École Polytechnique Fédérale de Lausanne

Blockchain-based Event Ticketing

by Michael Gysel

Master Thesis

Prof. Bryan Ford
Thesis Advisor

Louis-Henri Merino
Thesis Supervisor

EPFL IC IINFCOM DEDIS
BC 160 (Bâtiment BC)
Station 14
CH-1015 Lausanne

August 18, 2023

Contents

Part I

Introduction

Event Ticketing is a $78 Billion industry globally, with the secondary ticket market accounting for $19 Billion of this [12]. However, event organizers have no control over the secondary ticket market and attendees experience high rates of ticket fraud. In fact, Ticketmaster estimates that bots siphon off 60% of tickets for major events that are then resold at higher prices. Event organizers have no control over these secondary ticket prices and see none of the resale value [3]. Furthermore, 12% of adults in the United States have purchased fraudulent tickets online, creating a lack of trust in the secondary ticket market [7]. Thus, the inability of event organizers to control the secondary ticket market for their own events and the inability of attendees to trust the secondary ticket market both present major challenges in existing event ticketing systems.

Part 2 presents the business objectives of NFTickets, a proposed blockchain-based event ticketing system with the goals of giving event organizers control over the secondary ticket market and reducing fraudulent ticketing. The business use-case was developed through several business objectives. These include interviews and surveys conducted to better understand event organizers and attendees, event ticketing market research, competitor benchmarking, business model development, financial analysis, and steps taken to find potential customers and seek funding for further development.

Part 3 presents the academic objectives of this blockchain-based event ticketing system. An identification system and ticket market were developed to increase event organizer control over the secondary ticket market and reduce fraudulent ticketing. Several academic objectives were conducted, including designing, implementing, and evaluating the system, assessing a threat model, discussing limitations, and discussing future research needed.

Finally, Part 4 presents concluding remarks for the business and academic findings in this report.

Part II

Business

Chapter 1

Introduction

NFTickets is a proposed blockchain-based event ticketing company whose business use case was developed.

NFTickets proposes the use of event tickets as non-fungible tokens (NFTs), where each NFT corresponds to an event ticket on a blockchain. NFTs are unique digital identifiers recorded on a blockchain; moreover, NFTs can be used to certify ownership of physical or digital objects such as event tickets. Not only can NFTs aid in secondary market control and ticket fraud reductions, but can also be used to encode other information such as digital art and for novel forms of advertising to event attendees.

Several business objectives were completed to better understand how NFTickets can be developed into a viable business. In what follows, event organizer interviews and event attendee surveys are summarized in Chapter 2. Chapter 3 benchmarks existing competitors, including those event ticketing companies with the largest market share as well as blockchain-based event ticketing companies. Chapter 4 presents an analysis of the event ticketing market and the most advantageous segment in which to operate. Chapter 5 presents the business model through the use of the business model canvas to gain a better understanding of the most significant challenges and opportunities in building a blockchain-based event ticketing company. Chapter 6 presents a break-even analysis which includes detailed revenue and cost projections. Chapter 7 overviews steps taken to find NFTickets' initial customers and potential funding sources. Finally, Chapter 8 summarizes the key findings of this business analysis.

Chapter 2

Customer Interviews

This section presents the results of interviews conducted with 19 event organizers and surveys conducted with 40 event attendees. These interviews and surveys were conducted to better understand the issues faced by both event organizers and attendees with regard to event ticketing.

2.1 Event Organizers

Interviews were conducted with 19 event organizers ranging from small (less than 1,000 attendees), medium (between 1,000 and 2,000 attendees), and large-sized event organizers (greater than 2,000 attendees); to European and American event organizers; to technical, music, and sporting event organizers. While music and sporting market segments are commonplace, technical events refer to small events, exhibitions, and conferences focusing on topics such as business, science, education, and other professional topics.

The event organizers interviewed, including their event size and event type can be seen in Figure 2.1. Throughout these interviews it was learned that over 90% of event tickets sold are digital, whereas technical events typically sell digital-only tickets. Secondly, large events and technical events of any size often link event tickets to user identification, unlike other markets. Furthermore, approximately 58% of event organizers either currently check or are willing to check attendee identification at the event entrance. As described in greater detail below, the challenges faced by large event organizers substantially differ from those faced by small or medium-sized event organizers.

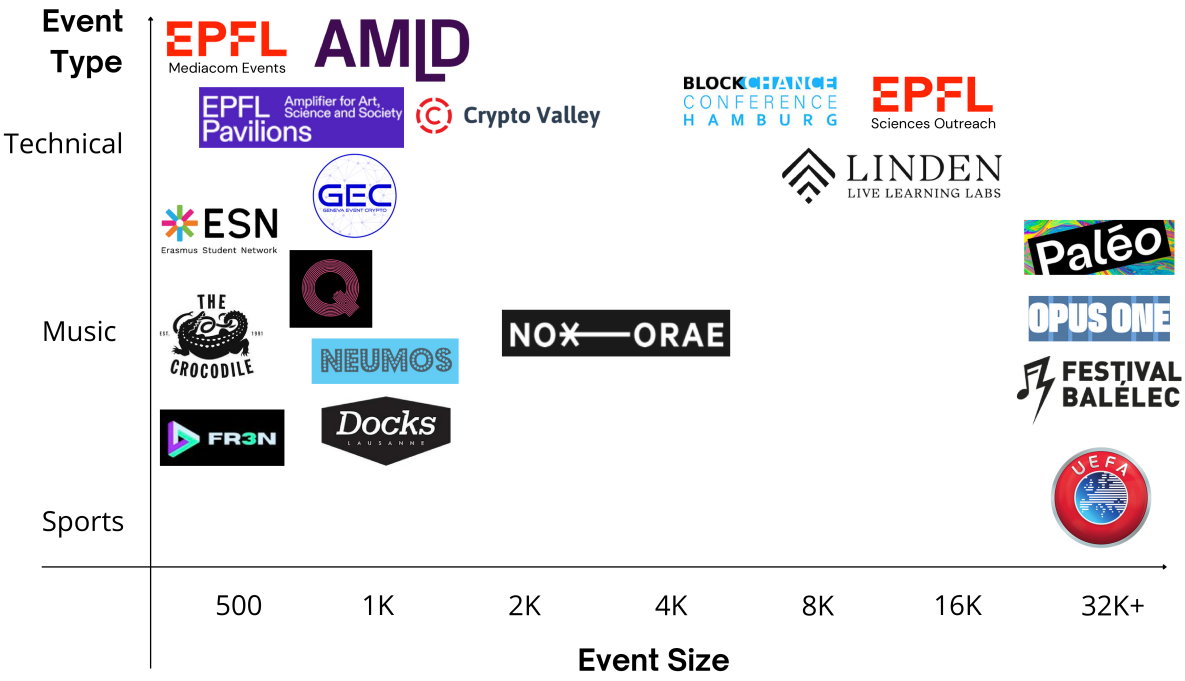


Figure 2.1: Event Organizers by Event Size and Event Type

2.1.1 Large Event Organizers

For the 9 large event organizers interviewed, lack of control over the secondary ticket market and fraudulent ticketing were viewed as major issues that are not adequately addressed. A variety of methods have been attempted to combat secondary market ticketing issues, such as limiting the number of tickets per person, activating ticket barcodes near the event, and finding patterns to blacklist users who buy many tickets through several accounts. A variety of methods have also been attempted to combat fraudulent ticketing issues, such as limiting ticket sales to specific points of sale and educating users on where to buy authentic tickets. Despite these efforts, the secondary market and fraudulent ticketing issues remain.

From these interviews, it was also learned that supporting large event organizers requires significant costs. Firstly, a large staff is required to support the thousands of event attendees and any issues they face at the event. For example, UEFA stated their event ticketing team consists of 30 full-time staff that balloons to 200 during the season. This staff handles all edge cases during the event, such as issues accessing tickets, lost tickets, and lost mobile phone connections on-site. Secondly, these events often entail tens of thousands of attendees all purchasing tickets simultaneously and then all using tickets simultaneously at the event. Thus, serving these customers requires costly and highly scalable event ticketing systems. Lastly, several large-sized event organizers use custom applications built for their events that don't just provide event ticketing services but also fan information, fan activities, and hospitality services. Thus, serving large event organizers often requires building customized applications for each.

2.1.2 Small to Medium-Sized Event Organizers

For the 10 small and medium-sized event organizers, secondary ticket market and fraudulent ticketing were rarely viewed as significant issues. This is due to the fact that small and medium-sized event organizers rarely experience ticketing demand that elicits large secondary ticket markets or fraudulent tickets being sold. Furthermore, if event ticketing demand is expected to be much larger than the venue capacity, a larger venue is typically used.

Despite this, small and medium-sized event organizers commonly cited facing three significant issues: growing their audience, engaging customers after events, and high fees from event ticketing companies. Audience growth was deemed by far the most significant factor when choosing an event ticketing service, as event ticketing services with large audiences can significantly impact event attendance, and thus event organizer revenue. For example, Nox Orae uses the event ticketing non-profit Petzi because they have grown a large audience that perfectly matches Nox Orae's customer base. Secondly, event organizers struggle to engage customers after their events but have attempted to use customer relationship management tools, email lists, and classic marketing campaigns such as online, newspaper, and email advertisements. Crypto Valley Association for example, has built a strong network of business and technical experts and created a wide range of educational tools; however, attempts to productively connect these users after events have remained a challenge. Lastly, event organizers are often faced with little choice but to use large event ticketing companies with exorbitant fees. For example, Les Docks has used SeeTickets, which charges a fixed fee, a fee on each ticket, and then an additional fee paid by the customer when purchasing the ticket. Furthermore, it is not uncommon that fees are miscalculated, which Les Docks must manually check and correct each event.

2.2 Attendees

A survey of 40 event attendees was conducted to gain a better understanding of issues event attendees face with event ticketing. While attendees are not the customer, they are the event ticket users and thus an important group to consider when designing an event ticketing system. The key survey findings can be seen in Figures 2.2 and 2.3.

As can be seen, event attendees encounter major issues with existing event ticketing services. The most common issues faced are the inability to buy event tickets to sold-out events, losing or failing to receive a ticket, and ticket fraud. Specific to secondary market ticketing, attendees commonly find secondary market tickets to be too expensive, are unable to find buyers or sellers, and do not trust secondary market sellers. Furthermore, 80% of respondents stated they have no issues with using digital-only tickets, though this leaves a substantial percentage of respondents who prefer paper tickets.

