IEEE ICBC'24 1570977344

LIMBOCOIN:
On the Denial-of-Service of Token based Retail CBDCs

Anonymous Author(s)

***Abstract*—Several nations across the world are contemplating optimal design choices for Central Bank Digital Currencies (CBDCs). We present LIMBOCOIN, an analytical framework for an arbitrary token based CBDC protocol. LIMBOCOIN, under practical state-of-the-art assumptions on secure system design and protocol incentivization, considers an adversarial behaviour to achieve denial-of-service on the CBDC's associated system and token economy. LIMBOCOIN outlines the quality of the CBDC system and economy resultant from the interaction of honest and adversarial users in the CBDC's jurisdiction. Through LIMBOCOIN, we show that in the worst case, the number of compromised CBDC wallets in circulation can exceed the number of uncompromised wallets in circulation in the CBDC's jurisdiction. We also show that in the worst case, the value associated with token based transactions that is denied service exceeds 90 percent of the value associated with token based transactions in legitimate service.**

I. INTRODUCTION

The design choices to realize central bank digital currencies (CBDCs) have been extensively explored [1]. Token-based CBDC solutions, which mimic bank notes in behaviour, and that need to be operational even when the central bank or its currency managing delegates are offline, have been considered by some central banks of populous nations [2]. However, current solutions point to the promise that CBDC systems would be successful on the condition that the central bank or its delegates maintain the account state in some form of the transacting users, and are always online [3], [4].

Unfortunately, there is a gap in the analysis between the viability of online account based and offline token based CBDC systems, especially at scale. Consequently, an analysis of the same is warranted. The biggest differentiator between the two said models comes from a qualitative standpoint: the verification overhead induced by a token based economy (similar to a banknote based economy), far exceeds the same in an account based economy. This verification overhead of a token based system can be exploited to paralyze the said system and bring the associated economy to a halt.

Our Contributions. We consider an arbitrary token based CBDC protocol, that needs to be deployed at scale. For the said protocol we contemplate denial-of-service (DoS) attacks that might be possible in the system deployment of the protocol and those that might be possible at the validation level of the token economy implied by the protocol. To that end, we present an analysis named LIMBOCOIN, detailed next.

1. For any offline CBDC system for a populous nation, there needs to be trustworthy deployment of computational resources in order to realize a legitimate system. One scalable and popular way to achieve such legitimacy is to ensure that all CBDC protocol specific computational resources are deployed distributively among stakeholders through trusted execution environments (TEEs) [5]. This principle has been ratified in [6], [7]. In the first part of the LIMBOCOIN analysis, we independently establish that for any given token based offline CBDC protocol, TEEs are an appropriate choice for deployment of the said protocol, considering scalability of the consequential economy (Section II-A). The LIMBOCOIN analysis then details that when the said protocol is deployed using TEEs with appropriate incentivization under a Cournot competition [8] (Section II-C), the number of wallets which have their private state leaked exceeds a large fraction of the uncompromised wallets in circulation in the associated national jurisdiction, especially if the jurisdiction where the protocol is deployed has a large population of adversarial users (Section V-A).

2. For any token based CBDC protocol, if the protocol supports an intermittent offline functionality [9] for its users, the state of each token exchanged during any offline phase must eventually be validated by the central bank or one of its delegates when the offline phase token holders eventually come online. In the second part of the LIMBOCOIN analysis, we show that even if the CBDC protocol in question adopts state-of-the-art transaction fee mechanisms from blockchain-like fee markets [10] (Section II-D), there exist adversarial CBDC transaction strategies under which tokens from honest users are delayed in verification and tokens from adversarial users are verified instead which have no economic consequence in the CBDC's jurisdiction (Section IV-B). To conclude our analysis, we show that for the most resilient of transaction fee mechanism's adoption, under a pessimistic denial-of-service measure considered by the adversary, the CBDC value denied service exceeds 20 percent of the CBDC value in legitimate service, and for a sub-optimal transaction fee mechanism's adoption, under an optimistic denial-of-service measure considered by the adversary, the CBDC value denied service exceeds 90 percent of the CBDC value in legitimate service (Section V-B).

Related Work. A token based e-cash solution has been proposed where the central bank can enforce simple regulatory rules such as payment limits [11]. A permissioned blockchain based auditable token management system under the UTXO model has also been proposed [12]. PEReDi [4] is an account based decentralized CBDC system which supports

the implementation of a token based economy. A sustainable peer-to-peer offline e-payment system leveraging TEEs and using one-time programs has also been proposed [13]. Project Sela [14] was a proof-of-concept of an accessible and secure retail CBDC system conducted by the Hong Kong monetary authority. A CBDC SSID App (a self sovereign identity wallet) [15] has been built for Apple iPhones allowing central banks and other financial institutions to securely issue, manage, and administer CBDCs. To the best of our knowledge, none of these solutions or others existing in the literature analyze an arbitrary token based CBDC system for its security in terms of service viability attacks on the associated system and/or the resultant token economy.

II. The LimboCoin System Model

We consider an arbitrary token based CBDC protocol Π which is specified to work in an offline setting. We first discuss options for secure deployments of Π. We then detail the optimal system design choices for Π. Following this, we provide incentivization models for the maintainers of the CBDC system to keep the corresponding economy correctly operational.

A. Architecture Choices for CBDC Systems

We require that the Π related CBDC system should have the following indispensable requirements: (A_1) *Ease of Deployment:* the system must be easy to interface and use for the CBDC users; (A_2) *Scalable Deployment:* the system must be deployable at the last mile in every potential jurisdiction, and so Π should be realizable on low budget handheld devices also; (A_3) *Sufficient State Management:* given the processing overheads of a token economy, the system must be able to support computation under large state machines; and (A_4) *Secure Deployment:* the system must be free from vulnerabilities. Keeping these requirements in mind, we consider next different system architectures to realize Π.

Specialized secure crypto-processor standards, such as trusted platform modules (TPMs) [16], which might be good choices under requirements A_1 and A_4, would have two problems in the deployment of protocols such as Π: (A_2) *Deployability at scale.* TPMs are slow, and cannot always be available in low budget handheld devices, depriving (or slowing down) financially lesser privileged users from participation in the CBDC economy; and (A_3) *Insufficient state management.* TPMs permit a small secure system state management, which could be insufficient for an offline token economy. Consider the case that the entire list of unverified token owners for the offline phase needs to be recorded for regulatory purposes: this cannot always be realizable in small state machine TPMs. A similar infeasibility exists for hardware security modules (HSMs) [17] in terms of scalable deployment, since they are hardware dependent and introduce unwanted latency (a fact corroborated as part of Project Sela [14]).

