CrowdCtrl: A Decentralized System for Event Ticketing

Lilith Froude
lilith@crowdctrl.io
www.crowdctrl.io

Abstract. A purely peer-to-peer version of electronic ticketing would allow for event tickets to be issued, sold, and transferred directly from one party to another without going through a centralized ticketing service. Digital signatures provide part of the solution, but the main benefits of true ownership and control are lost if a trusted third party is still required to prevent ticket fraud and double-spending. We propose a solution to this problem using a peer-to-peer network that leverages blockchain technology. The network records transactions in a public history, cryptographically secured in an ongoing chain of blocks that is computationally impractical for an attacker to change. This chain serves as proof of the sequence of events, with consensus among network participants ensuring its integrity. A key innovation is the use of smart contracts, which embed programmable rules directly into the tickets themselves, allowing for automated royalty distribution, enforcement of resale policies, and elimination of scalping. The system is designed with an architecture that delivers the security benefits of the blockchain while providing a seamless, consumer-grade user experience, eliminating technical barriers for mainstream adoption.

1. Introduction

Commerce for live events has come to rely almost exclusively on large, centralized financial institutions serving as trusted third parties to process ticket sales. While this system functions, it suffers from the inherent weaknesses of a trust-based model. In the U.S. market, the largest primary ticketing company controls an estimated 60 percent or more of the market for primary ticket sales for most major concert venues. This market concentration limits consumer choice and venue flexibility.

The cost of mediation and infrastructure leads to exorbitant fees for consumers, which are often not transparent. These fees can add a significant amount to the face value of a ticket, with one analysis showing they average 27 percent of the ticket's price. This lack of transparency erodes trust and creates significant friction.

The entire ecosystem is plagued by issues, from the use of bots to acquire tickets for resale at inflated prices to the sale of fraudulent tickets. No mechanism currently exists to manage tickets over a communications channel without a trusted party who controls the entire process. What is needed is an electronic ticketing system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a centralized intermediary. A system where transactions are computationally impractical to reverse would protect both buyers and sellers from fraud.

In this paper, we propose a decentralized system for event ticketing using a peer-to-peer network to generate computational proof of the chronological order of transactions. We adopt a model for a peer-to-peer electronic system similar to that first proposed by Nakamoto for Bitcoin, but adapt it with novel mechanisms for the specific challenges of event ticketing. The system is secure, transparent, and restores control to the hands of event creators and their fans.

2. Transactions

We define an electronic ticket as a unique digital asset, represented as a chain of digital signatures. Each owner transfers the ticket to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding this information to the end of the ticket's data. A payee, or ticket holder, can verify the chain of signatures to verify the chain of ownership.

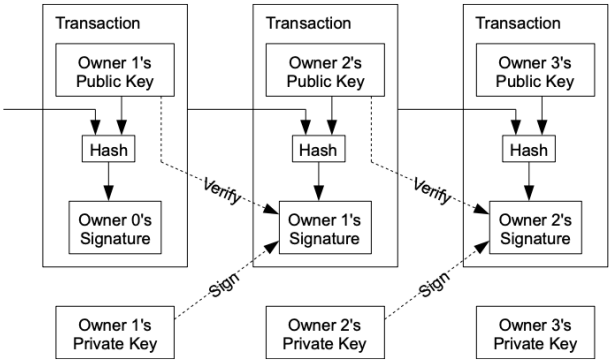

Figure 1: A ticket is a chain of digital signatures, showing the transfer of ownership. This concept is adapted from the work of Merkle (1980) and Haber & Stornetta (1991).

The problem, of course, is that a payee cannot verify that a previous owner did not double-spend the ticket—that is, sell the same ticket to someone else. A common solution is to introduce a trusted central authority (a "mint" or ticketing platform) that checks every transaction for double-spending. The problem with this solution is that the fate of the entire system depends on the company running it, with every transaction having to go through them, just like a bank.

We need a way for the ticket holder to know that the previous owners did not sign any earlier transactions. To accomplish this without a trusted party, transactions must be publicly announced. We need a system for all participants to agree on a single history of the order in which transactions were received. The payee needs proof that at the time of each transaction, the majority of network nodes agreed it was the first one received for that specific ticket.

3. The Network

The solution we propose begins with the concept of a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and publishing the hash. This timestamp proves that the data must have existed at that time. Each timestamp includes the previous timestamp in its hash, forming a chain where each additional timestamp reinforces the ones before it.

To implement this concept on a peer-to-peer basis, CrowdCtrl leverages the BASE blockchain's infrastructure. As an Ethereum Layer 2 (L2) network, BASE is designed to provide the security of a major blockchain while enabling high-volume transactions with minimal fees, which is critical for a consumer-grade ticketing system. Instead of relying on a central authority, the network allows participants to agree on a single, public history of transactions, effectively creating a distributed timestamp server. This public ledger provides the transparent and computationally secure proof needed to verify ticket ownership and prevent fraud.