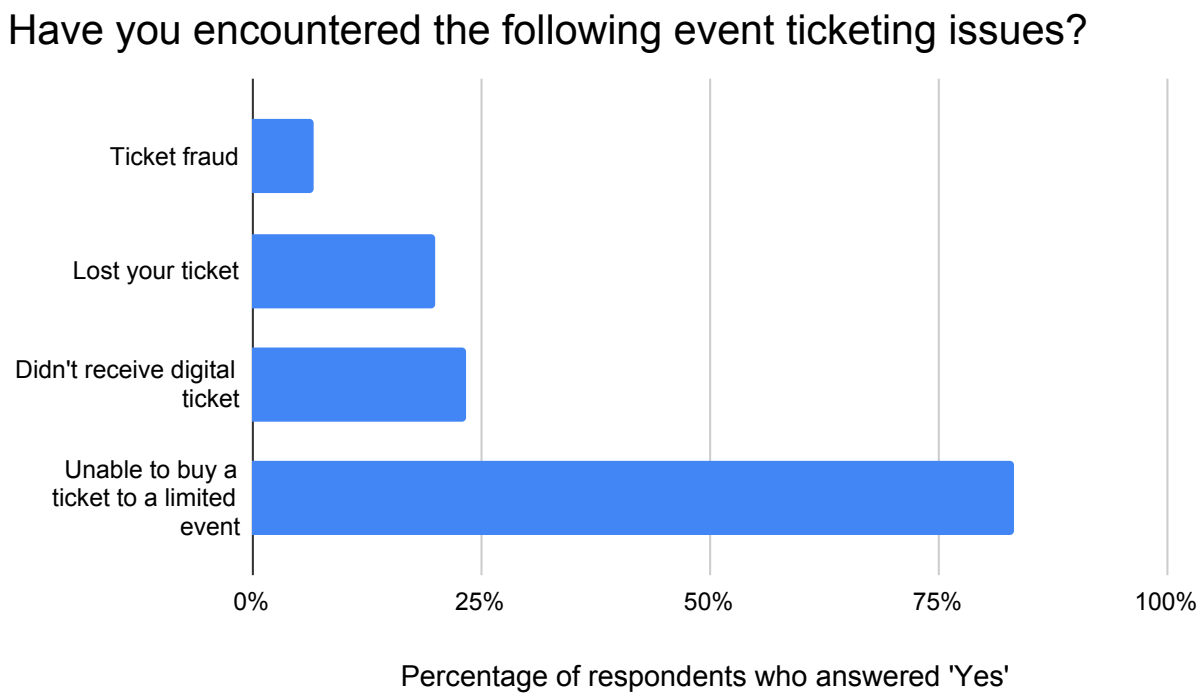


Figure 2.2: Event Ticketing Issue Survey Responses

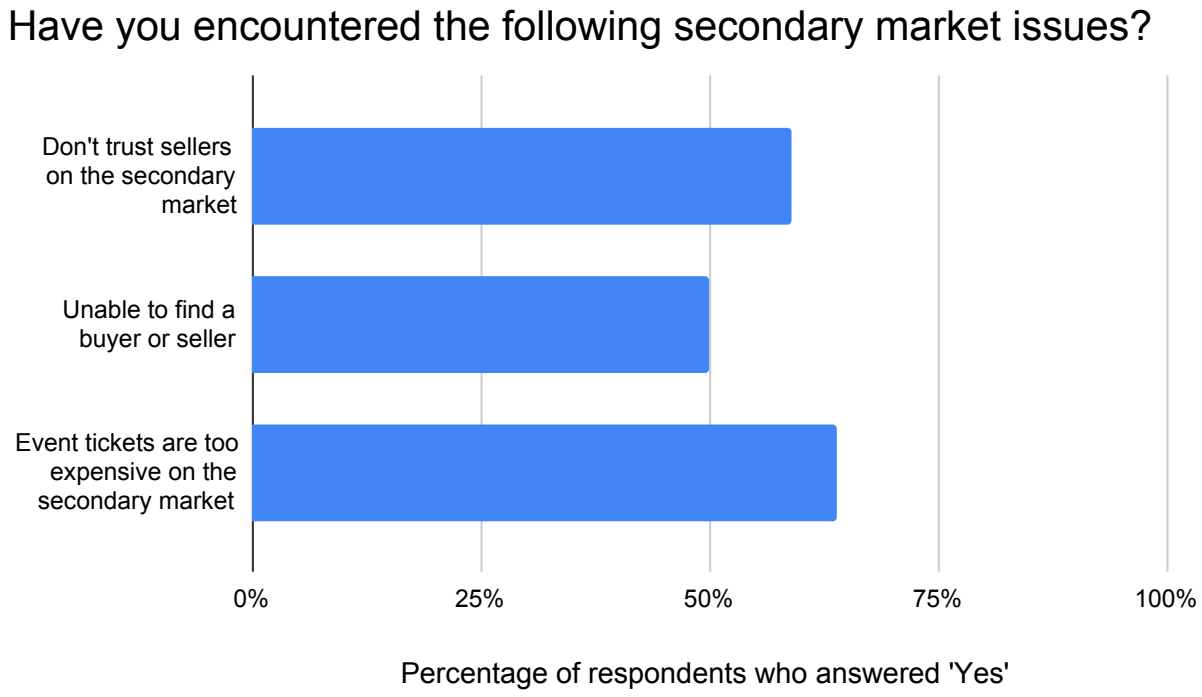


Figure 2.3: Secondary Market Issue Survey Responses

Chapter 3

Benchmarking

To better understand event ticketing competition, several competitors were benchmarked in terms of their product offering, value proposition, technology used, market segment, company size, and pricing. This was assessed for top competitors in the event ticketing industry and top competitors specifically in blockchain-based event ticketing. Figure 3.1 shows these event ticketing competitors by value proposition and cost as a percentage of ticket price.

Figure 3.1: Event Ticketing Competitors by Value Proposition and Price

3.1 Event Ticketing Companies with Largest Market Share

The event ticketing companies with the largest market share commonly provide attendees with a web and phone application to search for events, buy, and use event tickets and provide event organizers with a reporting dashboard, marketing tools, and data analytics tools to create and manage events. The value proposition of these competitors focus on marketing and data analytics tools, as these can improve event organizer ticket sales and thus increase their revenues. These marketing and data analytics tools are significant advantages for existing competitors as they have grown large user bases over decades of operation. These competitors serve a variety of event sizes and locations; however, they nearly all focus on music and sporting events, ignoring technical events altogether. Typically, these event ticketing companies charge several different fees ranging from 10% to 30% of the ticket price that are split between event organizers and attendees.

3.2 Blockchain-based Event Ticketing Companies

The blockchain-based event ticketing companies typically provide attendees with a web and phone application to buy and use event tickets and provide event organizers with a reporting dashboard to create and manage events. Furthermore, a variety of blockchains are used, including Ethereum, Polygon, Tezos, and private blockchains. The value propositions for these competitors typically focus on either increasing event organizer control over the secondary ticket market and reducing ticket fraud, or engaging attendees after the event. As these competitors are much smaller in size, they often serve small and medium-sized events throughout Europe and North America. Furthermore, they focus on music, comedy, art, and metaverse events, while largely ignoring technical events. These competitors typically charge several different fees set around 10% of the ticket price, including per-ticket fees, ticket resale fees, and subscription fees.

Chapter 4

Event Ticketing Market

This section analyzes the various event ticketing market segments and determines the most advantageous market segments in which to operate.

4.1 Market Segmentation

The event ticketing industry is a $78 Billion industry globally with primary market ticketing accounting for $59 Billion and secondary market ticketing accounting for $19 Billion [12]. As shown in Table 4.1, sporting events account for $22.2 Billion, music events $17.4 Billion, cinema $14.8 Billion, technical events such as exhibitions and conferences $11.6 Billion, festivals $7.7 Billion, and other events $4.3 Billion of total revenue. Furthermore, North America and Europe account for 67% of total event ticketing revenue globally [10]. While the event sizes for each market segment are unknown, approximately 85% of music events have an audience capacity below 1,000 while 15% of music events have an audience capacity greater than 1,000 [2]. It is also important to note that while cinema tickets account for $14.8 Billion of event ticketing revenue annually, cinema event ticketing is predominantly controlled in-house.

Market Segment	Size (in $Billions)
Sports	22.2
Music	17.4
Cinema	14.8
Technical	11.6
Festivals	7.7
Other	4.3

Table 4.1: Global Annual Revenue of Event Ticketing Market Segments

4.2 Go-To-Market Strategy

The decision was made to focus on serving small and medium-sized technical events and conferences in the short-term and focus on large-sized events in the long term.

In the short-term, small and medium-sized technical events are chosen as the target market because they are underserved by existing event ticketing companies, frequently use digital-only ticketing and check attendee identification, require relatively low scalability, and are the most likely user group to understand the benefits of blockchain-based event ticketing. Of the 19 competitors benchmarked, nearly all focus on serving music and sporting events. Thus, while competitors such as LiveNation and CTS Eventim have significant advantages in growing event organizer reach for music and sporting events, this advantage applies little to technical event ticketing. Secondly, nearly every technical event organizer interviewed uses digital-only ticketing and checks identification upon entrance. Thus, the event ticketing system prototype discussed in the academic section of this report could be used to serve these customers with little modification. Furthermore, small and medium-sized technical events are likely to understand the benefits of blockchain-based event ticketing and thus initially use it. For example, Blockchance GmbH was interviewed to discuss event ticketing for their annual conference that attracts approximately 5,000 attendees throughout the blockchain space. While Blockchance GmbH does not currently use a blockchain-based event ticketing system, they are likely to switch as blockchain technology is of interest to them and to their attendees. Lastly, small and medium-sized technical events do not require dozens of staff on-site or tens of thousands of customers buying tickets simultaneously. Thus, while many of these technical conferences have thousands of attendees, serving them would result in comparatively lower costs that a startup can afford.

In the long-term, large-sized events are chosen as the target market because these events most benefit from improvements in secondary market control and reductions in fraudulent ticketing. Large-sized events are not chosen as the initial target market due to the large costs

necessary in serving them. Scalable systems that allow tens of thousands of event tickets to be purchased simultaneously as well as dozens of ticketing staff would be required to serve large-sized events; however, this would be cost-prohibitive in the initial stages of a startup with few resources. Once the event ticketing system has been tested and improved on smaller events and event ticketing staff is increased however, it can be used to significantly improve large-sized event ticketing services. While the event ticketing companies with the largest market share maintain advantages in data analytics and marketing tools, none have implemented adequate mechanisms to improve secondary market control and reduce fraudulent ticketing. Thus, the proposed blockchain-based event ticketing system can be used to solve major issues for large-sized event organizers that are currently unaddressed.

Chapter 5

Business Model

This section presents the proposed business model through the business model canvas which was used to gain a better understanding of the most significant challenges and opportunities in building a blockchain-based event ticketing company. The business model canvas overviews the key partners, key activities, key resources, value propositions, customer relationships, customer segments, channels, revenue streams, and cost structure.

5.1 Key Partners

The key partners consist of event organizers and media relationships. Initially, this would focus on technical event organizers and media that cover such events and conferences; moreover, long term this would expand to focus on large-sized event organizers and media that cover such events. Media relationships would be particularly important in the early stages to gain free marketing and visibility when financing is low.

5.2 Key Activities

The key activities involve technical development of web and mobile applications where event organizers can create and monitor events and attendees can buy, resell, and use event tickets. This technical development includes scalably developing the decentralized systems such as the identification system and event marketplace. Secondly, relationships with technical event organizers must be further developed to expand the customer base. Marketing these events is also of great importance, as small and medium-sized event organizers consistently state that expanding their audience is the most important factor in choosing event ticketing systems.

5.3 Key Resources

The key resources include the technical team, which includes web and mobile application developers as well as decentralized systems developers for the identification system and event market. Furthermore, a business team is also needed to build relationships with technical event organizers, market events, and further develop business opportunities.

5.4 Value Propositions

In the short-term, the value proposition for small and medium-sized technical event organizers includes building a targeted marketplace for technical events and engaging audiences after the event. Focusing on technical events would allow NFTickets to build a specific audience base that can then be used to expand the audience of technical event organizers. Because technical events are rarely the focus of existing event ticketing companies, their existing advantages in marketing and data analytics tools least apply in this market segment. Secondly, NFT event tickets would allow NFTickets to engage audiences after the event in unique ways, particularly with blockchain-focused conferences that attract blockchain enthusiasts and artists. For example, NFTickets could partner with NFT artists to encode their artworks in the tickets themselves. Novel marketing methods such as NFT Airdrops, which refers to the sending of NFTs to select individual wallets, can also be leveraged to engage these blockchain enthusiasts after the event.

In the long-term, the value proposition for large-sized event organizers includes increased control over the secondary ticket market and reduced ticket fraud. These issues are commonly cited by large-sized event organizers and are not currently being addressed by the existing event ticketing industry. The use of blockchain-based event ticketing would allow these organizers to set a maximum resale price and take a percentage of resale royalty on every ticket resale. Furthermore, it would reduce fraudulent ticketing issues, where potential customers can spend hundreds only to realize they are unable to enter the event.

5.5 Customer Relationships

To obtain new customers, the company must spend time and money developing personal relationships with event organizers. A co-creation customer relationship should be formed in these initial stages, where direct input from event organizers is used to iterate upon product development. In the long term, automated services should be provided for small and medium-sized event organizers to reduce the costs of customer retention. Because large-sized event organizers often require customized ticketing services however, a co-creation customer relationship should be used to iterate upon product development that fits their needs.

5.6 Customer Segments

In the short-term, NFTickets will focus on small and medium-sized technical events in Europe, especially events in the blockchain space. This will allow NFTickets to most efficiently grow a targeted audience that technical event organizers can use to increase ticket sales. Furthermore, blockchain-focused events will most benefit from the use of NFT tickets, as partnering with NFT artists and novel marketing methods such as NFT Airdrops, can be used to market events to this customer base and engage them after the event. While blockchain-specific technical events are a niche market, they are the most likely initial customers and can be used to iterate upon initial product development.

In the long-term, NFTickets will focus on large-sized events in North America and Europe. Large-sized event organizers face the most significant issues regarding the secondary ticket market and fraudulent ticketing which are currently not served by event ticketing companies. Thus, this customer segment would most benefit from blockchain-based event ticketing.

5.7 Channels

In the short-term, NFTickets should develop personal relationships with event organizers. As the company grows, the company should create automated tools for small and medium-sized event organizers to use, and continue developing in-person relationships with large-sized event organizers. To reach event attendees, the company should test a variety of marketing tools such as an owned event marketplace website, social media marketing, email campaigns, NFT Airdrops, and partnerships with media organizations.

5.8 Revenue Streams

A detailed revenue breakdown is shown in the following section. The company's main revenue stream is a 10% fee on all ticket sales and resales. Furthermore, partnerships can be created with event sponsors in order to market their company to NFTickets' user base.

5.9 Cost Structure

A detailed cost structure is shown in the following section. Per these estimates, approximately 50% of the company's expenses consist of payroll for the technical and business teams, 30% for the technology stack, and 20% for marketing campaigns to reach event attendees.

Chapter 6

Break-Even Analysis

As shown in Figure 6.1, a break-even analysis was conducted to estimate when NFTickets will become profitable. The most significant cost is payroll, which includes the technical developers developing the web application, phone application, and decentralized systems, as well as the business team, focusing on customer acquisition, marketing, and business development. The technology stack is the next largest cost estimated at 30% of total costs, consisting mainly of website, database, and decentralized systems hosting and smart contract fees [18]. Next, marketing is estimated at 20% of total costs as marketing events and expanding event organizer reach is significant to the success of the company [13].

The estimated revenue consists mainly of a 10% fee on all ticket sales and resales. A 10% fee was determined as this is lower than most event ticketing competitors, and would still allow NFTickets to reach profitability in year 3. Secondly, revenue from partnerships with technical event sponsorships such as marketing to the customer base is estimated at 5% of total revenue. Revenue from ticket sales conservatively assumes a 40$ average ticket price [11]. Furthermore, a significant increase in ticket sales from year 1 to year 2 is anticipated as NFTickets develops its product offering, though an average 2.9% growth rate is assumed for further years, consistent with revenue growth for startups [4].