External hardware based authentication systems, like YubiKeys [18], which might be good candidates under requirements A_4 and A_3, would have at least two problems: (A_1) *Transaction execution overhead.* Connecting YubiKey hardware for every transaction (high or small in value) would be cumbersome and would significantly decrease the throughput of the token economy; and (A_2) *Deployability at scale.* YubiKey-like hardware authentication devices could be potentially incompatible for low budget handheld devices.

	Ease of deployment	Scalable deployment	Large state machine	Secure deployment
TPMs	✓	✗	✗	✓
YubiKeys	✗	✗	✓	✓
TEEs	✓	✓	✓	*moderate*

Fig. 1. Comparison of System Architectures

We now consider trusted execution environments (TEEs), under our four system requirements. TEEs, unlike TPMs, HSMs, and YubiKeys, pass the bar on all requirements A_1, A_2 and A_3. Although TEEs are prone to vulnerabilities, casting some doubts on A_4, which we discuss in Section V-A, their other advantages on deployment outweigh this deficiency.

Consequently, the best way to design a scalable and reliable token based digital currency system is to make the system realizable with commodity commercial solutions for computation, which makes trusted execution environments the natural choice for deploying CBDC specific computation. An equivalent but independent analysis on the viability of TEEs for CBDC systems was conducted in [6], [7]. We summarize our comparison in Figure 1.

B. The CBDC System Model

We detail next, ideal system modeling choices related to the protocol Π.

Retail CBDC: The Stakeholders. We assume that the central bank delegates a set of commercial banks or equivalent financial institutions as *maintainers* $\mathcal{M}$ executing the protocol Π for wallet state and token state verification. Given the jurisdiction where the protocol Π is deployed, we refer to the citizens of the jurisdiction that utilize the digital currency for retail purposes as *users*.

Tokens as (Computational) Legal Tenders. We assume that Π enforces a token based CBDC economy: the legal tenders in circulation replicate bank notes in the form of digital tokens (which are bit strings). Tokens are contained in digital wallets. Each token issued by the central bank contains at least three fields of interest: (i) the token *denomination* as determined by the central bank, which determines the worth of the token; (ii) the token *owner-list*, which specifies the user to which the legal tender is presently credited through some maintainer and the list of unverified owners from the offline phase, and is validated at the end of each offline phase by some maintainer; and (iii) the token *verification-fee-list*, which specifies the fee for the maintainer from the current (verified or unverified) owner of the token, for verifying each unverified transaction the token was a part of in the offline phase (this list can be empty in case Π dictates that central bank is ensuring the

incentivization of token verification, and not the owners).

Intermittently Offline [9] Token Verification. We assume tokens require periodic verification as per the specification of Π to ensure that the legal tenders in circulation are legitimate. There can exist bounded periods of time for which any user's wallet is offline but ready to transact and exchange tokens with other offline users.

Trusted Execution Environment [5] based Wallet State Verification. We assume that all protocol Π specific computation, memory and storage is deployed (distributively) among maintainers and users over trusted execution environments.

Incentivized Token Verification Prioritization Policies. The token state verification by a maintainer is incentivized for the maintainer, either through the central bank or its current owning user. The fee for token verification is some function of the current unverified state of the token.

Populous Nation [2]. We assume the protocol Π is deployed in a populous nation (which scales up both the honest and adversarial users in the system), of the order of hundreds of millions to a billion user wallets in operation.

C. Wallet State Verification Economy

We detail relevant economic properties to be considered for wallet state verification.

Incentivized Wallet Verification. Since the central bank delegated maintainers would be overburdened in performing wallet verification owing to scale constraints in populous nations, appropriate system design choice dictates that the verification process be incentivized by the central bank for the maintainers, as a function of the number of wallets verified.

A Cournot Duopoly. One appropriate economic model for the central bank under such settings is a Cournot competition [8]. Cournot games model competition between non-cooperative agents for the investment of a homogeneous good in a market, consistent with the law of supply and demand [19], and have been deployed for incentive compatibility in peer-to-peer systems [20], including blockchains [21]. A Cournot competition is more amenable over its closest alternate, the Bertrand competition [22], for a CBDC economy, as a Cournot game allows sellers to determine good quantities (which should be determined by users) instead of good prices in a Bertrand game (which should be determined by the central bank). Under a Cournot competition, the revenue per wallet for wallet verification by a given maintainer would decrease as the number of verified wallets increase. Given honest users $\mathcal{H}$ and adversarial users $\mathcal{A}$ leaking wallet states from victim users $\tilde{\mathcal{H}}$ ($\mathcal{A}$ and $\tilde{\mathcal{H}}$ may or may not intersect), if such a Cournot competition is deployed for wallet verification, the competition model reduces to a duopoly [8], where we consider that there would be $w_{\mathcal{H}}$ correct wallets passing verification and $w_{\tilde{\mathcal{H}}}$ compromised wallets passing verification. The payoffs for both types of users will be resultant of the joint protocol $(\sigma_{\mathcal{A}}, \Pi)$, and will be a function of the maximum revenue per verified wallet R, the number of each type of wallets verified, the cost for the maintainer of verifying each standard wallet c_{Π} (a function of the verification protocol Π) and that of leaking the private state of and verifying each compromised wallet $c_{\tilde{\mathcal{H}}} := c_{\tilde{W}} + c_{\Pi}$. Note that the cost of private state leak of the compromised wallet $c_{\tilde{W}}$ is borne by the adversary. Thus, the payoff functions for an arbitrary maintainer, as per the Cournot regime (for some specified demand slope k), given honest and adversarial users are:

$$\begin{aligned} u_{\mathcal{H}}(w_{\mathcal{H}}, w_{\tilde{\mathcal{H}}}) &:= (R - k(w_{\mathcal{H}} + w_{\tilde{\mathcal{H}}}))w_{\mathcal{H}} - c_{\Pi} w_{\mathcal{H}} \\ u_{\tilde{\mathcal{H}}}(w_{\mathcal{H}}, w_{\tilde{\mathcal{H}}}) &:= (R - k(w_{\mathcal{H}} + w_{\tilde{\mathcal{H}}}))w_{\tilde{\mathcal{H}}} - c_{\tilde{\mathcal{H}}} w_{\tilde{\mathcal{H}}} \end{aligned} \tag{1}$$

Note that the maintainer earns $u_{\mathcal{H}}(w_{\mathcal{H}}, w_{\tilde{\mathcal{H}}}) + u_{\tilde{\mathcal{H}}}(w_{\mathcal{H}}, w_{\tilde{\mathcal{H}}})$ from the central bank.

