewarding off-chain computing nodes is also another direction to ensure computational correctness. A formal security analysis of the off-chained system in the UC framework was skipped since the work do not modify the underlying cryptographic primitives. However, this can be attempted as a future work.

REFERENCES

Boneh, D., Boyen, X., and Shacham, H. (2004). Short group signatures. In *Annual international cryptology conference*, pages 41–55. Springer.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology—CRYPTO 2001, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*, pages 213–229. Springer.

Buccafurri, F., Angelis, V., and Lazzaro, S. (2022). A blockchain-based framework to enhance anonymous services with accountability guarantees. *Future Internet*, 14:243.

Camenisch, J., Dubovitskaya, M., Haralambiev, K., and Kohlweiss, M. (2015). Composable and modular anonymous credentials: Definitions and practical constructions. In Iwata, T. and Cheon, J. H., editors, *Advances in Cryptology – ASIACRYPT 2015*, pages 262–288, Berlin, Heidelberg. Springer Berlin Heidelberg.

Camenisch, J. and Lysyanskaya, A. (2001). An identity escrow scheme with appointed verifiers. In *Advances in Cryptology—CRYPTO 2001, Santa Barbara, California, USA, August 19–23, 2001 Proceedings 21*, pages 388–407. Springer.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044.

Connolly, A., Lafourcade, P., and Perez Kempner, O. (2022). Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes. In *Public-Key Cryptography – PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part I*, Berlin, Heidelberg. Springer-Verlag.

Eberhardt, J. and Heiss, J. (2018). Off-chaining models and approaches to off-chain computations. In *Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, SERIAL'18, page 7–12, New York, NY, USA. Association for Computing Machinery.

Eberhardt, J. and Tai, S. (2017). On or off the blockchain? insights on off-chaining computation and data. In *Service-Oriented and Cloud Computing: 6th IFIP WG 2.14 European Conference, ESOCC 2017, Oslo, Norway, September 27-29, 2017, Proceedings 6*, pages 3–15. Springer.

Eberhardt, J. and Tai, S. (2018). Zokrates - scalable privacy-preserving off-chain computations. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1084–1091.

Fuchsbauer, G., Hanser, C., and Slamanig, D. (2018). Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *Journal of Cryptology*, 32.

Garman, C., Green, M., and Miers, I. (2014). Decentralized anonymous credentials. *Network and Distributed System Security Symposium (NDSS), San Diego, California*.

Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98.

Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Fischlin, M. and Coron, J.-S., editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 305–326, Berlin, Heidelberg. Springer Berlin Heidelberg.

Hébant, C. and Pointcheval, D. (2022). Traceable constant-size multi-authority credentials. In Galdi, C. and Jarecki, S., editors, *Security and Cryptography for Networks*, pages 411–434, Cham. Springer International Publishing.

Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S. M., and Felten, E. W. (2018). Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1353–1370, Baltimore, MD. USENIX Association.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209.

Liu, C., Bodorik, P., and Jutla, D. (2021). A tool for moving blockchain computations off-chain. In *Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, BSCI '21, page 103–109, New York, NY, USA. Association for Computing Machinery.

Liu, C. G., Bodorik, P., and Jutla, D. (2022). Automating smart contract generation on blockchains using multi-modal modeling [j]. *Journal of Advances in Information Technology*, 13.

Miers, I., Garman, C., Green, M., and Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy*, pages 397–411. IEEE.

Miller, V. S. (1986). Use of elliptic curves in cryptography. In Williams, H. C., editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 417–426, Berlin, Heidelberg. Springer Berlin Heidelberg.

Molina-Jimenez, C., Sfyrakis, I., Solaiman, E., Ng, I., Weng Wong, M., Chun, A., and Crowcroft, J. (2018). Implementation of smart contracts using hybrid architectures with on and off–blockchain omponents. In *2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2)*, pages 83–90.

Muth, R., Galal, T., Heiss, J., and Tschorsch, F. (2023). Towards smart contract-based verification of anonymous credentials. *Financial Cryptography and Data Security. FC 2022 International Workshops*, pages 481–498.

Naaz, A., Pavan Kumar B, T. V., Francis, M., and Kataoka, K. (2022). Integrating threshold opening with threshold issuance of anonymous credentials over blockchains for a multi-certifier communication model. *IEEE Access*, 10:128697–128720.

Pointcheval, D. and Sanders, O. (2016). Short randomizable signatures. In *Topics in Cryptology-CT-RSA 2016: The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29-March 4, 2016, Proceedings*, pages 111–126. Springer.

Rathee, D., Policharla, G. V., Xie, T., Cottone, R., and Song, D. (2022). ZEBRA: anonymous credentials with practical on-chain verification and applications to KYC in defi. *IACR Cryptol. ePrint Arch.*, page 1286.

Ren, Q., Wu, Y., Liu, H., Li, Y., Victor, A., Lei, H., Wang, L., and Chen, B. (2022). Cloak: Transitioning states on legacy blockchains using secure and publicly verifiable off-chain multi-party computation. In *Proceedings of the 38th Annual Computer Security Applications Conference*, pages 117–131.

Rosenberg, M., White, J., Garman, C., and Miers, I. (2023). zk-creds: Flexible anonymous credentials from zk-snarks and existing identity infrastructure. In *2023 2023 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1882–1900, Los Alamitos, CA, USA. IEEE Computer Society.

Sanders, O. (2020). Efficient redactable signature and application to anonymous credentials. In Kiayias, A., Kohlweiss, M., Wallden, P., and Zikas, V., editors, *Public-Key Cryptography – PKC 2020*, pages 628–656, Cham. Springer International Publishing.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE symposium on security and privacy*, pages 459–474. IEEE.

Smith, J. and Doe, J. (2022). Off-chaining models and approaches to off-chain computations. *Journal of Off-chain Computing*, 1(1):1–10.

Sonnino, A., Al-Bassam, M., Bano, S., Meiklejohn, S., and Danezis, G. (2019). Coconut: threshold issuance selective disclosure credentials with applications to distributed ledgers. *26th Annual Network and Distributed System Security Symposium (NDSS), San Diego, California.*

Teutsch, J. and Reitwießner, C. (2019). A scalable verification solution for blockchains. *arXiv preprint arXiv:1908.04756*.

Yu, Y., Zhao, Y., Li, Y., Wang, L., Du, X., and Guizani, M. (2019). Blockchain-based anonymous authentication with selective revocation for smart industrial applications. *IEEE Transactions on Industrial Informatics*, PP:1–1.

Zhu, Y., Song, X., Yang, S., Qin, Y., and Zhou, Q. (2018). Secure smart contract system built on smpc over blockchain. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1539–1544. IEEE.