As shown in Figure 6.2, NFTickets is expected to break even in year 4, with a net income of $5.8 Million in year 4 and $7.5 Million in year 5.

				Year 1	Year 2	Year 3	Year 4	Year 5
Costs								
Number of Employees				5	6	7	15	25
Payroll	Technical and Business employees	100000	$100k per employee	$500,000	$600,000	$700,000	$1,500,000	$2,500,000
Office Space	No office space until year 3	500	$500 per employee per month	$0	$0	$42,000	$90,000	$150,000
Tech Stack	Domain name, website/database hosting, smart contracts	0.3	30% of total costs	$312,161	$393,206	$526,738	$1,181,821	$2,226,200
Legal Costs	Incorporation, on-going costs	0.02	$2k incorporation in first year 2% of revenue on-going costs	$4,756	$15,781	$41,966	$117,900	$338,111
Accounting	Accounting services	0.04	4% of revenue	$5,513	$27,563	$79,931	$231,801	$672,222
Team-related Costs	Travel, attending events	2000	$2,000 per employee per year	$10,000	$12,000	$14,000	$30,000	$50,000
Marketing	Digital marketing, relationships with media companies	0.2	20% of total costs	$208,108	$262,138	$351,159	$787,880	$1,484,133
TOTAL				$1,040,538	$1,310,688	$1,755,794	$3,939,402	$7,420,665

				Year 1	Year 2	Year 3	Year 4	Year 5
Revenue								
Tickets Sold		2.9	Assumes - 5x increase in tickets year 2 - Average 2.9x increase after	25,000	125,000	362,500	1,051,250	3,048,625
Revenue from Tickets Sold	Revenue from all ticket sales and resales		Revenue assumes - 10% of all ticket sales and resales - 5% of all tickets sold are resold - $40 average ticket price	$131,250	$656,250	$1,903,125	$5,519,063	$16,005,281
Revenue from event sponsorships	Revenue from partnerships with event sponsorships such as marketing to customer base		5% of total revenue	$6,563	$32,813	$95,156	$275,953	$800,264
TOTAL				$137,813	$689,063	$1,998,281	$5,795,016	$16,805,545

			Year 1	Year 2	Year 3	Year 4	Year 5
Break Even Analysis		Break Even Analysis					
EBITDA		EBITDA	$ (902,725.00)	$ (621,625.00)	$ 242,487.50	$ 1,855,613.75	$ 9,384,879.88
Taxes		Taxes	$ -	$ -	$ 50,922.38	$ 389,678.89	$ 1,970,824.77
Net Income		Net Income	$ (902,725.00)	$ (621,625.00)	$ 191,565.13	$ 1,465,934.86	$ 7,414,055.10
Break Even?		Break Even?	$ (902,725.00)	$ (1,524,350.00)	$ (1,332,784.88)	$ 133,149.99	$ 7,547,205.09

Figure 6.1: Detailed Cost-Revenue Breakdown

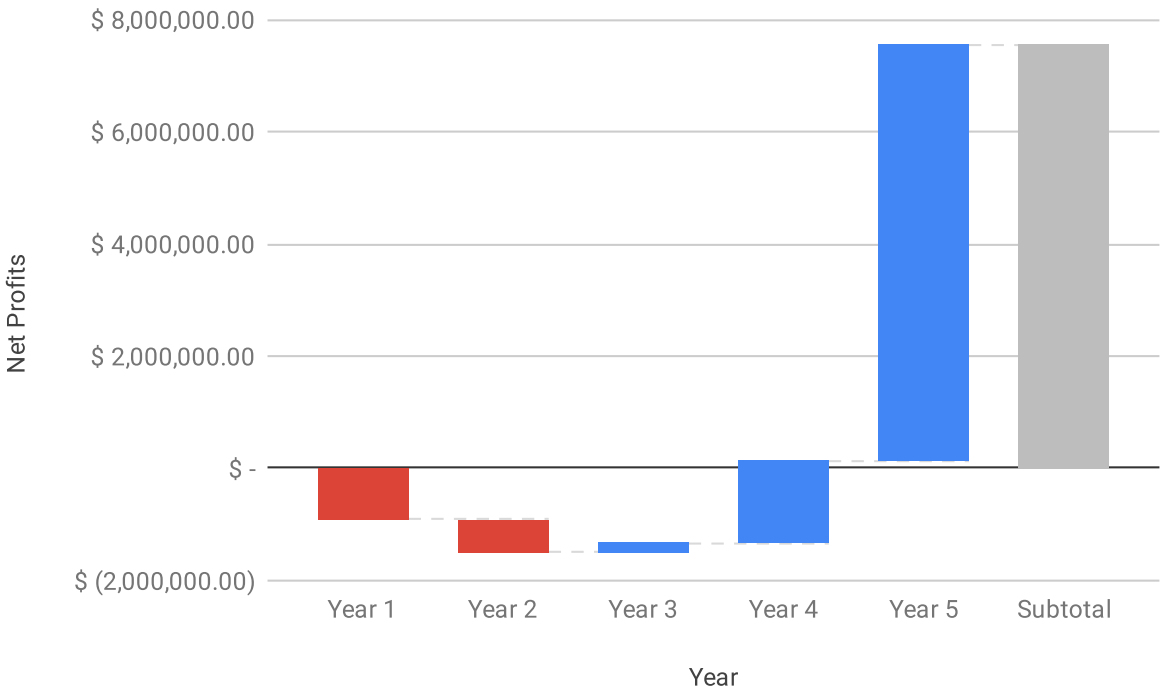


Figure 6.2: Net Profits over Time

Chapter 7

Next Steps

This section presents steps taken to further the development of NFTickets, including finding potential customers and funding sources.

7.1 Potential Customers

After interviewing 19 event organizers, a few were targeted to deepen relationships, including three of whom showed direct interest in using NFTickets when a market-ready prototype has been developed: EPFL Pavilions, Geneva Event Crypto, and Fr3n.

EPFL Pavilions hosts multiple exhibitions and symposiums each year on topics that merge art and science. The opening events for the exhibitions attract around 400 attendees while the symposiums attract around 100 attendees. As EPFL Pavilions focuses on art and technology, unique ticket offerings could be provided. For example, their past exhibit on "deep fake" photos could be leveraged to encode these photos into NFT tickets, providing each attendee with a unique event ticket. Their past exhibit on cosmos archaeology harnessed immersive visualization tools to visualize astrophysical data into sounds and images. These data could also be encoded in NFT event tickets, providing attendees with tickets that could be explored even after the event. Furthermore, EPFL Pavilions would allow NFTickets to co-develop a product offering in a low-risk environment that does not require highly scalable services.

Geneva Event Crypto (GEC) hosts one event per year with up to 1,000 attendees. The event focuses on blockchain-specific topics for technical and business professionals in the industry, NFT artists, and cryptocurrency traders. Thus, after NFTickets' product offering is developed and proven on a smaller scale with EPFL Pavilions, the product offering can be scaled to a medium-sized event with GEC. Because GEC attracts blockchain enthusiasts, partnerships with NFT artists attending the event can be forged to create artistic event tickets the attendees value.

Fr3n is a startup that focuses on providing blockchain-based tools to help build communities, and has shown interest in NFTickets providing blockchain-based event ticketing services. Unlike EPFL Pavilions and GEC, Fr3n would allow NFTickets to gain an ongoing revenue stream from any event organizers using the Fr3n platform. Thus, after NFTickets proves its product offering, new event organizers can be found in a lower-cost, automated fashion.

7.2 Funding

To find sources of funding for NFTickets, I met numerous angel investors and venture capital professionals (VCs) at startup and blockchain-focused conferences and events, including StartupDays, Crypto Valley Conference, Blockchance Conference, and smaller local events. Most of these angel investors and VCs stated that NFTickets would need around 3-10 medium-sized event organizers prior to investing; moreover, I now have these contacts to call upon when NFTickets reaches that size. Secondly, I applied to multiple incubators and accelerator programs to aid in finding additional team members, finding funding sources, and technical and business expertise. These programs include Tech4Trust, Crypto Valley Labs, InnMind Accelerator, and the Innosuisse startup training and coaching programs.

Chapter 8

Conclusion

To develop the business use case for blockchain-based event ticketing, the following business objectives were completed: customer interviews, competitor benchmarking, market segmentation, go-to-market strategy, business model, break-even analysis, and steps taken to find potential customers and funding sources.

Through 19 customer interviews, it was determined that lack of secondary market control and ticket fraud are major issues for large-sized event organizers that are currently unaddressed by major event ticketing companies. However, small and medium-sized event organizers do not face these issues as their events do not typically result in secondary markets. Above anything else, small and medium-sized event organizers cite expanding their audience as the most significant factor in an event ticketing service.

When benchmarking event ticketing competitors with the largest market share, it was determined their most significant advantage lies in their marketing and data analytics tools that allow event organizers to expand their audience. Furthermore, blockchain-based event ticketing companies typically focus on either increasing event organizer secondary market control and reducing ticket fraud, or engaging their audience after the event. Notably, nearly all competitors focus on music, sports, comedy, art, and metaverse events, ignoring technical events altogether.

When assessing event ticketing market segments, it was determined the global event ticketing industry is a $78 Billion industry globally with the secondary ticket market accounting for $19 Billion of this. While sports, music, and cinema account for $54.4 Billion of this, technical events such as exhibitions and conferences still account for $11.6 Billion. Furthermore, the North American and European markets make up 67% of the total event ticketing market.

After interviewing event organizers, benchmarking competitors, and assessing the event ticketing market, it was determined that small and medium-sized technical events are the short-term target market and large-sized events are the long-term target market. The focus on technical events in the short term allows NFTickets to grow a specific audience base that most competitors

ignore, and that can be used to expand the audience of technical event organizers. Once NFTickets has the resources to serve larger clients however, large-sized event organizers can be served. These event organizers would most benefit from the increased control over secondary market ticketing and reduced ticket fraud; moreover, these are both important issues to large-sized event organizers that are unaddressed by major competitors.

To create and assess the NFTickets business model, the business model canvas was completed and a break-even analysis was conducted. NFTickets will offer its services for a 10% fee on all ticket sales and resales and seek to partner with conference sponsors for additional marketing revenue. The major costs involve payroll, the technology stack, and marketing of events. This analysis concluded that NFTickets will break even in year 4, with an expected net income of $1.5 Million in year 4 and $7.4 Million in year 5.

Relationships were further developed with the event organizers EPFL Pavilions, Geneva Event Crypto, and Fr3n, who showed interest in using NFTickets when a market-ready prototype is ready. To find additional funding sources, relationships were developed with angel investors and venture capital professionals, and applications were submitted to several incubators and accelerator programs.

Part III

Academic

Chapter 9

Introduction

Event Ticketing is a $78 Billion industry globally, with the secondary ticket market accounting for $19 Billion of this [12]. However, event organizers have no control over the secondary ticket market and attendees experience high rates of ticket fraud. In fact, Ticketmaster estimates that bots siphon off 60% of tickets for major events that are then resold at higher prices. Event organizers have no control over these secondary ticket prices and see none of the resale value [3]. Furthermore, 12% of adults in the United States have purchased fraudulent tickets online, creating a lack of trust in the secondary ticket market [7]. Thus, the inability of event organizers to control the secondary ticket market for their own events and the inability of attendees to trust the secondary ticket market present major challenges in existing event ticketing systems.

Past research has been conducted on blockchain-based event ticketing systems to address these issues, but they lack adequate mechanisms to prevent off-chain ticket sales. More specifically, ticket resellers can sell tickets to specific buyers on-chain while taking additional money from these users off-chain. Regner et al. and Tackmann propose a system that would allow event organizers to sell tickets and users to purchase and use tickets through event smart contracts [9, 14]. This system allows event organizers to set resale prices and receive a percentage of resale royalty. However, there are no proposed mechanisms to prevent ticket resellers from requesting additional payments outside of the event smart contract. Lee et al. propose a mutual collateral system to solve this issue, where both buyer and seller place a collateral deposit on each ticket purchase to disincentivize dishonest behavior [6]. For example, if the ticket reseller requests additional money from the ticket buyer off-chain, the ticket buyer can report this. The ticket reseller's collateral is then kept and the ticket buyer is returned their collateral and ticket payment. However, this system fails to address whether the claims of the ticket buyer are honest and reduces the liquidity of both buyer and seller.

Given challenges with existing event ticketing systems and the drawbacks of past research, the purpose of this research is to implement a blockchain-based event ticketing system with the following properties:

- Control over secondary market: Guarantees the event organizer can set secondary ticket market prices and take a percentage of resale royalties.
- Anti-forgery: Guarantees the ticket buyer can verify the ticket is not fake.
- Prevent off-chain ticket sales: Guarantees the ticket reseller cannot resell the ticket for a price higher than that set by the event organizer.
- No deposit: Avoids the need for the buyer and seller to make a deposit.
- Unlinkability: Guarantees an attacker cannot link an attendee to multiple events.

This paper proposes a blockchain-based event ticketing system that achieves these properties through the use of an identification system and ticket market.

The identification system allows user identities to be linked to event tickets in a privacy-preserving manner. Prior to purchasing an event ticket, ticket buyers scan their identification card and gain anonymous event credentials that can be used to purchase event tickets. When purchasing an event ticket, ticket buyers submit their payment and event credential, which is stored in the event ticket. At the event, attendees scan their event ticket and identification card, where the event credential is again computed from the identification card. The event organizer admits entrance if the event ticket is valid and contains the matching event credential.