Wallet State Verification Equilibrium. Given the law of the invisible hand in a free market economy [23], the wallet verification CBDC system on operation over time will converge to a steady state which will maximize the payoff of the maintainer. That steady state will correspond to the Nash equilibrium $(w^*_{\mathcal{H}} = \frac{R - 2c_{\Pi} + c_{\tilde{\mathcal{H}}}}{3k}, w^*_{\tilde{\mathcal{H}}} = \frac{R + c_{\Pi} - 2c_{\tilde{\mathcal{H}}}}{3k})$ [8] under the above Cournot duopoly specification.

D. Token State Verification Mechanism

We will assume that each maintainer requires a fee for servicing each token on behalf of the central bank. Each maintainer maintains queues for tokens for their verification after the offline phase. The queues are prioritized according to one of the following three policies, which we believe are incentive compatible for maintainers.

M_1. *Token Ownership Length based Queues.* The maintainer will prioritize verification of tokens which have passed through most wallets (have most unverified owners from the offline phase). The token verification fee is based on the unverified ownership length and is provided by the central bank.

M_2. *Token Transaction Value based Queues.* The maintainer will prioritize verification of tokens which have the highest unverified cumulative offline transaction value. *We define the offline transaction value of a token as the denomination of the token times the number of unverified owners associated with it during the offline phase.* The token verification fee is based on the cumulative offline transaction value of the said token and is provided by the central bank.

M_3. *Token Transaction Fee based Queues.* The maintainer will prioritize verification of tokens which have the highest verification fee for the maintainer, associated with them. The token verification fee is provided by the user.

A Welfare-based Dynamic Posted Price Mechanism [10]. Dynamic posted price mechanisms are inspired from blockchain fee markets where limited block payload space must be auctioned off for transactions competing to go on-chain. In a dynamic posted price mechanism, there exists a base price $\mathcal{T}$ such that transactions that have a fee bid at least $\mathcal{T}$, are eligible to be considered to go on-chain by the block proposer. The transactions that go on-chain pay a fee of $\mathcal{T}$ units to the block proposer. The base price $\mathcal{T}$ is dynamic, in the sense that there exists an update rule for $\mathcal{T}$ for every auction, and that update rule is a function of the previous

base price and the fee bids of transactions going on-chain. More specifically, we consider the welfare-based dynamic posted price mechanism (WDPP). Given some $\mu \in (0,1)$, a block size of Q transactions, and a set txs of transactions going on-chain, the update rule of $\mathcal{T}$ under WDPP is given by:

$$\mathcal{T} \leftarrow \mu \times \frac{\sum_{\mathsf{tx} \in \mathsf{txs}} \mathsf{tx.bid}}{Q} + (1-\mu) \times \mathcal{T} \tag{2}$$

WDPP Equilibrium. It can be shown for certain regimes of bid values of transactions, there exist optimal choices for μ such that $\mathcal{T}$ is asymptotically stable (converges to a fixed point), and the revenue welfare of the block proposer at this stable point is no worse than $\frac{1}{2}$ of the revenue welfare of the block proposer under any ideal transaction fee mechanism. For details please see (Sec.5, [10]).

Applicability of WDPP for CBDC Token Verification. WDPP is an appropriate mechanism for token verification in an arbitrary CBDC protocol Π as it is incentive compatible for both the maintainers and the transacting users. We will denote the adoption of WDPP for CBDC token verification by Γ. In Γ, we make the following reduction from a blockchain system to a CBDC token economy: (i) block proposers will be replaced by maintainers, and blockchain users will be replaced by CBDC users; (ii) blockchain transactions are replaced by unverified CBDC tokens; (iii) transaction fee bids are replaced by a function of the unverified tokens (as per one of M_1, M_2 and M_3); and (iv) the base price for maintainers will again be a function of the tokens (as per one of M_1, M_2 and M_3).

III. The Ideal Adversary Model

The adversary, in the ideal case, can mount a full stack of a denial-of-service (DoS) attack without selfish financial interests in the attack[1]. The ideal stack that we consider is similar to the TCP/IP network stack (Link/Network/Transport/Application), except that the adversary can split the application layer to two sub-layers: the *system layer*, which specifies attacks based on how the CBDC system is deployed, and the *transaction layer*, which specifies attacks based on how the CBDC tokens exchanged are verified. The attack stack is outlined next.

1. Link Layer DoS. The adversary can jam the traffic at the MAC layer preventing p2p token exchange between honest wallet holders.

2. Network Layer DoS. The adversary can attack the origin IP address of honest wallet holders to misrepresent it outside the jurisdiction of the CBDC system, thereby introducing enough doubt in the mind of the maintainer to blacklist the associated wallet.

3. Transport Layer DoS. The adversary can introduce alternate competing flows with the maintainers with a high traffic volume so that honest wallet specific traffic is dropped.

4. System Layer DoS. The adversary can attack/breach the TEE associated with the deployment of the honest wallet and consequently compromise the integrity of the honest wallet.

5. Transaction Layer DoS. Depending on the post offline phase token processing policy of the maintainer, the adversary controlling some wallets of its own initiates redundant token exchanges at scale such that adversarial wallet specific token exchange verification is prioritized and honest wallet specific token exchange verification is delayed.

In this paper, we will only consider a specification (Section IV) and evaluation (Section V) for attacks 4 and 5, for an arbitrary CBDC protocol Π. We will also provide an outline for attacks 1, 2 and 3 (Section VI).

[1]We will discuss financial incentives as an alternate adversarial policy in Section VI.

IV. Denial of Token Service

We formalize the denial-of-service attacks on Π, on both its deployment and the associated token economy.

A. The System Layer

For the system layer denial of token service, we will give evidence that privileged information is extractable from TEEs (like keys in case of the Trusense attack [24]) which will lead to wallet state leak: private information associated with the wallet is compromised, requiring reinstantiation of the wallet by the maintainers.

We now detail the adversarial behaviour that can be considered for compromising wallets which pass verification under Π. We assume that there are honest users $\mathcal{H}$ who exchange tokens under un-tampered correct wallets, verifiable under Π. There are also *adversarial* users $\mathcal{A}$ who are willing to collude (under instructions from some adversarial entity with a common goal of inducing DoS), by generating compromised wallets through local or remote computation for victim users $\tilde{\mathcal{H}}$, that eventually pass verification under Π.