The network operates by bundling new transactions, such as ticket creation or transfer, into blocks that are cryptographically linked together in a chronological chain. Each new block added to the chain reinforces the integrity of the entire history, making it computationally impractical for an attacker to alter past transactions. This process creates a secure and immutable public record of every ticket's lifecycle. By building on BASE, the system ensures that all participants can trust the sequence of events and verify the authenticity of a ticket without needing a centralized intermediary.

The network operates as follows:

1. New transactions (e.g., ticket creation, sale, transfer) are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. The block is submitted to the BASE network, where it is validated and consensus is reached.
4. Once finalized, the block is cryptographically added to the public chain, and all participating nodes update their copy of the ledger.
5. Nodes accept the block only if all transactions in it are valid (e.g., tickets are authentic and not already spent) and always work on extending the longest, most secure version of the chain.

This process creates a secure, chronological, and immutable public history of all transactions, solving the double-spending problem.

4. Smart Contracts

The core innovation of the CrowdCtrl platform is its use of smart contracts to redefine a ticket as a truly programmable digital asset. This aligns with the broader financial trend of asset tokenization, where real-world assets are represented as unique tokens on a blockchain. By tokenizing tickets, we unlock new models of digital ownership and value exchange that are transparent, efficient, and not possible in traditional systems.

Beyond solving for double-spending, the CrowdCtrl system introduces a layer of programmable logic directly into the tickets themselves using smart contracts. These are self-executing contracts with the terms of the agreement written directly into code. The rise of decentralized applications built on this technology is a key feature of the Web3 landscape. This allows CrowdCtrl to move beyond simple ownership verification to create a ticket with dynamic, enforceable rules.

Our smart contract architecture is built on the BASE blockchain and includes several core contracts:

1. TicketNFT (ERC-721 + EIP-2981): The contract for each ticket, which is a unique NFT that includes a standardized royalty protocol.
2. EventFactory: A contract that deploys event-specific rules for pricing, ticket supply, and royalties.
3. Marketplace: The contract that governs primary and secondary sales and automates fee distribution.

Key programmable behaviors include:

1. Resale Price Ceilings: Organizers can set a maximum price for which a ticket can be resold on the secondary market, effectively eliminating scalping.
2. Automated Royalty Distribution: A percentage of every secondary market sale can be automatically sent back to the original creator, artist, or venue. A fee is also directed to the platform.

3. Transfer Restrictions: Rules can be set to limit when or how a ticket can be transferred, such as locking transfers until 24 hours before an event.
4. Conditional Access: Tickets can be programmed to grant access to special perks or VIP experiences, with rules verified on the blockchain.

5. System Architecture and Interfaces

The CrowdCtrl platform is designed as a digital ecosystem accessible via web browsers and mobile applications. The architecture is modular, allowing for easy maintenance and scalability. The system comprises several key interfaces and components:

- **Interfaces**
  - **Marketplace UI:** The primary user interface, built with the Next.js framework, where users can perform event discovery and ticket purchasing.
  - **Venue App (PWA)**: A Progressive Web App for event staff to scan attendee QR codes , which validates ownership on the BASE blockchain and updates the ticket's redemption status.
  - **Customer Care Console:** An administrative backend that allows the CrowdCtrl team to attend to user queries, confirm ticket ownership, modify resell policies, and freeze tickets in cases of suspected fraud.
- **Operating Environment**
  - The platform leverages the BASE blockchain to facilitate transparent and secure transactions. Our choice of an efficient Layer 2 network is key to economic viability, enabling features like one-click USDC checkout with zero fees on BASE through Base Pay.
  - Integration with existing blockchain protocols and services enables users to interact with the system without requiring specialized knowledge.
  - High performance for features like event discovery is achieved by using Redis Cache on AWS, which stores frequently accessed data in a high-speed, in-memory system.

6. User Experience

A primary barrier to the adoption of many new technologies is poor usability. The design should ensure users can easily navigate the system and accomplish their goals without confusion. The CrowdCtrl platform is engineered to solve this problem by making the underlying blockchain technology effectively invisible to the end-user. This aligns with core usability heuristics, such as matching the system to the real world and providing a clean, minimalist design.

The user journey is designed to be as simple and familiar as any traditional e-commerce platform:

1. **Simple Sign-Up:** Users sign up with an email or social login using the Privy SDK, which automatically creates a secure Smart Wallet for them. This process abstracts away complexity and results in 70% fewer signatures for the user. As a fallback and to accommodate experienced Web3 users, additional wallet connectivity will be offered.
2. **Familiar Payments:** Tickets can be purchased easily with a standard credit or debit card. Behind the scenes, our system instantly converts the payment into digital currency on the BASE network using services like Base Pay and Coinbase Onramp, ensuring a seamless checkout. Direct cryptocurrency payments are also supported.