The ticket market utilizes an event smart contract that allows event organizers to create events and sell tickets and attendees to buy, resell, and use tickets. In the primary ticket market, ticket buyers purchase event tickets directly through the event smart contract. In the secondary ticket market, ticket resellers and buyers utilize Flash Freezing Flash Boys (F3B), which relies on a commit-reveal scheme that enables encrypted transactions and delayed execution [17]. Thus, secondary ticket market resellers and buyers commit to encrypted transactions, which are later shuffled, decrypted, and executed, thereby sending the ticket resellers the ticket payment and the ticket buyers the event tickets.

Notably, the identification system and secondary ticket market prevent off-chain ticket sales. Firstly, the identification system attaches event tickets to user identities, disallowing event tickets to be purchased by one user and then used by another. Secondly, the secondary ticket market uses encrypted transactions that are then shuffled, decrypted, and executed. Thus, the ticket reseller has no ability to request off-chain payments from the ticket buyer as they have no ability to choose the ticket buyer.

A prototype of this event ticketing system was built on EPFL Decentralized and Distributed Systems Laboratory's Dela blockchain. This prototype meets the control over secondary market, anti-forgery, prevent off-chain ticket sales, no deposit, and unlinkability properties. Furthermore, the storage required by the event market increases linearly with the number of ticket owners, requiring 256kB for an event with 1,000 ticket owners. The latency of the identification system was evaluated, showing that a credential issuance committee of only 3 nodes would result in

a 3.4-second latency, mainly due to the secure-multiparty computation used to deduplicate identities. The throughput of the primary and secondary ticket markets were then evaluated, resulting in throughputs of around 3 transactions per second for the primary ticket market and 0.15 transactions per second for the secondary ticket market. Thus, improvements in scalability must be made before the system can be used for large-sized event organizers.

The key contributions of this paper include:

1. To our knowledge, this is the first work to design and implement a blockchain-based event ticketing system with the control over secondary market, anti-forgery, prevent off-chain ticket sales, no deposit, and unlinkability properties.
2. An evaluation was conducted to determine the storage, latency, and throughput of the system.

Chapter 10

Background

This section presents a brief background on Dela, the Flash Freezing Flash Boys (F3B) protocol, CanDID Identification System, and MP-SPDZ framework utilized to develop the blockchain-based event ticketing system.

10.1 Dela

The EPFL Decentralized and Distributed Computing Laboratory's Dela was utilized to develop the event smart contract where event organizers can sell tickets and attendees can buy, resell, and use event tickets [8]. Dela is a set of modular abstractions and an implementation of a distributed ledger architecture whose purpose is to provide a modular and universal framework that can be used to run a distributed ledger. Dela is built around the following six core modules:

- Access: Access is an access control service that authorizes which users are able to interact with smart contracts. It reads storage to determine permissions associated with each credential and can update existing credentials.
- Execution: Execution is a service that defines the primitives necessary for executing a transaction, such as all previous transactions that have been executed and the results of the transaction execution.
- Ordering: The ordering service creates blocks, thereby extending the blockchain. While the ordering service does not determine the consensus method, it does define how values are read from the ledger.
- Store: Store defines the primitives necessary for a simple key/value storage that provides atomicity and that smart contracts can write to and read from.

- Transaction: The transaction pool offers clients a single entry point for transactions to be propagated throughout the network. Transactions are sent to the transaction pool while the ordering service waits for enough transactions to create a new block.
- Validation: The validation service protects against malicious behavior by ensuring transactions are valid. This service protects against replay attacks, ensures transaction execution is correct, and provides a manager to help create and sign transactions.

10.2 Flash Freezing Flash Boys (F3B)

Flash Freezing Flash Boys (F3B) was used to allow secondary ticket market transactions to be encrypted and their execution delayed. Thus, when tickets for an event are sold out, ticket resellers and buyers encrypt resell and buy transactions; moreover, at a set time before the event, these transactions are shuffled, decrypted, and executed [17]. Originally designed to prevent front-running attacks, F3B relies on a commit-reveal scheme where encrypted transactions are committed and then later revealed by a decentralized secret-management committee. As shown in Figure 3.1, a transaction sender encrypts their transaction tx with a symmetric key k, resulting in the encrypted transaction c_{tx}. Next, the sender encrypts k with the public key of the secret-management committee, resulting in c_k. Finally, the sender submits both c_{tx} and c_k in the form of a write transaction. Once the transaction is committed, the secret-management committee later releases secret key shares to the underlying consensus group, where the secret key is reconstructed. With the secret key reconstructed, the consensus group is able to decrypt c_k and obtain k, decrypt c_{tx} and obtain tx, and execute tx.

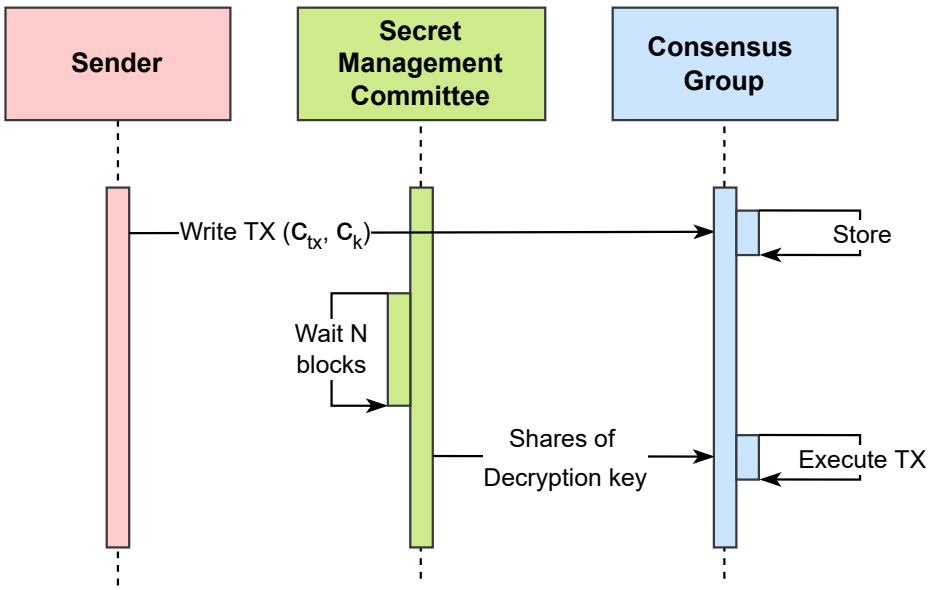


Figure 10.1: Flash Freezing Flash Boys Architecture

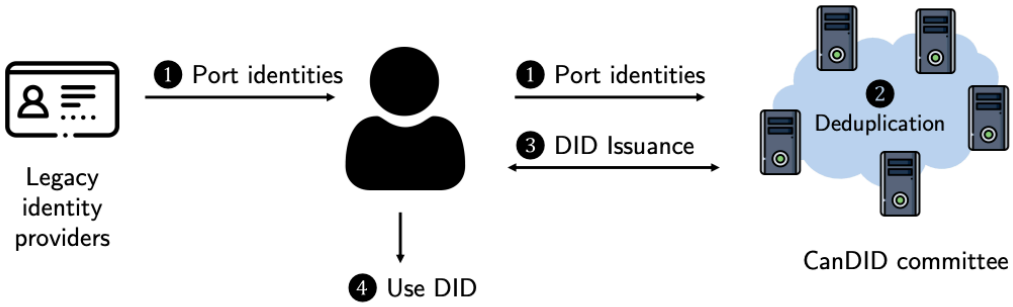
10.3 CanDID Identification System

CanDID is a decentralized identity system that allows users to create decentralized identifiers (DIDs), which are used to deduplicate user identities and to attach event tickets to user identities in a privacy-preserving manner [8]. CanDID achieves this through the use of a credential-issuance committee, which is a decentralized collection of nodes. As can be seen in Figure 10.2, users interact with the credential-issuance committee in order to obtain anonymous credentials that can be used for anonymous authentication. The CanDID system allows for the creation of DIDs while achieving the following properties:

- Legacy compatibility: To achieve legacy compatibility, CanDID allows users to import identities from existing systems such as email or bank accounts using the oracles DECO and Town Crier [15, 16]. This allows users to prove their identity originates from this source, and receive trustworthy credentials from the CanDID committee.
- Sybil-resistance: To achieve sybil-resistance, CanDID uses secure multi-party computation to compute a hash of the user's identification. This hash is then stored, ensuring that no user with the same identification can obtain multiple credentials.
- Accountability: To achieve accountability, CanDID screens each user in a privacy-preserving manner, comparing each user to a sanctions list while learning nothing of users not on the sanctions list.
- Key recovery: To achieve key recovery, users have the ability to backup keys on multiple devices using secret sharing, and to setup a recovery policy with the credential-issuance committee.

10.4 MP-SPDZ

MP-SPDZ is a secure multi-party computation (MPC) software that is used in the identification system to deduplicate the user's identity without learning the user's identity [5]. As a result, each user is only able to obtain one master credential for their identity, disallowing them from attaching event tickets to several identities. More specifically, MP-SPDZ is an implementation of 34 MPC protocol variants that can be used with a high-level programming interface based on Python. MP-SPDZ was designed to benchmark various MPC protocols in a variety of security models such as honest and dishonest majority, semi-honest/passive, and malicious/active corruption. Furthermore, MP-SPDZ employs the following primitives: secret sharing, oblivious transfer, homomorphic encryption, and garbled circuits.



(a) High-level credential-issuance workflow.

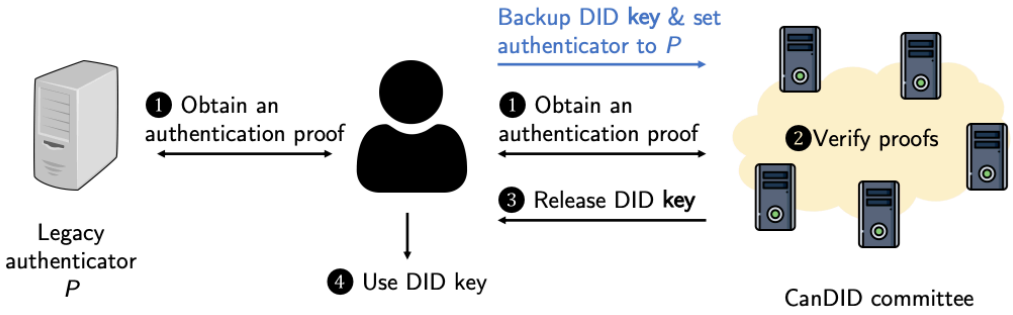


Figure 10.2: CanDID Identification System Architecture [8]

Chapter 11

Design

This section presents the system design for the blockchain-based event ticketing system, overviewing the system as a whole, and then the web application, identification system, primary ticket market, and secondary ticket market in greater detail. Key design decisions are also discussed for the web application, identification system, primary ticket market, and secondary ticket market.

11.1 Design Goals

As mentioned previously, the design goals of the event ticketing system are the following:

- Control over secondary market: Guarantees the event organizer can set secondary ticket market prices and take a percentage of resale royalties.
- Anti-forgery: Guarantees the ticket buyer can verify the ticket is not fake.
- Prevent off-chain ticket sales: Guarantees the ticket reseller cannot resell the ticket for a price higher than that set by the event organizer.
- No deposit: Avoids the need for the buyer and seller to make a deposit.
- Unlinkability: Guarantees an attacker cannot link an attendee to multiple events.

11.2 System Overview

To meet these design goals, the event ticketing system was implemented using a ReactJS web frontend, Flask web backend, MongoDB database, DELA blockchain, CanDID identification

system credential-issuance committee, and F3B secret-management committee. The system architecture can be seen in Figure 11.1.

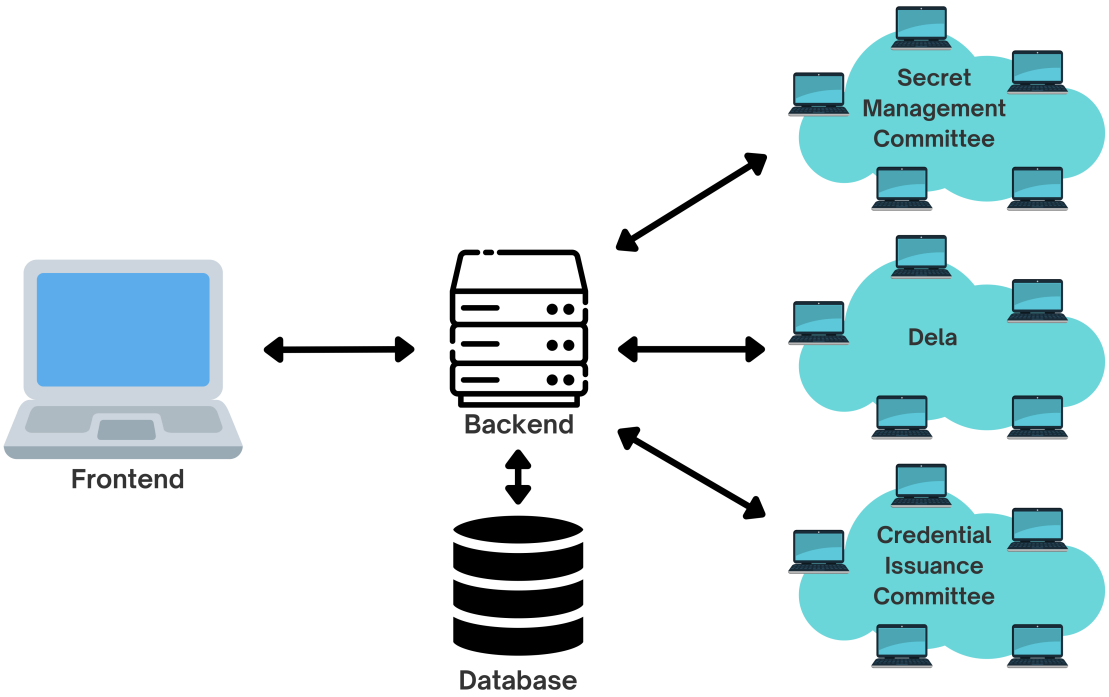


Figure 11.1: Dela Architecture

Before describing each of these system components in greater detail, the overall system will be described through common user scenarios:

11.2.1 Create Account

To create an account, the user fills in a form using the web frontend specifying their username and password. Submitting this form sends a request to the web backend, which creates a user account. Their username and password hash are stored in the database along with a public and private key that is used to interact with the Dela blockchain. Storage of the user public and private keys makes the event ticketing system a custodian and therefore a single point of failure. While this is not ideal, this was deemed sufficient for the purposes of the prototype. This design decision is discussed in greater detail in Section 11.3.1.