1) The TEE based Wallet Compromise Attacks.: We will give evidence later that TEEs are prone to attacks (Section V). Consequently, we consider that the probability to compromise a TEE according to a specified attack that leads to wallet compromise is $\tilde{p}_\sigma$ (> 0).

We consider a first attack on wallet state leakage.

Definition 1 (Attack $\tilde{W}_1$). *On a TEE breach, disclose some private state from the victim user's wallet to some maintainer* $\in \mathcal{M}$.

$\tilde{W}_1$ essentially negates the utilization of a specific wallet due to non-private state. Also, if the protocol Π specifies that each wallet must maintain a minimum balance of v_Π CBDC currency units, $\tilde{W}_1$ sets the baseline for the more severe attack presented next.

Definition 2 (Attack $\tilde{W}_2$). *On a TEE breach, disclose some private state from the victim user's wallet, to some maintainer* $\in \mathcal{M}$*, where the victim user's wallet has an enforced balance of at least* v_Π (> 0).

Note that for both $\tilde{W}_1$ and $\tilde{W}_2$, we assume that the victim user has his/her wallet compromised and so cannot verify any tokens correctly while claiming wallet state privacy with the maintainer, at the end of the intermittent offline phase.

2) The Adversarial Action Protocol.: Given wallet compromise attacks $\tilde{W}_1$ and $\tilde{W}_2$, we now show how the adversary can strategize to compromise the CBDC system.

DEFINITION 3 (Attack Protocol $\sigma_{\mathcal{A}}$). *All users $\in \mathcal{A}$ try to compromise a specific TEE individually according to a specified common attack. On a successful breach by at least one user $\in \mathcal{A}$ on said TEE, the successful user $\in \mathcal{A}$ leaks the compromised wallet state to some maintainer $\in \mathcal{M}$ according to $\tilde{W}_1$ or $\tilde{W}_2$. If the breach is unsuccessful, attempt another round.*

At the end of compromising the system and when the verification is due, we assume that the average cost per attack round of $\sigma_{\mathcal{A}}$ is $\tilde{c}_\sigma$. The expected number of rounds of $\sigma_{\mathcal{A}}$ for achieving success is $\frac{1}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}$ as per the geometric distribution. So the cost to generate a single compromised wallet under the attack $\tilde{W}_1$ is $c_{\tilde{W}_1} = \frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}$, and the cost to generate a single compromised wallet under the attack $\tilde{W}_2$ is $c_{\tilde{W}_2} = c_{\tilde{W}_1} - v_\Pi$. Finally, the cumulative cost to successfully generate and verify a single compromised wallet will be denoted by $c_{\tilde{\mathcal{H}}}$, and will be defined in the next section.

B. The Transaction Layer

For the transaction layer DoS attack, we will assume that $\mathcal{A}$ is a collusion of users under the control of state actors, which initiate token transactions among themselves based on the verification prioritisation policy of the maintainers (one of M_1, M_2 or M_3), to induce denial-of-service for honest token holders. We formalize this idea in the definition below.

DEFINITION 4 (Attack Protocol $\tau_{\mathcal{A}}$). *All users $\in \mathcal{A}$ identify the maintainers' token verification prioritization policy from Π. Then, all users $\in \mathcal{A}$ generate redundant CBDC transactions amongst themselves with transaction values, fees and ownership changes such that their tokens are prioritized in the maintainers' queues as per Π over any competing tokens.*

Note that the transactions generated by adversarial users amongst themselves are *non-retail*: there is no economic consequence for them as the associated tokens are not exchange for a quid-pro-quo for any commodity or asset. As opposed to this, the transactions generated by honest users with other honest users are *for-retail*: there is an economic consequence for them as the associated tokens are exchanged for some commodity or asset of value. Thus, we will consider the utility function for the adversary in mounting the denial-of-token-service as the ratio of (the total value of verified non-retail transactions and unverified retail transactions) to the total value of verified retail transactions.

V. EVALUATION

We now evaluate the implications of the denial of token service attacks on the CBDC system and token economy associated with Π.

A. TEE based CBDC Systems

We briefly discuss the susceptibility of TEEs to attacks, and then present the implications of mounting the attacks $(\{\tilde{W}_1, \tilde{W}_2\}, \sigma_{\mathcal{A}})$ on Π.

1) TEEs: Vulnerabilities and Attacks: TEEs in general are not short on vulnerabilities [25], [5]. There exist specific attacks on Intel SGX [26] and ARM TrustZone [27], [28] (a popular choice for handheld devices) such that the associated TEEs can be compromised with a certain probability (which we denote by $\tilde{p}_\sigma$). Key extraction is especially malicious as it can lead to disclosing private wallet state, and thereby enable attacks $\tilde{W}_1$ and $\tilde{W}_2$. As an example of a λ-bit AES key extraction attack, the TruSense exploit [24] targets ARM TrustZone cache event timing that succeeds with a non-negligible probability $\tilde{p}_{TS}$ to breach kernel access. Post breach, it takes a constant number of encryption query rounds to recover every fresh bit of the key, which implies that if the breach allows $r_{\lambda'}$ rounds of observation, thereby recovering λ' bits, $\tilde{p}_\sigma \geq \frac{\tilde{p}_{TS}}{r_\lambda \times 2^{\lambda-\lambda'}}$, which is non-negligible if $(\lambda - \lambda') \in O(\log \lambda)$. The exploit (Fig.5, [24]) shows that $r_\lambda = 3000$ for $\lambda = 128$. Moreover, the post kernel breach phase of TruSense succeeds in < 3 seconds. It has also been established more recently, that securing TEEs from TruSense-like attacks is computationally expensive, and so rather impractical [29], [30]. Another key extraction attack (dissimilar from this approach) exists for Intel SGX [31].

2) Failure Dynamics for the CBDC Wallets: In order to understand the trade-off between the number of compromised wallets and legitimate wallets in circulation as a consequence of both passing verification under Π, we analyze the wallet compromise factor $\sigma^*_W := \frac{w^*_{\tilde{\mathcal{H}}}}{w^*_{\mathcal{H}}} = \frac{R+c_\Pi-2c_{\tilde{\mathcal{H}}}}{R-2c_\Pi+c_{\tilde{\mathcal{H}}}}$ which determines the steady state quality of the CBDC economy induced by Π. The wallet compromise factor σ^*_W will vary under the different wallet compromise attacks $\tilde{W}_1$ and $\tilde{W}_2$. For $\tilde{W}_1$, we will denote the wallet compromise factor by $\sigma^*_{\tilde{W}_1}$, and similarly for $\tilde{W}_2$, we will denote the wallet compromise factor by $\sigma^*_{\tilde{W}_2}$. In the following arguments, we will show that there exists a measure σ^*, such that $\sigma^*_{\tilde{W}_2} > \sigma^*_{\tilde{W}_1} = \sigma^*$, and that in a very specific albeit practical case of the adversary mounting $\tilde{W}_2$, $\sigma^*_{\tilde{W}_2} \geq 1$.