3. **Seamless Ownership:** Once purchased, the ticket (as an NFT) is deposited into the user's smart wallet. They can view, manage, and transfer their ticket through our user-friendly web or mobile interface, without ever needing to interact directly with the blockchain.

This "invisible blockchain" approach is critical for mass adoption. It delivers the powerful benefits of the technology—true ownership, security, and fraud prevention—without the friction that has hindered other platforms.

By solving these fundamental usability challenges, the CrowdCtrl platform provides the foundation for next-generation fan loyalty programs. The seamless user experience allows for the integration of Web3 mechanics—such as collecting digital memorabilia, earning rewards through participation, and accessing tiered experiences—without the friction that has hindered mainstream adoption. This transforms the ticket from a simple proof of entry into a gateway for deeper, more meaningful, and continuous fan engagement

7. Privacy and Security

The traditional banking model achieves privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly on a blockchain precludes this method. However, privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that a ticket was transferred from one address to another, but without additional information linking the address to a real-world identity, the transaction remains private.

A framework for responsible digital transformation should include a focus on security and data protection by design. The security for the CrowdCtrl system is multi-layered to align with these principles:

1. Network and Smart Contract Security: We leverage the robust security of the BASE blockchain, which is built as an Ethereum Layer 2. This architecture is fundamentally secure because it allows BASE to inherit the full security and decentralization of the main Ethereum network, which serves as its ultimate settlement layer. All transaction data is anchored to Ethereum, meaning our system is protected by the work of thousands of globally distributed validators. Our smart contract architecture is built using battle-tested open standards like ERC-721 for the tickets and EIP-2981 for royalty payments. By using these widely-audited standards, we minimize the risk of introducing common vulnerabilities.

   Furthermore, the architecture of the Ethereum Virtual Machine (EVM), which BASE utilizes, ensures that transactions are atomic. This means that complex operations—such as a ticket sale that must simultaneously pay a seller, distribute royalties to an artist, and send a fee to the platform—are bundled into a single, all-or-nothing transaction. This entire bundle will either succeed completely or fail entirely, leaving no trace on the blockchain if it fails. This prevents the system from ever being left in an inconsistent or exploitable intermediate state. This fundamental feature provides powerful, built-in guarantees for the financial integrity of every sale on the platform.

2. User Authentication: We use modern identity management solutions like the Privy SDK to manage secure user sessions and access. We do not store any user private keys, which could compromise their assets.

3. Compliance and Audits: We will implement Know Your Customer (KYC) verification for all registered event promoters to comply with financial identification requirements. All smart contracts will be thoroughly audited by third-party security firms before they are deployed for commercial use to ensure they are free from vulnerabilities.

8. Conclusion

We have proposed a system for electronic transactions in the event ticketing space that does not rely on trust. We started with the framework of tickets as digitally signed assets, which provides strong control of ownership but is incomplete without a way to prevent fraud and double-spending. To solve this, we proposed a peer-to-peer network using the BASE blockchain to record a public history of transactions, which quickly becomes computationally impractical for an attacker to change.

The network is robust in its unstructured simplicity. We have extended this model with smart contracts that represent tickets as ERC-721 NFTs, which enforce programmable rules and incentives, such as resale price caps and automated EIP-2981 royalties, directly on the blockchain. By combining this powerful backend with a user-friendly interface that abstracts away all technical complexity using tools like Privy and Base Pay, we have created a system that is both secure and accessible to a mainstream audience.

This creates a transparent, efficient, and creator-controlled ecosystem that stands in stark contrast to the centralized, extractive model that defines the ticketing industry today.

References

Bobrova, P., & Perego, P. (2025). The Development of User-Centric Design Guidelines for Web3 Applications: An Empirical Study. *Computers*, *14*(2), 46. https://doi.org/10.3390/computers14020046

Boston Consulting Group. (2023). *Web3 opens new paths to customer loyalty*. https://www.bcg.com/publications/2023/web3-customer-loyalty-program-opportunities

Haber, S., Stornetta, W.S. How to time-stamp a digital document. *J. Cryptology* 3, 99–111 (1991). https://doi.org/10.1007/BF00196791

R. C. Merkle, "Protocols for Public Key Cryptosystems," 1980 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 1980, pp. 122-122, doi: 10.1109/SP.1980.10006. keywords: {Protocols;Public key;Encryption;Authentication;Contracts},

Nielsen Norman Group. (2022). *Usability heuristics for user interface design*. https://www.nngroup.com/articles/ten-usability-heuristics/

U.S. Government Accountability Office. (2018). *Event ticket sales: Market characteristics and consumer protection issues* (GAO-18-347). https://www.gao.gov/products/gao-18-347

World Economic Forum. (2025). *Asset tokenization in financial markets: The next generation of value exchange*. https://reports.weforum.org/docs/WEF_Asset_Tokenization_in_Financial_Markets_2025.pdf