In order to later buy, resell, or use event tickets, the user must also obtain a master credential from the identification system. To obtain this, the user fills in a form using the web frontend specifying their name. Submitting this form sends a request to the web backend, which obtains the master credential from the credential issuance committee and stores it in the database.

11.2.2 Create Event

To create an event, the event organizer fills in a form using the web frontend specifying the event name, number of tickets, ticket price, maximum resale price, and resale royalty. Submitting this form sends a request to the web backend, which launches an event smart contract on the Dela blockchain with these parameters.

11.2.3 Buy Ticket on Primary Market

To buy a ticket on the primary market, the user fills in a form using the web frontend, specifying the number of tickets they want to purchase from an event. Submitting this form sends a request to the web backend, which first obtains an event credential from the identification system which is used to buy event tickets. The web backend then submits a buy transaction to the event smart contract where the user is stored as a ticket owner, along with their event credential.

11.2.4 Resell Ticket on Secondary Market

To resell a ticket on the secondary market, the user fills in a form using the web frontend, specifying the number of tickets and price per ticket they want to resell on the secondary market. Submitting this form sends a request to the web backend, which encrypts the transaction using the secret-management committee and then stores the transaction on the Dela blockchain.

11.2.5 Buy Ticket on Secondary Market

To buy a ticket on the secondary market, the user fills in a form using the web frontend, specifying the number of tickets and price per ticket they want to buy on the secondary market. Submitting this form sends a request to the web backend, which first reads the user's event credential from the database and verifies the event credential with the identification system. If the event credential is verified, the web backend then sends the buy transaction to the secret-management committee to be encrypted. This encrypted buy transaction is then stored on the Dela blockchain.

At a set time before the event, the secret-mangement committee reads the encrypted secondary market transactions from Dela, shuffles them, decrypts them, and sends them to the event smart contract to be executed. With each secondary market transaction executed, the ticket reseller receives their payment and the ticket buyer is noted as a ticket owner.

11.2.6 Use Ticket

To use an event ticket, the user submits their ticket to be used from the web frontend, specifying their name. Submitting this form sends a request to the web backend, which again obtains an event credential from the identification system. The web backend then submits this event credential to the event smart contract. If the event credential matches that on the user ticket, the event ticket state is updated to "used".

11.3 System Components

This section presents the web application, identification system, primary ticket market, and secondary ticket market system components in greater detail.

11.3.1 Web Application Components

A ReactJS web frontend, Flask web backend, and MongoDB database were used to develop the web application for event organizers and ticket buyers and sellers to interact with the event ticketing system. ReactJS, Flask, and MongoDB are used because they allow for prototype web applications to be quickly created and modified. ReactJS allows for the flexible use of components that can be built and reused throughout the frontend, Flask allows for REST API's to be quickly created, and MongoDB allows for data to be flexibly stored in JSON format. Secondly, my experience using ReactJS, Flask, and MongoDB also enabled the prototype web application to be quickly created and modified.

Two major design decisions were made with regard to the web application components. Firstly, the web application uses Flask to interact with Dela and the identification system through the command-line interface. This choice was made for the purposes of developing the prototype, as it makes use of existing Dela and dkg command-line infrastructure. However, future iterations of the blockchain-based event ticketing system should use separate servers to interact with both Dela and the identification system. Secondly, the prototype currently stores user private keys in a database, a decision also made for the purposes of developing the prototype. However, this creates a single point of failure as any attacker who gains access to the database could obtain these private keys and control event organizer and attendee accounts. Future iterations of the blockchain-based event ticketing system should manage user private keys from the client side to avoid these issues.

11.3.2 Identification System

The identification system architecture is shown in Figure 11.2. The purpose of the identification system is to connect user identities to event tickets in a privacy-preserving manner. In order to achieve this, the user first obtains a master credential from the identification system and then a separate event credential for each event they buy tickets for.

To obtain the master credential, the user uploads their identification information which is hashed and secret-shared. The user's public key and secret share are each sent to separate identification system nodes. The identification system then computes a hash of the user's identification using secure multi-party computation, which disallows the identification system from ever learning the user's identity. This hash is then stored by the identification system which prevents users from obtaining multiple credentials for each identity. If the identification system does not have the user's hash stored, each node computes a partial signature on the user's public key, the signatures are sent to the user, and the user reconstructs these partial signatures to obtain their master credential.

In order to obtain an event credential, the user sends their public key, master credential, and the name of the event to the identification system. If the identification system verifies the master credential, each node computes a partial signature on the user's public key and event name. These partial signatures are then sent to the user and the user reconstructs them to obtain the event credential.

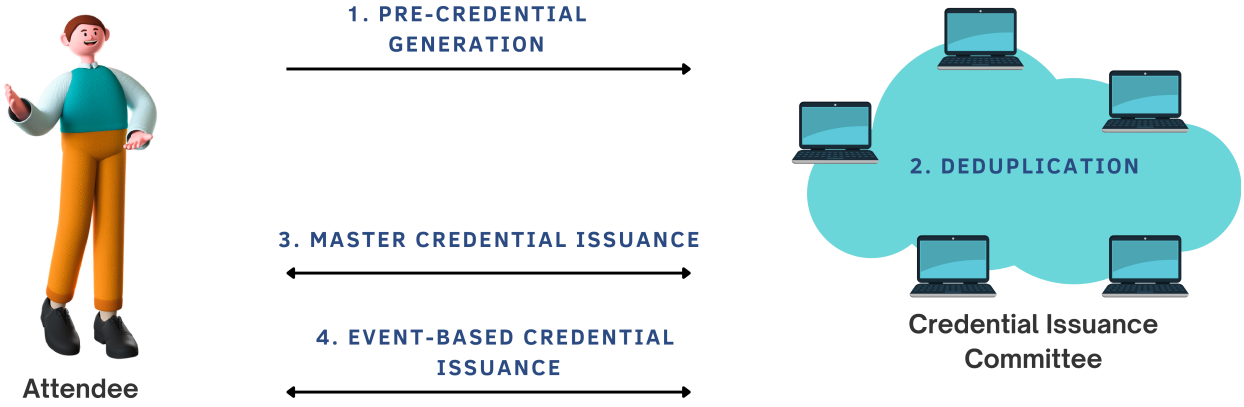


Figure 11.2: Identification System Architecture

The identification system master and event credentials were chosen to help prevent off-chain ticket sales and to prevent attackers from linking attendees to multiple events. Firstly, the use of master and event credentials allows user identities to be linked to event tickets. This prevents ticket resellers from reselling tickets to ticket buyers off-chain, as the event ticket would still be attached to the reseller's identity. Thus, when identification cards are checked at the event entrance, the ticket buyer would not gain entry to the event. Secondly, because ticket buyers gain different event credentials for each event and these event credentials are not linkable, their

attendance at different events is unlinkable.

11.3.3 Primary Ticket Market

The primary ticket market architecture is shown in Figure 11.3. To purchase an event ticket, the ticket buyer sends a buy transaction to the event smart contract that includes the number of tickets they are purchasing, the payment, and their event credential. In response, the event smart contract transfers the payment and stores the event credential and number of tickets the ticket buyer now owns.

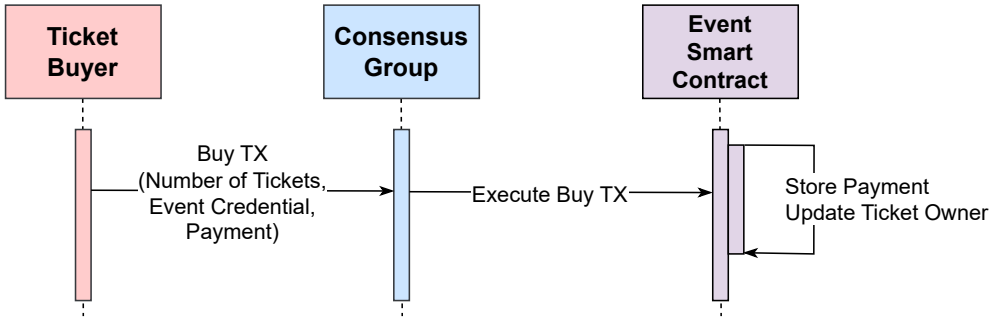


Figure 11.3: Primary Ticket Market Architecture

The most significant primary ticket market design decision made was to store the ticket buyer's event credential with their event ticket. Doing so attaches the buyer's identity to their ticket, helping to prevent off-chain ticket sales. Furthermore, because these event credentials are computed using secure-multiparty computation, a ticket buyer's identity is never learned.

11.3.4 Secondary Ticket Market

If the event is sold out, users can then resell and buy tickets on the secondary market, as shown in Figure 11.4. The secondary ticket market introduces the Flash Freezing Flash Boys (F3B) secret-management committee, which allows ticket resellers and buyers to commit to encrypted transactions that are then stored on Dela.

In the case of a sold-out event, n ticket resellers send encrypted resell transactions and k ticket buyers send encrypted buy transactions to be stored on Dela. At set times, such as a week before an event, the secret-management committee reads these n encrypted resell transactions and k encrypted buy transactions and shuffles, decrypts, and executes them. The event smart contract then receives these resell and buy transactions and transfers the resale royalty to the event smart contract and the remaining ticket payment to the ticket reseller. The event smart contract then removes ticket ownership for the ticket reseller, stores the event credential for the ticket buyer, and stores the ticket buyer as the new ticket owner. Because these buy transactions

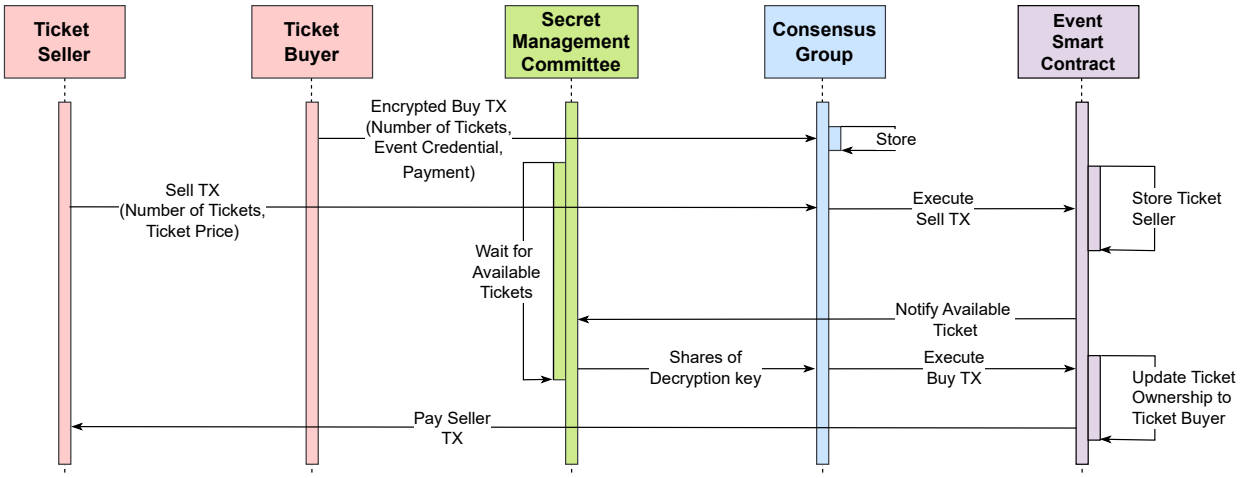


Figure 11.4: Secondary Ticket Market Architecture

are shuffled before they are decrypted and executed, the ticket reseller is unable to demand off-chain ticket payments from the ticket buyer as they are unable to choose the ticket buyer.

Two key design decisions were made regarding the secondary ticket market. Firstly, F3B was used to encrypt both secondary market buy and resell transactions that are later shuffled, decrypted, and executed. This prevents ticket resellers from requesting additional off-chain payments from ticket buyers as they are unable to choose which ticket buyer will receive their event ticket. Furthermore, encrypting both secondary buy and resell transactions gives attackers little information to collude with, as discussed later in the Threat Model. Secondly, secondary market transactions can be shuffled, decrypted, and executed after n secondary transactions have been written to Dela, or at a set time. If the secret-management committee were to execute transactions after n are written to Dela, this would allow secondary market buyers to initiate this resale process. For example, if there are currently $n - 5$ encrypted secondary transactions written to Dela, a buyer can submit 5 additional secondary transactions, thereby triggering the secondary transactions to be shuffled, decrypted, and executed. If the secret-management committee executes these transactions at a set time however, the buyer gains no such advantage.