Wallet Compromise Factor Measure. Section III shows that the expected cost to generate a single compromised wallet under either of the attacks $\tilde{W}_1$ or $\tilde{W}_2$ is upper-bounded by the function $\frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}$. Consequently, we consider and analyze the expression $\sigma^* = \frac{R-c_\Pi-2\frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}}{R-c_\Pi+\frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}}$. We parameterize the maximum revenue per verified wallet R and the average cost $\tilde{c}_\sigma$ per $\sigma_{\mathcal{A}}$ attack round as a linear function of the wallet verification cost c_Π, in order to study their relative effect on the factor σ^*. Under the setting $R = (\rho_R+1) \times c_\Pi, \tilde{c}_\sigma = \rho_{\tilde{c}_\sigma} \times c_\Pi$, please see the trends of σ^* as a function of $(\rho_R, \rho_{\tilde{c}_\sigma}, \tilde{p}_\sigma, |\mathcal{A}|)$, in Figure 2. We show next that σ^* is at least a lower-bound for both wallet compromise factors.

Wallet Compromise Factor under $\tilde{W}_1$. Given that no revenue apart from wallet verification is collected under $\tilde{W}_1$, it can be seen that $\sigma^*_{\tilde{W}_1} = \frac{R-c_\Pi-2c_{\tilde{W}_1}}{R-c_\Pi+c_{\tilde{W}_1}}$. Considering $\sigma^* = \frac{R-c_\Pi-2\frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}}{R-c_\Pi+\frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}}$ and since $c_{\tilde{W}_1} = \frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}$, it is true that $\sigma^*_{\tilde{W}_1} = \sigma^*$.

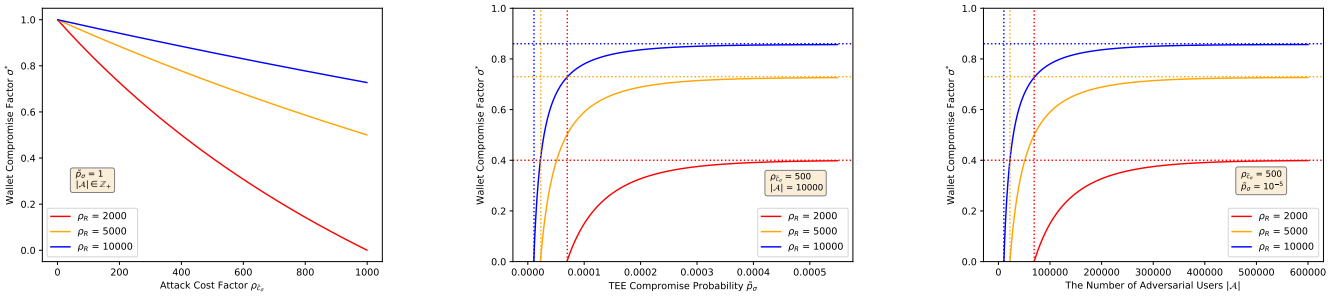

Fig. 2. LIMBOCOIN Evaluation (System Layer). (a) [Left] σ^* as a function of $\rho_{\tilde{c}_\sigma}$: As the maximum revenue for wallet verification increases, so does the wallet compromise factor. This implies there is a higher incentive for the adversary to compromise the system as the maximum revenue for wallet verification increases. (b) [Middle] σ^* as a function of $\tilde{p}_\sigma$: Considering a high verification revenue CBDC economy, the attack $\sigma_{\mathcal{A}}$ is feasible for $\tilde{p}_\sigma$ at least 1.1×10^{-5}, and σ^* maximizes at 0.86. Even for a low verification revenue CBDC economy, σ^* can reach 0.40. (c) [Right] σ^* as a function of $|\mathcal{A}|$: For a TEE compromise probability of at least $\tilde{p}_\sigma = 10^{-5}$, the attack $\sigma_{\mathcal{A}}$ is feasible for $|\mathcal{A}|$ at least 10536 (which is plausible in populous nations), given a high verification revenue CBDC economy.

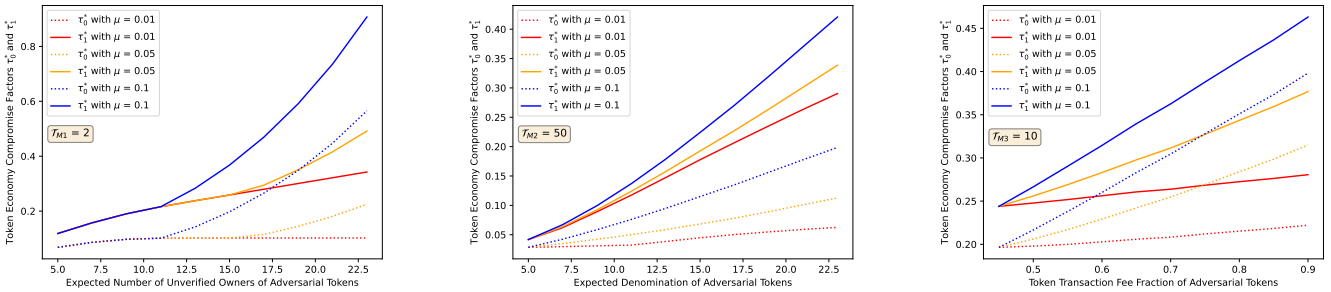

Fig. 3. LIMBOCOIN Evaluation (Transaction Layer). (a) [Left] τ_0^* and τ_1^* as a function of the number of unverified owners of adversarial tokens: For an aggressive verification threshold update policy by the maintainers, τ_1^* peaks at above 90 percent for 23 unverified adversarial owners in expectation. (b) [Middle] τ_0^* and τ_1^* as a function of the denomination of unverified adversarial tokens: For an aggressive verification threshold update policy by the maintainers, τ_0^* peaks at 20 percent and τ_1^* peaks at above 40 percent, given the expected denomination of adversarial tokens as 23 USD. In this case $v_{\mathcal{A}} \geq v_{\tilde{\mathcal{H}}}$. (c) [Right] τ_0^* and τ_1^* as a function of the fee fraction of unverified adversarial tokens: For an aggressive verification threshold update policy by the maintainers, τ_1^* peaks at above 40 percent if the adversary is willing to pay a fee above 90 percent of each transaction value.

