# **Abstract**

Event tickets being sold in their electronic instances are subject to counterfeiting, profiteering, and black markets. Therefore, suitable service management mechanisms are required to overcome such deficits. This work designs, develops, and evaluates the approach of a Decentralized Ticketing platform—called DeTi—for managing the distribution of electronic event tickets and “regulating” the aftermarket. DeTi offers a dedicated service management functionality by operating through Smart Contracts of Ethereum, such that users can verify tickets’ validity for a given event. Especially, a new mechanism for users to detect fraudulent events is introduced, too. The evaluation performed indicates that DeTi invalidates or validates tickets effi ciently via its decentralized and BC-based service management approach. By securing technically a set of underlying processes, DeTi obviates forging, replication, and scalping of tickets, allowing for a well-managed resale ecosystem of tickets based on and limited to the organizers’ initial pricing.

# **1 Introduction**

Today’s event ticketing industry has fundamental flaws. Existing systems for distributing tickets are open for arbitrage during the time the ticket is sold until the event happens. For example, Ed Sheeran’s “Benefit Concert” at Albert Hall (UK) in 2017 for the Teenage Cancer Trust was abused for heavy profiteering, where tickets with a fee value of 75 £ have been resold for up to 2330 £ [1]. Beyond the reputation and fairness concerns, the black market is also problematic due to fraud related to the ticket themselves. Tickets are often fake or have already been used, rendering them invalid. This means that besides the primary seller of the tickets (e.g., event organizer) intermediaries make a profit by buying, reselling, and counterfeiting tickets. Figure 1 illustrates today’s event ticketing landscape with its key actors and their interactions. Here, event organizers are “Hosts”. Event visitors are “Guests”, and the black market determines the concerns with respect to fraud, high reselling prices, and ticket scalpers scooping profits through it.

To tackle such major concerns, different centralized ticketing management services have been introduced in the past. However, since centralized approaches inherit the key deficit of being a single point of failure, this work here focuses on decentralized solutions for the management of ticketing, such as offering a Blockchain (BC)-based service management functionality on the application layer. BCs are distributed ledgers, which store data via a network of distributed nodes [2]. BCs establish a tamper-proof ecosystem by its nodes, i.e., miners. All users, i.e., BC clients, show equal write and read rights. Miners perform a set of actions to mine blocks of Transactions (TX). These actions are specified by the consensus mechanism defined for that BC. Various consensus mechanisms exist and are used by different BCs, such as Proof-of-Work (PoW) in Bitcoin and Ethereum, Proof-of-Stake (PoS) in Cardano and Algorand, or Byzantine Fault Tolerant (BFT) and its variations in Hyperledger, Ripple, and Stellar [3].

In the BC realm, the Ethereum BC has distinguished itself by enabling distributed autonomous computation, while enabling data storage in a distributed setting, too [2]. Ethereum started by a proprietary PoW-based consensus, but with higher scalability than Bitcoin. Ethereum introduced Smart Contracts (SC) as distributed applications developed like programs, i.e., written by programming languages, but run in a decentralized manner and accessing in a decentral manner data stored. The invention of SCs has been a linchpin for decentralized management and computation of many applications, which led to the emergence of many services [4], includ ing a decentralized ticketing management. BCs bring trust and transparency by their underlying cryptographic structure. However, such a decentralization, while preserving data with a high level of security, comes with various costs. For instance, PoW-based BCs suffer from scalability concerns with respect to low TX validation rates [5]. There exists also the user privacy concern with respect to the data being publicly available and not deletable. Another concern with using BCs is the cost of data storage.

The research questions to be answered in this paper are formulated as follows. (i) What are the requirements of ticketing platforms in order to prevent fraud and black markets. (ii) How BCs and SCs can be employed for addressing such requirements in managing presale, aftermarket, and identification processes. Therefore, this work studies user requirements to be addressed via a potentially reliable and secure ticketing platform, and collects key concerns experienced with existing ticketing platforms. Based on the collected information, this work proposes a novel decentralized ticketing management platform termed DeTi (Decentralized Ticketing Management Platform). DeTi approach’s novelty is briefed as follows.

• A presale logic which prevents front-running attacks and will not lead to sudden surges in gas prices and guarantees a fair distribution of tickets if the demand for an event is higher than its supply via a transparent and publicly available lottery approach.

• A trustless queue-based approach for aftermarket that enables buyers and sellers to transact with each other. Ticket scalpers have no scope of action in DeTi and they are prohibited on protocol level. Thus no black market is possible.

• Tickets cannot be sold for higher prices than their original price. • Enabling high flexibility in identity management such as incentivizing interested parties to act as Identity Approvers, whom would be used to identify guests.

• Enabling an economic incentive management that considers all the stakeholders in the ticketing business.

• Employing social trust certificates to create a decentralized layer of trust for higher trust than offered in current ticketing platforms.

The remainder of this paper is organized as follows. User requirements and deficits of current ticketing systems are discussed in Sect. 2 followed by Sects. 3 to 3.11 covering design specifications and implementation details of DeTi. Section 4 discusses the economic incentive management of DeTi. Section 5 discusses evaluation results, while covering a comparison of the related work and DeTi. Finally, Sect. 6 provides a summary of achieved goals.

# **6 Summary and Discussion**

DeTi addresses the requirements identified in Sect. 2 by the integrated and tightly coupled aftermarket logic. DeTi provides a novel function that is not available on ticketing platforms as of today. The proposed presale design guarantees a fair distribution if the demand for an event is higher than its supply. The lottery approach is transparent and publicly available. Furthermore, the presale logic prevents front running attacks and will not lead to sudden surges in gas prices. Furthermore, both the question of validity when buying a ticket from another user, and the inflated prices on tickets with high demand are addressed. The queuing-based architecture of aftermarket enables buyers and sellers to transact with each other. Also, there is no trust needed when exchanging a ticket on the aftermarket. A seller cannot trick buyers by not sending the ticket after receiving the money, since the SCs used guarantee that the ownership is only transferred if the correct amount of money is sent.

The architecture of the DeTi benefits all stakeholders in the system. Event guests profit from fair ticketing pricing, even on the aftermarket. Tickets cannot be sold for higher prices than the original cost of a ticket, since ticket scalpers have no scope of action and are prohibited on the protocol level. Event guests do not need to check whether a ticket for the same event is offered on any other platform, since they all connect to the same data. To prohibit scalpers from misusing the aftermarket DeTi verifies the identity of the guests and only verified accounts can buy tickets from the SC. This crucial part of identifying and approving the identity of a guest and linking the identity to an Ethereum address is done by the ID approver. As the identity SC is used to store the identities, every entity may act as an ID approver. Moreover, social trust certificates used in DeTi to create a layer of trust that is higher than in current online ticketing platforms without the need of a trusted third party. Aggregating ownership proofs across multiple social profiles in the event listing increases the legitimacy of an event. DeTi creates a new market for ID approvers, who are needed in a decentralized system, since there are no restrictions from creating a wallet and interacting with the platform. ID approvers are incentivized to act trustworthy since they are financially compensated if they are chosen by the event hosts.

As part of the future work, it is foreseen to reduce the fees for creating new instances of the same contract by using the proxy pattern e.g., as introduced in EIP1167 [26]. In addition, an analysis of loading times for the performance evaluation of the client-side caching mechanism when deployed on an Ethereum main net can provide real world verification of the DeTi’s performance, which is deemed worthy to consider as a future work. Finally, moving forward in adapting DeTi to newer generations of BCs such as Eth 2.0, employing a randomness models such as Beacon chain is one potential way to be considered