Chapter 12

Implementation

This section presents the implementation of the blockchain-based event ticketing system, overviewing the web frontend, web backend, database, identification system, ticket market, and testing.

12.1 Web Frontend

The web application frontend contains the following pages:

- Landing Page: The landing page allows users to signup or login using their email address and password.
- Homepage: The homepage allows users to enter their identification and obtain a master credential later used to buy event tickets. Secondly, the homepage displays the user's tickets that are owned and up for sale.
- Add Event: The Add Event page allows event organizers to create new events by specifying the event name, number of tickets to be sold, price per ticket, maximum resale price, and resale royalty.
- Events: The events page displays a list of events created by event organizers.
- Event: The event page displays event details including the event name, the number of tickets remaining, the price per ticket, the maximum resale price, and the resale royalty. If the event is not yet sold out, users can purchase tickets from the primary ticket market. If the event is sold out, users can submit transactions to buy tickets on the secondary market when they become available.

- Admin: The admin page allows the administrator to view the balance of the events, the tickets owned by each user, and the tickets up for sale by each user. The administrator can also initiate secondary ticket market resales, which notify the F3B secret-management committee to shuffle, decrypt, and execute the secondary ticket market buy transactions.

12.2 Web Backend

The web application backend contains the following REST API routes:

- **Authentication**:
  - /auth/register: Allows the user to register with their email and password.
  - /auth/login: Allows the user to login with their email and password.
- **User**:
  - /user/profile: Returns the user's profile information from the database, which is used to display their master credential.
- **Value**:
  - /sc/value/write: Writes a key-value pair to the Dela value smart contract.
  - /sc/value/read: Given a key, reads a value from the Dela value smart contract.
  - /sc/value/list: Lists all key-value pairs from the Dela value smart contract.
- **Event**:
  - /sc/event/get-events: Returns all events from the database.
  - /sc/event/get-event/<event_id>: Returns the event information from the event smart contract, specifically the event name, number of tickets remaining, price per ticket, maximum resale price, and resale royalty.
  - /sc/event/create: Allows event organizers to create an event using the event smart contract.
  - /sc/event/buy: Allows users to buy tickets to an event on the primary market.
  - /sc/event/resell: Allows users to resell tickets to an event.
  - /sc/event/rebuy: Allows users to buy tickets to an event on the secondary market.
  - /sc/event/decrypt-execute-secondary: Allows the administrator to initiate the secondary market resale transactions, where the secondary transactions are shuffled, decrypted, and executed. As a result, these secondary resell and buy transactions are stored on the event smart contract, but transfer of ticket payments and ownership do not yet take place.

  - /sc/event/transact-secondary: Allows the administrator to transfer ticket payments and ownership. As a result, the event organizer receives their resale royalty from each ticket resale, the ticket reseller receives their payment, and the ticket buyer receives their ticket.
  - /sc/event/read: Reads all data from an event smart contract, such as the event name, tickets remaining, ticket owners, and tickets that are up for sale.

- **DKG**:
  - /dkg/encrypt: Allows data to be encrypted using the secret-management committee.
  - /dkg/decrypt: Allows data to be decrypted using the secret-management committee.

- **Identification**:
  - /identification/issue-master-credential: Given a user's identification, issues the user a master credential through the identification system.
  - /identification/auth-event-tx: Used to verify if a user has the proper event credential to buy event tickets to an event. If the user does not have an event credential, the user interacts with the identification system to create and verify an event credential. If the user has an event credential, the user interacts with the identification system to verify the event credential.

12.3 Database

The web application database contains the following tables:

- **Users**:
  - user_id: User's id used for database access.
  - email: User's email address.
  - password: Hash of the user's password.
  - sk: User's secret key used to interact with Dela.
  - pk: User's public key used to interact with Dela.
  - id_hash: Hash of the user's identification computed by the identification system.
  - master_credential: User's master credential computed by the identification system.
  - master_signatures: User's master signatures, which are the individual signatures signed by the identification system that are used to construct the master credential.
  - event_credential: Array of the user's event credential computed by the identification system for each event the user buys or resells tickets to.

  - event_signatures: Array of the user's event signatures, which are the individual signatures signed by the identification system that are used to construct the event credentials.

- **Events**:
  - event_id: The event's id used for database access.
  - owner: The public key of the event organizer who created the event.
  - name: Name of the event.
  - num_tickets: Total number of tickets that can be sold.
  - price: Price per ticket.
  - max_resale_price: Maximum resale price that tickets can be resold for on the secondary market.
  - resale_royalty: The percentage resale royalty the event organizer receives for every ticket resale.

12.4 Identification System

The identification system utilizes MP-SPDZ in order to compute the hash of the user's identification in secure-multiparty computation (MPC) and Dela's existing dkg infrastructure to compute and verify master and event credentials.

12.4.1 MP-SPDZ MiMC Pseudo-Random Function

To compute the hash of the user's identification using MP-SPDZ, a MiMC Pseudo-random Function is used because it runs efficiently in arithmetic circuits [1]. The following MiMC class in MP-SPDZ is used to accomplish this [5]:

```
class MiMC(object):
    def __init__(self, _rounds, _key, num_calls):
        self.rounds = _rounds
        self.constants = self.get_rounds_constants()
        self.key = _key
        if use_cubes:
            self.kd_pre = KDPreprocessing(num_calls, self.rounds)

    def get_rounds_constants(self):
        return [sint.get_random_triple()[0].reveal() for i in range(self.rounds)]
```

```
@vectorize
def encrypt(self, m):
    key = self.key
    x = m + key
    for r in range(self.rounds):
        x = x ** 3
        x = x + key + self.constants[r]
    x = x + key
    return x
```

The MiMC class computes the pseudo-random function of the message by iterating a round function r times, where each round consists of a key addition with the key k, the addition of a round constant, and the application of a non-linear function $F(x) = x^3$. First, the MiMC class is instantiated with the number of rounds $\_rounds$, key $\_key$, and the number of times the class will be used to encrypt a message num_calls. Next, the $encrypt$ function is used to compute the MiMC pseudo-random function of a message m. Notably, the message used is the hash of the user's identification which is secret-shared, with one share sent to each identification system node. The $@vectorize$ decorator on the encrypt function notes that the encrypt function operates on a vector of secret shares, despite each secret share being shared to only one identification system node.

12.4.2 Master and Event Credentials

Once the hash of the user's identification is computed in secure multi-party computation, the user is able to obtain their master and event credentials. In order to compute and verify master and event credentials, the following functions were developed atop Dela's existing dkg package:

- IssueMasterCredential(idHash, pk): IssueMasterCredential first stores the user's $idHash$ which was computed in secure-multiparty computation using MP-SPDZ and checks to ensure the idHash is not already stored. If the user's $idHash$ is already stored, the user is denied a master credential to ensure deduplication. If the user's $idHash$ is not already stored, the identification system nodes compute partial signatures on the user's public key and the user reconstructs these partial signatures to obtain their master credential.
- IssueEventCredential(pk, eventName, masterCredential): IssueEventCredential first verifies the user's master credential by checking the cosignature on the user's public key matches the master credential. If the master credential is verified, the identification system nodes compute partial signatures on the user's public key and the name of the event they are seeking tickets for. The user then reconstructs these partial signatures to obtain their event credential
- VerifyEventCredential(pk, eventName, eventCredential): VerifyEventCredential verifies

the user's event credential by checking the cosignature on the user's public key and name of the event matches the event credential. If so, the event credential is verified.

In order to compute and verify partial signatures, the Kyber bdn package was used, which implements the Boneh-Drijvers-Neven signature scheme. This allows identification system nodes to compute partial signatures the user can then aggregate into master and event credentials. Furthermore, it allows identification system nodes to then verify these master and event credentials.

12.5 Ticket Market

An event smart contract was developed to allow event organizers to create events and sell event tickets, and users to buy, resell, and use event tickets. The event smart contract class diagram can be seen in Figure 12.1 and the smart contract commands are described in greater detail below:

- Init(Name, NumTickets, Price, MaxResalePrice, ResaleRoyalty): Init is called by the event organizer in order to create a new event, thereby initializing the event owner, name of the event, the number of tickets to be sold, the price per ticket, the maximum resale price authorized on the secondary ticket market, and the resale royalty the event organizer receives for each ticket resale.
- Buy(NumTickets, Payment, EventCredential): Buy is called by a ticket buyer to purchase event tickets, specifying the number of tickets they are purchasing, their payment, and the event credential that is to be attached to each ticket. In response, the event smart contract transfers the payment to the event smart contract. The event smart contract then stores the buyer's event credential and the number of tickets they now own.
- Resell(NumTickets, Price): Resell transactions are created by the secondary ticket market resellers, though its execution is delayed by F3B's secret-management committee. Resell includes the number of tickets for sale for a specific price per ticket. The event smart contract ensures the ticket reseller has the number of tickets available and if so, stores the number of tickets and price per ticket to be resold on the secondary market.
- Rebuy(NumTickets, Price, EventCredential): Rebuy transactions are created by the secondary ticket market buyers, though its execution is delayed by F3B's secret-management committee. Rebuy includes the buyer's event credential and the number of tickets and price per ticket they are looking to purchase on the secondary market. If tickets are available, Rebuy transfers the ticket payment to the ticket reseller and ticket ownership to the ticket buyer.
- ReadEventContract(): ReadEventContract is called by the web application backend in order to obtain current information for the event, such as updated ticket owners and number of

tickets remaining. Whenever the event smart contract is written to, the web application backend calls ReadEventContract and sends these updates to the web application frontend where they are viewed by the user.

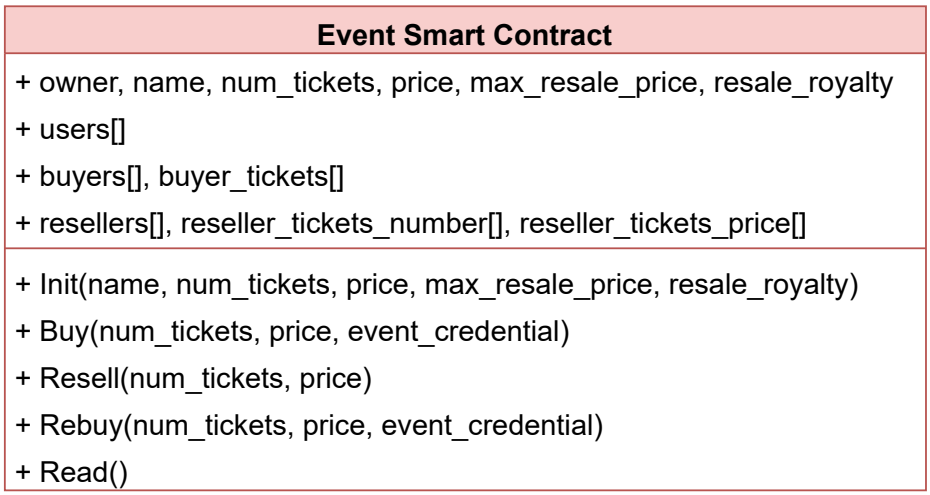


Figure 12.1: Event Smart Contract Class Diagram

12.6 Testing

Unit tests are implemented to test the identification system and event smart contract, and integration tests are implemented to test the event ticketing system as a whole. The code coverage of these unit tests can be seen below:

- Identification System: 74.3%
- Event Smart Contract: 62.2%

Chapter 13

Evaluation

This section presents the evaluation of the blockchain-based event ticketing system. The system was evaluated using a Macbook Pro laptop with a 2.2 GHz Intel Core i7 processor. The blockchain-based event ticketing system was evaluated qualitatively in terms of the design goals and quantitatively in terms of storage, latency, and throughput.

13.1 Qualitative Evaluation

As mentioned previously, the design goals of the event ticketing system are the following:

- Control over secondary market: Guarantees the event organizer can set secondary ticket market prices and take a percentage of resale royalties.
- Anti-forgery: Guarantees the ticket buyer can verify the ticket is not fake.
- Prevent off-chain ticket sales: Guarantees the ticket reseller cannot resell the ticket for a price higher than that set by the event organizer.
- No deposit: Avoids the need for the buyer and seller to make a deposit.
- Unlinkability: Guarantees an attacker cannot link an attendee to multiple events.

The blockchain-based event ticketing system meets all five properties as described below:

- Control over secondary market: The event smart contract allows the event organizer to set secondary ticket market prices and take a percentage of resale royalties on every ticket resale.

- Anti-forgery: The event smart contract allows each ticket buyer to verify the ticket is not fraudulent, thereby ensuring they are purchasing valid event tickets.
- Prevent off-chain ticket sales: The identification system allows identities to be attached to event tickets, thereby preventing tickets from being purchased from one user and used by another. Furthermore, the secondary ticket market shuffles a set of secondary market transactions, disallowing the ticket reseller from choosing the ticket buyer.
- No deposit: Both ticket buyer and reseller avoid making a deposit on all ticket sales and resales. Even when encrypted buy transactions are sent in advance of purchasing a ticket on the secondary market, F3B allows for the execution of these buy transactions to be delayed. Thus, ticket resellers make no deposit and ticket buyers do not transfer their payment until a ticket has become available.
- Unlinkability: While each user only obtains one master credential from the identification system, they obtain separate event credentials for each event they purchase tickets to. Because separate event credentials are used for different events, and these event credentials are not linkable, this guarantees an attacker cannot link an individual attendee to multiple events.