Wallet Compromise Factor under $\tilde{W}_2$. Since $c_{\tilde{W}_2} = c_{\tilde{W}_1} - v_\Pi$ and $v_\Pi > 0$, we have $\sigma^*_{\tilde{W}_2} = \frac{R - c_\Pi - 2c_{\tilde{W}_2}}{R - c_\Pi + c_{\tilde{W}_2}} = \frac{R - c_\Pi - 2(c_{\tilde{W}_1} - v_\Pi)}{R - c_\Pi + (c_{\tilde{W}_1} - v_\Pi)} > \sigma^*_{\tilde{W}_1} = \sigma^*$. Furthermore, $\sigma^*_{\tilde{W}_2} \geq 1$ for $v_\Pi \geq \frac{\tilde{c}_\sigma}{1-(1-\tilde{p}_\sigma)^{|\mathcal{A}|}}$. This implies that *the number of compromised wallets in operation will be no less than the number of legitimate wallets in operation in the instance that the wallet specific profit made from compromising each wallet is at least the expected cost of mounting the attack $(\tilde{W}_2, \sigma_{\mathcal{A}})$ per wallet.*

B. WDPP based CBDC Token Transaction Verification

Simulation Setup. We will consider a fully flexible token economy in terms of denominations issuable from the central bank: every user can request any number of tokens of any positive denomination. We assume no regulatory cap on denominations, number and frequency of tokens exchanged during the offline phase. A single peer-to-peer transaction can consist of multiple token transactions that amount to the transacted value.

Token Verification Overhead. Contrary to account based systems, where only account states need to be verified for every peer-to-peer transaction, token based systems require the token state and associated wallet (sub-)states to be verified for each peer-to-peer transaction. This verification overhead limits the unverified token queue size that each maintainer can sustain. In our simulations, we model maintainers keeping this overhead in mind.

Adversarial Payoff. We will denote the total inconsequential non-retail value exchanged by adversarial users $\in \mathcal{A}$ by $v_{\mathcal{A}}$. We will denote the total consequential retail value exchanged by honest users which passes verification with a maintainer as $v_{\mathcal{H}}$. We will denote the total consequential retail value exchanged by honest users which goes unverified due to the adversarial strategy $\tau_{\mathcal{A}}$ as $v_{\tilde{\mathcal{H}}}$ (note that in this case $\mathcal{A}$ and $\tilde{\mathcal{H}}$ are strictly disjoint). As part of the LIMBOCOIN analysis, we will study the utility for the adversary to mount the denial-of-service through the functions: $\tau_0^* := \frac{v_{\tilde{\mathcal{H}}}}{v_{\mathcal{H}}}$ and $\tau_1^* := \frac{v_{\tilde{\mathcal{H}}} + v_{\mathcal{A}}}{v_{\mathcal{H}}}$.

Simulation Parameters. We will compute τ_0^* and τ_1^* under different attack policies of the adversary. We will average the results from $|\mathcal{M}| = 100$ maintainers, each of which maintains a token verification queue of $Q = 20,000$ tokens, under the WDPP mechanism. The statistical properties of honest

and adversarial tokens and wallets across all maintainers are identical. Per maintainer, there are 1000 honest wallets containing 20 tokens each. The denomination of each honest token is normally distributed with a mean value of 25 USD and a standard deviation of 5 USD. Per maintainer, there are 250 adversarial wallets containing 20 tokens each. The denomination of each adversarial token is normally distributed with a mean value of 5 USD and a standard deviation of 2 USD. We will vary the properties of the adversarial tokens as a function of the WDPP queuing strategy of the maintainers.

1) Token Unverified Owners' based Queues: We first consider token verification queues (type M_1) where the base fee of the maintainer (charged from the central bank) for validating each unverified token corresponds to 2 unverified owners per token, initially. For each token, honest or adversarial, we model the number of unverified owners per token under a normal distribution. For honest tokens, we fix the expected number of unverified honest token owners as 5 with a standard deviation of 3. For adversarial tokens, we vary the expected number of unverified adversarial token owners with a standard deviation of 3. The expected value of τ_0^* and τ_1^* as a function of the expected number of unverified owners of adversarial tokens is given in Fig.3(a). We see that for an aggressive base fee update rule by the maintainers, with $\mu = 0.1$, $\tau_1^* \geq 0.9$ asymptotically.

2) Unverified Token Transaction Value based Queues: We consider token verification queues (type M_2) where the base fee of the maintainer (charged from the central bank) for validating each unverified token corresponds to 50 USD unverified transaction value per token, initially. For each token, honest or adversarial, we model the denomination per token under a normal distribution. For honest tokens, we fix the expected denomination per token as 25 USD with a standard deviation of 5 USD. For adversarial tokens, we vary the expected denomination per token with a standard deviation of 3 USD. The expected value of τ_0^* and τ_1^* as a function of the expected denomination per adversarial token is given in Fig.3(b). We see that for an altruistic base fee update rule by the maintainers, with $\mu = 0.01$, $\tau_0^* \approx 0.2$ eventually.

3) Unverified Token Transaction Fee based Queues: Finally, we consider token verification queues (type M_3) where the base fee of the maintainer (charged from the user) for validating each unverified token corresponds to a 10 USD cumulative fee from the unverified transaction value per token, initially. For each token, honest or adversarial, we model the fee fraction of the unverified value per token deterministically. For honest tokens, the fee fraction of the unverified value per token is fixed at 0.1. For adversarial tokens, the fee fraction of the unverified value per token is varied progressively. The expected value of τ_0^* and τ_1^* as a function of the fee fraction of the unverified value per adversarial token is given in Fig.3(c). We see that for an aggressive base fee update rule by the maintainers, with $\mu = 0.1$, $\tau_1^* \geq 0.45$ asymptotically.

VI. Conclusion and Future Directions

Through this study, which is prescriptive in nature, we have attempted to show that the overheads for maintaining a token based CBDC economy can be exploited for denial-of-service attacks, and so considering and adopting account based CBDC systems might be more prudent. We end by outlining future directions for alternate attacks that can be mounted by an adversary which are independent of the specification of Π.