13.2 Quantitative Evaluation

The blockchain-based event ticketing system was evaluated quantitatively in terms of storage, latency, and throughput of the identification system, primary ticket market, and secondary ticket market.

13.2.1 Storage

Blockchains store data across a collection of distributed nodes, and are thus not ideal for storing large quantities of data. In terms of blockchain-based event ticketing systems, this could result in significant energy usage or costs of the system, particularly for large events. As such, the quantity of data stored by the event smart contract was evaluated. As can be seen in Table 13.1, the storage increases linearly as the number of ticket owners increases, as ticket owners, buyers, and resellers are stored on the event smart contract.

Number of Ticket Owners	Size (kBytes)
10	2.8
50	13.0
100	25.8
1,000	256.2
10,000	2560.2

Table 13.1: Storage vs Event Size

13.2.2 Latency of Identification System

The latency of the identification system was evaluated, measured as the time taken from the user entering their identification information to the user's event credential being verified. This is significant because larger latencies can cause delays in a user's ability to purchase event tickets and can cause long wait times at the event.

As can be seen in Figure 13.1, latency was measured for the user to obtain the hash of their identification in multiparty computation using MP-SPDZ, to obtain and verify their master credential, and to obtain and verify their event credential, as well as the total latency. Latency was measured for identification systems with 3, 5, 8, 16, 32, and 64 nodes, though MP-SPDZ only allowed for computations of up to 8 nodes. As can be seen, MP-SPDZ is by far the largest contributor to identification system latencies, with a latency of 3.7 seconds for 3 nodes and 36.8 seconds for 8 nodes. Thus, while larger identification system committee sizes are acceptable for issuing and verifying master and event credentials, large identification system committee sizes using MP-SPDZ would lead to long delays in the user's ability to purchase tickets and enter events.

13.2.3 Throughput of Primary Ticket Market

The throughput of the primary ticket market was evaluated, measured as the total number of buy transactions that can be executed per second. Throughput is significant, especially for large-sized events, as these events often require tens of thousands of users to purchase tickets simultaneously.

As can be seen in Figure 13.2, throughput was measured for Dela sizes of 3, 8, 16, and 32 nodes and for 10, 50, 100, 500, and 1,000 buy transactions. As is expected, the throughput is significantly lower for larger Dela sizes. For example, Dela with only 3 nodes maintains a transaction per second rate greater than 4 while Dela with 32 nodes maintains a transaction per second rate

Figure 13.1: Identification System Latency

less than 0.5. Furthermore, these throughput rates suggest the blockchain-based event ticketing system would face challenges with large-sized events, regardless of the number of Dela nodes.

13.2.4 Throughput of Secondary Ticket Market

The throughput of the secondary ticket market was evaluated, measured as the total number of secondary market buy and sell transactions that can be decrypted and executed by the F3B secret-management committee. Secondary ticket market throughput is also significant for large-sized events.

As can be seen in Figure 13.3, throughput was measured for F3B secret-management committee sizes of 8, 16, 32, and 64 nodes and for 10, 50, and 100 encrypted secondary transactions. As the number of encrypted secondary market transactions increases, the throughput of different secret-mangement committee sizes remains similar, at around 0.13 transactions per second. Nevertheless, the throughput rates of the secret-managment committee suggest the blockchain-

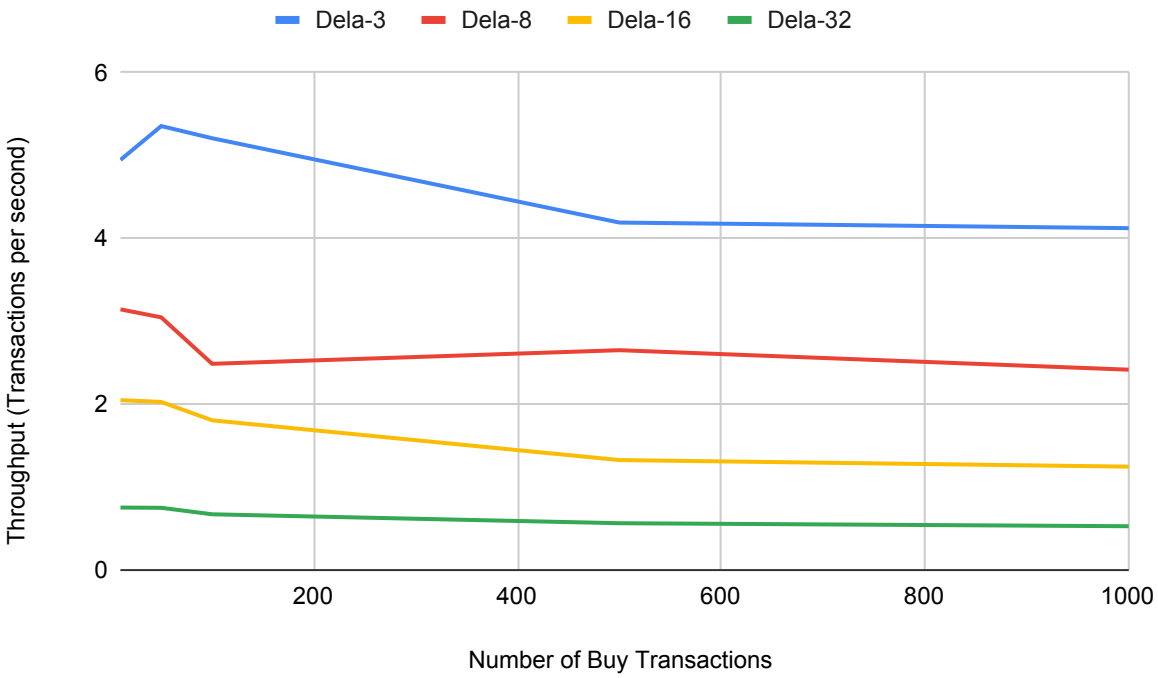


Figure 13.2: Primary Ticket Market Throughput

based event ticketing system would face challenges serving large-sized events.

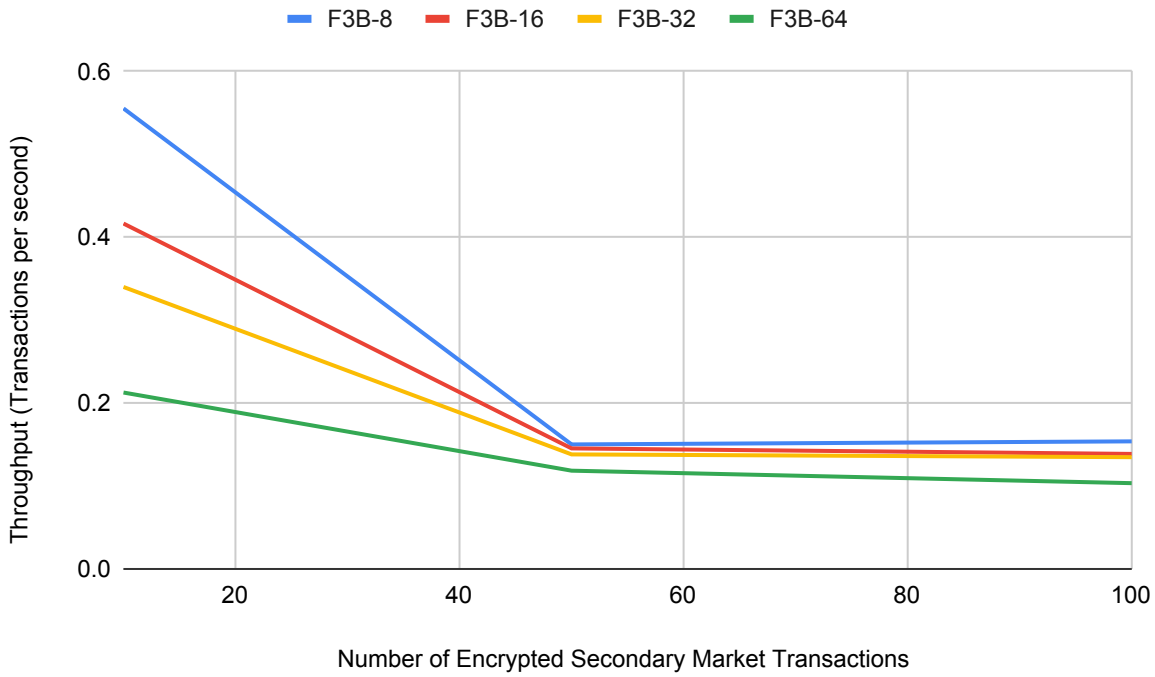


Figure 13.3: Secondary Ticket Market Throughput

Chapter 14

Threat Model

This section discusses the threat model, including the system actors, attack vectors, and mitigation.

14.1 System Actors

As can be seen in Figure 14.1, the system actors are the buyer, reseller, event organizer, credential issuance committee, secret-management committee, and event smart contract. The secondary market ticket reseller and buyer are assumed untrusted as they are incentivized to collude off-chain. This would allow the secondary market reseller to sell tickets for higher than that specified by the event organizer and to avoid resale royalties on ticket resales. Secondly, the event organizer is assumed trusted as they are incentivized to increase their control over the secondary market and prevent these off-chain ticket sales. Lastly, the event smart contract, secret-management committee, and credential issuance committees are assumed byzantine fault-tolerant trusted due to the properties of these decentralized systems.

14.2 Attacks and Mitigations

A major goal of this blockchain-based event ticketing system is to prevent off-chain ticket sales. This guarantees the ticket reseller cannot resell event tickets to a buyer for more than the maximum resale price; furthermore, it also guarantees the event organizer receives a percentage of resale royalty on every ticket resale. As such, the ability of the secondary market reseller and buyer to collude was analyzed in detail and mitigation measures proposed. In these scenarios, the goal of the ticket reseller is to resell tickets for prices higher than that set by the event organizer and to avoid resale royalties; the goal of the ticket buyer is to buy tickets to a sold-out event.

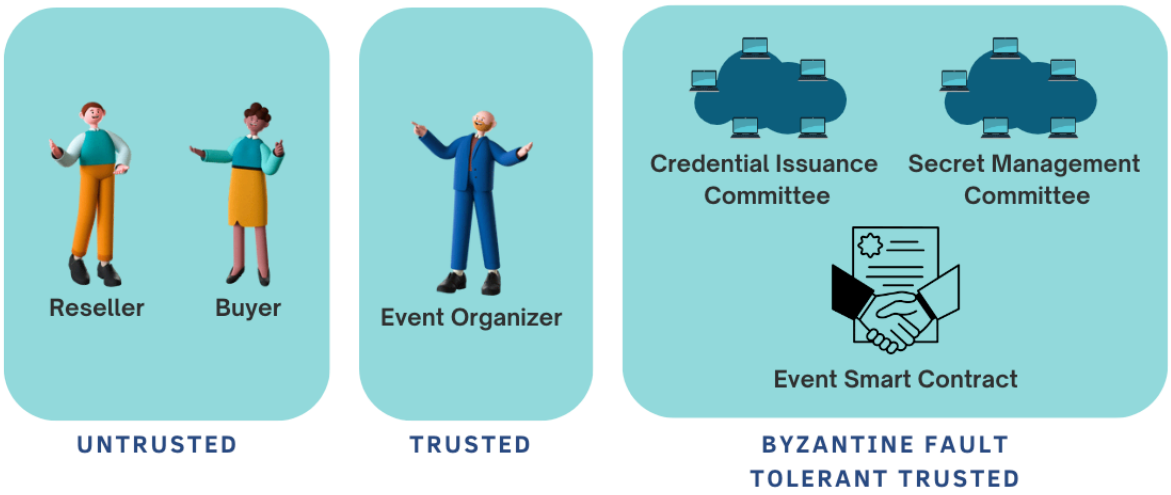


Figure 14.1: System Actors

14.2.1 Strawman I

The first attack analyzed involves the ticket reseller attempting to sell an event ticket to a buyer while requesting an additional payment off-chain. This attack is prevented by the identification system and secondary market structure. Due to the identification system, event tickets are connected to user identities. Thus, a ticket reseller cannot resell tickets off-chain as the event ticket would still be attached to the reseller's identity. Because identification cards are checked at the event entrance, the ticket buyer would have no way of accessing the event. Secondly, the secondary market uses the F3B secret-management committee to store encrypted secondary market buy and sell transactions that are then decrypted, shuffled, and executed. Thus, the ticket reseller cannot request additional payments off-chain as they have no ability to choose the ticket buyer.

14.2.2 Strawman II

While Strawman I is prevented by the blockchain-based event ticketing system, the secondary market reseller and buyer are still able to learn information from encrypted transactions sent to the F3B secret-management committee. Specifically, the reseller and buyer can learn how many secondary market transactions are currently stored on Dela. This information would allow the ticket buyer to request ticket owners to resell additional event tickets, thereby increasing the ticket buyer's odds of receiving an event ticket.

For example, suppose 10 encrypted transactions have been submitted to the F3B secret-management committee and are stored on Dela. If we assume the number of secondary sell and buy transactions are randomly distributed, this would mean a ticket buyer has a 50% chance of

receiving an event ticket. If a ticket buyer is willing to pay $1000 more for an event ticket, they are likely willing to pay $100 if they can increase their chances of receiving an event ticket by 10%. Thus, the ticket buyer can pay $20 to five ticket owners who place their tickets for sale. Now, the ticket buyer has increased their chances of receiving an event ticket to 60%.

This attack can be mitigated by submitting additional transactions to the secret-management committee to prevent an attacker's ability to calculate their likelihood of receiving an event ticket. For secret-management committees that are only used by the event ticketing system, dummy transactions can be submitted and stored on Dela. Secondly, secret-management committees that are widely used would store transactions across a wide variety of use cases, not just event ticketing. Thus, in both these cases, the attacker would be unable to calculate their likelihood of receiving an event ticket and unable to solicit ticket owners off-chain.

Chapter 15

Limitations and Future Research Directions

This section presents the limitations of the blockchain-based event ticketing system and future research directions.

The blockchain-based event ticketing system prototype currently assumes that event organizers check identification cards at the event. While 58% of event organizers interviewed already check or are willing to check identification cards at the event entrance, this leaves a sizable chunk who are not. Porting user identities from other sources using trustworthy oracles presents an exciting future research direction. The CanDID identification system recommends the use of DECO and TownCrier to port identities from a variety of oracles such as email addresses, phone numbers, social media accounts, bank accounts, government accounts, and a variety of other methods; however, these oracles cannot currently port identification information [8, 15, 16]. The use of various identification methods should be explored to determine which are most suitable for event organizers not willing to check identification cards at the event entrance.

A second limitation of the blockchain-based event ticketing system prototype is the custodial key management method. Currently, the prototype manages user public and private keys through the use of a database, which creates a single point of failure. If user data leaks from the database, attackers could obtain user private keys thereby taking ownership of their event tickets. While non-custodial key management remains an issue for blockchain-based systems, the CanDID key-recovery functionality could be implemented to allow users to prespecify recovery accounts of their choice, for example using their email or social media accounts. Future research should be conducted to determine secure and usable methods for users to manage their own private keys and to further develop oracles such as DECO or TownCrier to aid in key recovery [15, 16].

The latencies and throughputs of the identification system, Dela, and the secret-management committee must also be improved in order to serve large-sized events. These events often require

tens of thousands of tickets to be purchased simultaneously; moreover, the throughputs of Dela and the secret-management committee would disallow the system from being used in these cases. Furthermore, these events also require tens of thousands of attendees to enter the events; thus, the latency of the identification system could lead to long wait times. Further research should be conducted to scale each of these decentralized systems so that it may serve these large-sized events.

The blockchain-based event ticketing system prototype currently interacts with the Dela blockchain, secret-management committee, and identification system through the command line interface. For the system to avoid single points of failure, separate servers should be created to interact with the Dela blockchain, secret-management committee, and identification system separately. Furthermore, the nodes on each of these decentralized systems should not be located on the same computer hardware. Further research should be conducted to determine scalable methods for the event ticketing system to interact with multiple, separate, decentralized systems.

Part IV

Conclusion

Event Ticketing is a $78 Billion industry globally, with the secondary ticket market accounting for $19 Billion of this [12]. However, event organizers have no control over the secondary ticket market and attendees experience high rates of ticket fraud. In fact, Ticketmaster estimates that bots siphon off 60% of tickets for major events that are then resold at higher prices. Event organizers have no control over these secondary ticket prices and see none of the resale value [3]. Furthermore, 12% of adults in the United States have purchased fraudulent tickets online, creating a lack of trust in the secondary ticket market [7]. Thus, the inability of event organizers to control the secondary ticket market for their own events and the inability of attendees to trust the secondary ticket market both present major challenges in existing event ticketing systems.

NFTickets is a proposed blockchain-based event ticketing company that can solve these issues. Its business use-case was developed through several business objectives. These include interviews and surveys conducted to better understand event organizers and attendees, event ticketing market research, competitor benchmarking, business model development, financial analysis, and steps taken to find potential customers and seek funding for further development. Through this, it was learned that large-sized event organizers do consider secondary market control and ticket fraud as major issues; however, small and medium-sized event organizers consider expanding their audience as the most significant factor in an event ticketing service. After analyzing event ticket market segments, it was determined the short-term target market is small and medium-sized technical event organizers because they are underserved by existing competitors and require fewer resources to serve. Furthermore, it was determined the long-term target market is large-sized event organizers because they would most benefit from improvements in secondary market and ticket fraud. Based on a detail cost and revenue breakdown, it was estimated that NFTickets will be profitable in year 3 and break even in year 4.

The blockchain-based event ticketing system was also designed, implemented, and evaluated. Specifically, the system utilizes an identification system that attaches identities to event tickets in a privacy-preserving manner and a primary and secondary event market that prevents off-chain ticket sales. Through these academic objectives, it was determined the system meets the secondary market control, anti-forgery, off-chain ticket sale prevention, no deposit, and unlinkability properties. However, the blockchain-based event ticketing system faces issues in identification system latency and primary and secondary ticket market throughput that must be addressed before serving large-sized clients.

Bibliography

[1] Martin Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. "MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity". In: *Advances in Cryptology – ASIACRYPT 2016*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 191–219. ISBN: 978-3-662-53887-6.

[2] Live DMA. *The Survey: Facts Figures of Music Venues in Europe*. URL: https://www.live-dma.eu/wp-content/uploads/2018/09/Live-DMA-Survey-report_live-music-venues_data-2015_publication-January-2018.pdf. (accessed: 15.03.2023).

[3] The Economist. *The war on ticket bots is unlikely to be won*. URL: https://www.economist.com/united-states/2017/01/05/the-war-on-ticket-bots-is-unlikely-to-be-won. (accessed: 01.03.2023).

[4] Equidam. *Average Growth Rate for Startups*. URL: https://www.equidam.com/average-growth-rate-for-startups. (accessed: 01.06.2023).

[5] Marcel Keller. *MP-SPDZ: A Versatile Framework for Multi-Party Computation*. Cryptology ePrint Archive, Paper 2020/521. https://eprint.iacr.org/2020/521. 2020. DOI: 10.1145/3372297.3417872. URL: https://eprint.iacr.org/2020/521.

[6] Tralyn Le, Yoohwan Kim, and Ju-Yeon Jo. "Implementation of a Blockchain-Based Event Reselling System". In: *2019 6th International Conference on Computational Science/Intelligence and Applied Informatics (CSII)*. 2019, pp. 50–55. DOI: 10.1109/CSII.2019.00016.

[7] Megan Leonhardt. *About 12 percent of people buying concert tickets get scammed*. URL: https://www.cnbc.com/2018/09/13/about-12-percent-of-people-buying-concert-ticketsget-scammed-.html. (accessed: 01.03.2023).

[8] Deepak Maram, Harjasleen Malvai, Fan Zhang, Nerla Jean-Louis, Alexander Frolov, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller. "CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability". In: *2021 IEEE Symposium on Security and Privacy (SP)*. 2021, pp. 1348–1366. DOI: 10.1109/SP40001.2021.00038.

[9] Ferdinand Regner, Nils Urbach, and André Schweizer. "NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application". In: (2019).

[10] Allied Market Research. *Events Industry Market*. URL: https://www.alliedmarketresearch.com/events-industry-market. (accessed: 15.03.2023).

[11] Statista. *Average ticket price for music tour concert admission from 2011 to 2019 worldwide*. URL: https://www.statista.com/statistics/380106/global-average-music-tour-ticket-price/. (accessed: 01.06.2023).

[12] Statista. *Event Tickets - Worldwide*. URL: https://www.statista.com/outlook/dmo/eservices/event-tickets/worldwide. (accessed: 01.03.2023).

[13] The CMO Survey. *Marketing Spending and Hiring Growth Slows Amidst Economic Uncertainty*. URL: https://cmosurvey.org/. (accessed: 01.06.2023).

[14] Björn Tackmann. "Secure Event Tickets on a Blockchain". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Ed. by Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, Hannes Hartenstein, and Jordi Herrera-Joancomartí. Cham: Springer International Publishing, 2017, pp. 437–444. ISBN: 978-3-319-67816-0.

[15] Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. "Town Crier: An Authenticated Data Feed for Smart Contracts". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS '16. Vienna, Austria: Association for Computing Machinery, 2016, pp. 270–282. ISBN: 9781450341394. DOI: 10.1145/2976749.2978326. URL: https://doi.org/10.1145/2976749.2978326.

[16] Fan Zhang, Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels. "DECO: Liberating Web Data Using Decentralized Oracles for TLS". In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. CCS '20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 1919–1938. ISBN: 9781450370899. DOI: 10.1145/3372297.3417239. URL: https://doi.org/10.1145/3372297.3417239.

[17] Haoqian Zhang, Louis-Henri Merino, Vero Estrada-Galiñanes, and Bryan Ford. "Flash Freezing Flash Boys: Countering Blockchain Front-Running". In: *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. 2022, pp. 90–95. DOI: 10.1109/ICDCSW56584.2022.00026.

[18] Zylo. *Drive Business Impact with Insights from the 2023 SaaS Management Index*. URL: https://zylo.com/reports/2023-saas-management-index/. (accessed: 20.05.2023).

Appendix A

Project Files, Setup, Run Event Ticketing System

This appendix presents the project folder structure and files, the project setup, and how to run the blockchain-based event ticketing system.

A.1 Project Files

The project folder structure and files are outlined below:

- backend
  - credentials
    - credentials.json: This file contains the connection string to connect to the MongoDB database instance, and should thus be kept secret.
  - dela
    - contracts
      - event: The event folder contains the event smart contract used for the primary and secondary ticket markets, the event smart contract controller, and unit testing for both the smart contract and controller.
    - dkg: The dkg folder contains the F3B secret-management committee and identification system credential issuance committee implementations. The existing dkg infrastructure was used to apply additional credential issuance committee functionality including issuing and verifying the master and event credentials.
    - test: The test folder contains integration tests for the event smart contract as well as throughput measurement tests for the primary and secondary ticket markets.

  - mpspdz: The mpspdz folder contains the implementation of the user identification deduplication, specifically computing a hash of the user's identification using secure multi-party computation.
    * Player-Data: The Player-Data folder is where user identification secret shares are written to so that MP-SPDZ nodes can read from these files.
    * Programs/Source
      · prf_mimc_mine.mpc: This file contains the implementation of the MiMC Pseudo-Random Function, used to compute the hash of the user's identification.
  - routes
    * routes: The routes folder handles all requests sent to the web backend server and returns responses. These routes receive HTTP Requestsfrom the web frontend; communicate with the identification system, secret-mangement committee, and Dela blockchain; and return HTTP Responses to the web frontend.
    * objects: The objects folder contains event and user classes that are used to interact with the MongoDB database event and user tables, respectively.
  - setup_dela.py: setup_dela.py is run to start the Dela blockchain.
  - setup_dkg.py: setup_dkg.py is run to start the secret-management committee and credential issuance committees.
  - server.py: server.py is run to start the web backend server.
- frontend
  - src
    * pages: The pages folder contains the frontend web pages, such as the landing page, homepage, events page, event page, add event page, and admin page.
    * components: The components folder contains React components reused throughout the web frontend.
    * helpers: The helpers folder contains api.js which is used to send HTTP Requests to the web backend and read HTTP Responses. It also contains context.js, which is the global storage for the frontend.

A.2 Setup the Project

Prior to running the blockchain-based event ticketing system, the web frontend, web backend, and Dela blockchain must be setup and dependencies installed.

A.2.1 Setup Web Frontend

The frontend React application can be found in the $frontend$ directory. Install all dependencies as follows:

```
cd frontend
npm install
```

A.2.2 Setup Web Backend

The backend Flask application can be found in the 'backend' directory. Install all dependencies as follows:

```
cd backend
pip3 install -r requirements.txt
```

A.2.3 Setup Dela

The project was developed using Go v1.18, consistent with the F3B implementation. The project can be built using the project Makefile.

1. Install Go v1.18.
2. Install the $crypto$ utility from Dela:

   ```
   git clone https://github.com/dedis/dela.git
   cd dela/cli/crypto
   go install
   ```

   Go will install the binaries in $GOPATH/bin, so be sure this it is correctly added to you path (e.g. export PATH=$PATH:/Users/user/go/bin).

A.2.4 Setup Number of Nodes and Ports

The ports used for the backend server, dela nodes, and identification system nodes can be found and updated in $backend/setup\_info.json$. The ports used for the frontend can be found in $frontend/src/helpers/api.js$. Ensure the $server\_port$ in $backend/setup\_info.json$ matches $this.url$ found in $frontend/src/helpers/api.js$ so the frontend and backend can communicate.

A.3 Run the Project

To run the project, open four separate terminals, which will be used for the Dela blockchain, identification system, frontend, and backend, respectively.

In the first terminal, run the dela blockchain as follows

```
cd backend
python3 setup_dela.py
```

In the second terminal, run the identification system credential-issuance committee as follows

```
cd backend
python3 setup_dkg.py
```

In the third terminal, run the web backend server as follows

```
cd backend
python3 server.py
```

In the fourth terminal, run the web frontend as follows

```
cd frontend
npm start
```

This will run and automatically launch the web application on $http://localhost:3000$. Now you can create events and buy and sell tickets on the primary and secondary ticket markets!