A. A Decentralized Adversary

The adversary $\mathcal{A}$ can also be deployed as a set of non-state actors operating as a private/permissioned anti-state decentralized autonomous organization (DAO) [32]. Since the sole aim of $\mathcal{A}$ is crippling the economy induced by Π for the associated jurisdiction, the private wallet state of victim CBDC users can be announced by $\mathcal{A}$, on the (dark) DAO distributed ledger. This distributed ledger can be used to run a bounty for black hat actors on the victim users' wallets ownership change, similar to bug bounties [33]. Considering HOTSTUFF [34] as a potential blockchain protocol to maintain such a distributed ledger, the adversary will require a worst case communication complexity of $O(f \times |\mathcal{A}|)$, while tolerating $f < \frac{|\mathcal{A}|}{3}$ Byzantine-faults in its permissioned DAO system.

The tradeoff of the cost for the adversary to maintain a replicated state of leaked wallet information, on the investment in compromising the CBDC system, can be considered as a future study.

B. A Utilitarian Adversary: Ransomware Attacks

Ransomware are particularly notorious as they have inflicted monetary losses to businesses and governments alike, causing damages in the worst case worth billions of US dollars [35]. Given that ransomware can lock out users from workstations and handheld devices allowing the victims to regain access to their systems in exchange for a fee, such malware can pose a threat to any CBDC system, independent of its specification.

C. Adversary at the Communication Layers

Link Layer DoS: Personal Area Network Vulnerabilities. The adversary can leverage standard DoS [36] attacks in Bluetooth to stall currency transfers between victim CBDC users.

Network Layer DoS: IP Spoofing. Adversarial state actors can spoof source IP addresses of victim users' CBDC network traffic, through a man-in-the-middle attack to reflect traffic origination from outside the CBDC's jurisdiction [37], [38], [39], invalidating the wallets' legitimacy.

Transport Layer DoS: Competing Transaction Flows. It is highly probable that every maintainer will provide financial services alternate to the CBDC system maintenance. The adversary can determine some viable alternate financial services where with minimum investment it can generate short-term TCP flows [40] to disrupt long-term TCP flows associated with CBDC maintenance traffic.

D. Alternate Economies and Mechanisms

In future, we can consider alternate economic models of non-cooperative duopolies (such as a Bertrand Competition [22]), and analyze the relative degree to which the CBDC wallet states are compromised in those settings. For token verification we can consider prioritization policies based on both latencies and bids [41], or models from multi-dimensional blockchain fee markets [42].

APPENDIX A
NOTATION

We provide a summary of the notation used throughout the paper, in Table I. We ignore the symbols used to reference results outside this paper.

Symbol	Definition
Π	A Token based CBDC Protocol
$\mathcal{M}$	Set of Maintainers
$\mathcal{H}$	Set of Honest Users
$\mathcal{A}$	Set of Adversarial Users
$\tilde{\mathcal{H}}$	Set of Victim Users
$w_{\mathcal{H}}$	Number of Valid Wallets
$w_{\tilde{\mathcal{H}}}$	Number of Compromised Wallets
R	Maximum Revenue per Verified Wallet
c_{Π}	Cost of Wallet Verification
$c_{\tilde{\mathcal{H}}}$	Cost of Generation and Verification of a Compromised Wallet
$c_{\tilde{W}}$	Cost of Leaking Private Wallet State
k	Cournot Demand Slope
$u_{\mathcal{H}}$	Payoff Function for Honest Wallet Holders
$u_{\tilde{\mathcal{H}}}$	Payoff Function for Victim Wallet Holders
$w^*_{\mathcal{H}}$	Number of Valid Wallets under Nash Equilibrium
$w^*_{\tilde{\mathcal{H}}}$	Number of Victim Wallets under Nash Equilibrium
μ	WDPP Convergence Parameter
$\mathcal{T}$	Base Fee from WDPP
Q	Maintainer Token Queue Size
Γ	Adoption of WDPP for CBDC Token Verification
$\sigma_{\mathcal{A}}$	System Layer Attack Protocol
$\tilde{p}_{\sigma}$	TEE Compromise Probability
$\tilde{c}_{\sigma}$	TEE Compromise Expected Cost
v_{Π}	Central Bank Enforced Minimum Wallet Balance
$\tilde{W}_1$	First Wallet Attack under $\sigma_{\mathcal{A}}$
$\tilde{W}_2$	Second Wallet Attack under $\sigma_{\mathcal{A}}$
$c_{\tilde{W}_1}$	First Wallet Attack Cost
$c_{\tilde{W}_2}$	Second Wallet Attack Cost
σ^*_W	Wallet Compromise Factor under W
$\sigma^*_{\tilde{W}_1}$	Wallet Compromise Factor under $\tilde{W}_1$
$\sigma^*_{\tilde{W}_2}$	Wallet Compromise Factor under $\tilde{W}_2$
σ^*	Wallet Compromise Factor
ρ_R	Wallet Revenue Factor
$\rho_{\tilde{c}_{\sigma}}$	Attack Cost Factor
$\tau_{\mathcal{A}}$	Transaction Layer Attack Protocol
$v_{\mathcal{A}}$	Verified Value exchanged by Adversarial Users
$v_{\mathcal{H}}$	Verified Value exchanged by Honest Users
$v_{\tilde{\mathcal{H}}}$	Unverified Value Exchanged by Honest Users
τ^*_0, τ^*_1	Token Economy Compromise Factors

TABLE I
LIMBOCOIN NOTATION

REFERENCES

[1] J. Clark, "Design handbook for central bank digital currencies," *Available at SSRN 3775045*, 2020.

[2] T. R. B. o. I. FinTech Department, "Concept note on central bank digital currency," *Available at: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CONCEPTNOTEACB531172E0B4DFC9A6E506C2C24FFB6.PDF*, October 2022.

[3] K. Wüst, K. Kostiainen, N. Delius, and S. Capkun, "Platypus: a central bank digital currency with unlinkable transactions and privacy-preserving regulation," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2947–2960.

[4] A. Kiayias, M. Kohlweiss, and A. Sarencheh, "Peredi: Privacy-enhanced, regulated and distributed central bank digital currencies," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 1739–1752.

[5] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/Ispa*, vol. 1. IEEE, 2015, pp. 57–64.

[6] Y. Chu, J. Lee, S. Kim, H. Kim, Y. Yoon, and H. Chung, "Review of offline payment function of cbdc considering security requirements," *Applied sciences*, vol. 12, no. 9, p. 4488, 2022.

[7] M. Christodorescu, W. C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu *et al.*, "Towards a two-tier hierarchical infrastructure: an offline payment system for central bank digital currencies," *arXiv preprint arXiv:2012.08003*, 2020.

[8] J. C. Cox and M. Walker, "Learning to play cournot duopoly strategies," *Journal of economic behavior & organization*, vol. 36, no. 2, pp. 141–161, 1998.

[9] I. S. Bank, "Project polaris: secure and resilient cbdc systems offline and online," *Available at: https://www.bis.org/about/bisih/topics/cbdc/polaris.htm*, Online; Accessed 07-Aug-2023.

[10] M. V. Ferreira, D. J. Moroz, D. C. Parkes, and M. Stern, "Dynamic posted-price mechanisms for the blockchain transaction-fee market," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 86–99.

[11] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Balancing accountability and privacy using e-cash," in *International conference on security and cryptography for networks*. Springer, 2006, pp. 141–155.

[12] E. Androulaki, J. Camenisch, A. D. Caro, M. Dubovitskaya, K. Elkhiyaoui, and B. Tackmann, "Privacy-preserving auditable token payments in a permissioned blockchain system," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 255–267.

[13] L. Mainetti, M. Aprile, E. Mele, and R. Vergallo, "A sustainable approach to delivering programmable peer-to-peer offline payments," *Sensors*, vol. 23, no. 3, p. 1336, 2023.

[14] H. K. Monetary Authority, "Project sela – an accessible and secure retail cbdc ecosystem," *Available at: https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2023/20230912e3a1.pdf*, Online; Accessed 14-Sep-2023.

[15] S. W. N. P. Ltd., "Apple iphone cbdc ssid app," *Available at: https://apps.apple.com/us/app/cbdc-ssid/id1625625229*, Online; Accessed 14-Sep-2023.

[16] S. L. Kinney, *Trusted platform module basics: using TPM in embedded systems*. Elsevier, 2006.

[17] M. H. Murtaza, H. Tahir, S. Tahir, Z. A. Alizai, Q. Riaz, and M. Hussain, "A portable hardware security module and cryptographic key generator," *Journal of Information Security and Applications*, vol. 70, p. 103332, 2022.

[18] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A tale of two studies: The best and worst of yubikey usability," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 872–888.

[19] D. Gale, "The law of supply and demand," *Mathematica scandinavica*, pp. 155–169, 1955.

[20] R. Gupta and A. K. Somani, "Game theory as a tool to strategize as well as predict nodes' behavior in peer-to-peer networks," in *11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, vol. 1. IEEE, 2005, pp. 244–249.

[21] J. Chiu and T. Koeppl, *Incentive compatibility on the blockchain*. Springer, 2019.

[22] M. Janssen and E. Rasmusen, "Bertrand competition under uncertainty," *The Journal of Industrial Economics*, vol. 50, no. 1, pp. 11–21, 2002.

[23] B. Ingrao and G. Israel, "The invisible hand," 1990.

[24] N. Zhang, K. Sun, D. Shands, W. Lou, and Y. T. Hou, "Trusense: Information leakage from trustzone," in *IEEE INFOCOM 2018-IEEE conference on computer communications*. IEEE, 2018, pp. 1097–1105.

[25] A. Muñoz, R. Ríos, R. Román, and J. López, "A survey on the (in) security of trusted execution environments," *Computers & Security*, vol. 129, p. 103180, 2023.

[26] S. van Schaik, A. Seto, T. Yurek, A. Batori, B. AlBassam, C. Garman, D. Genkin, A. Miller, E. Ronen, and Y. Yarom, "Sok: Sgx. fail: How stuff get exposed," 2022.

[27] F. Zhang and H. Zhang, "Sok: A study of using hardware-assisted isolated execution environments for security," in *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*, 2016, pp. 1–8.

[28] D. Cerdeira, N. Santos, P. Fonseca, and S. Pinto, "Sok: Understanding the prevailing security vulnerabilities in trustzone-assisted tee systems," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 1416–1432.

[29] S. Zhao, Q. Zhang, Y. Qin, W. Feng, and D. Feng, "Sectee: A software-based approach to secure enclave architecture using tee," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1723–1740.

[30] R. Bahmani, F. Brasser, G. Dessouky, P. Jauernig, M. Klimmek, A.-R. Sadeghi, and E. Stapf, "{CURE}: A security architecture with {CUstomizable} and resilient enclaves," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 1073–1090.

[31] W. Huang, S. Xu, Y. Cheng, and D. Lie, "Aion attacks: Manipulating software timers in trusted execution environment," in *Detection of Intrusions and Malware, and Vulnerability Assessment: 18th International Conference, DIMVA 2021, Virtual Event, July 14–16, 2021, Proceedings 18*. Springer, 2021, pp. 173–193.

[32] S. Hassan and P. De Filippi, "Decentralized autonomous organization," *Internet Policy Review*, vol. 10, no. 2, pp. 1–10, 2021.

[33] T. Walshe and A. Simpson, "An empirical study of bug bounty programs," in *2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*. IEEE, 2020, pp. 35–44.

[34] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus in the lens of blockchain," *arXiv preprint arXiv:1803.05069*, 2018.

[35] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," *ACM Computing Surveys (CSUR)*, vol. 54, no. 11s, pp. 1–37, 2022.

[36] S. Figueroa Lorenzo, J. Añorga Benito, P. García Cardarelli, J. Alberdi Garaia, and S. Arrizabalaga Juaristi, "A comprehensive review of rfid and bluetooth security: Practical analysis," *Technologies*, vol. 7, no. 1, p. 15, 2019.

[37] F. Ali, "Ip spoofing," *The Internet Protocol Journal*, vol. 10, no. 4, pp. 1–9, 2007.

[38] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[39] W. Jiang, B. Liu, C. Wang, and X. Yang, "Security-oriented network architecture," *Security and Communication Networks*, vol. 2021, pp. 1–16, 2021.

[40] S. Ebrahimi-Taghizadeh, A. Helmy, and S. Gupta, "Tcp vs. tcp: a systematic study of adverse impact of short-lived tcp flows on long-lived tcp flows," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2. IEEE, 2005, pp. 926–937.

[41] A. Mamageishvili, M. Kelkar, J. C. Schlegel, and E. W. Felten, "Buying time: Latency racing vs. bidding for transaction ordering," in *5th Conference on Advances in Financial Technologies (AFT 2023)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2023.

[42] T. Diamandis, A. Evans, T. Chitra, and G. Angeris, "Dynamic pricing for non-fungible resources: Designing multidimensional blockchain fee markets," *arXiv preprint arXiv:2208.07919*, 2022.