Securing Authenticity in Secondary Market Luxury Goods Auctions: A Binance Smart Chain-Based Blockchain Solution with Advanced Cryptographic Techniques

MSc Research Project
Cloud Computing

Animesh Tewari
Student ID:22247963

School of Computing
National College of Ireland

Supervisor: Prof. Sean Heeney

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Animesh Tewari
Student ID:	22247963
Programme:	Cloud Computing
Year:	2024
Module:	MSc Research Project
Supervisor:	Prof. Sean Heeney
Submission Due Date:	12/08/2024
Project Title:	Securing Authenticity in Secondary Market Luxury Goods Auctions: A Binance Smart Chain-Based Blockchain Solution with Advanced Cryptographic Techniques
Word Count:	7624
Page Count:	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	12th August 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing Authenticity in Secondary Market Luxury Goods Auctions: A Binance Smart Chain-Based Blockchain Solution with Advanced Cryptographic Techniques

Animesh Tewari
22247963

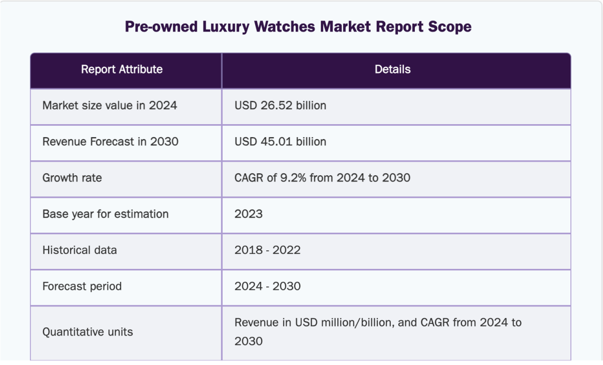
Abstract

With the advancement of Blockchain technology and its usage, an area of improvement was identified, where with the use of this advanced technology, more secure and reliable systems can be built in order to solve a specific problem within the resale luxury goods market. One of the biggest issues that the luxury brands have been facing, in resale market, is counterfeiting. Due to the fake products, circulating the market, not only the reputation of these brands, built over the years with exclusivity and great quality products, is destroyed but these products also impact the customers' trust and loyalty towards the brand. Since, the resale market of luxury goods, especially the luxury watches, is ever increasing, we can use Blockchain to counter this issue of counterfeit products. This technology has potential to make a great impact, by helping verifying the authenticity of luxury products, that has been put up for sale.

In this research, a blockchain-cloud off-chain authentication mechanism for E-Auction system is built, with the help of smart contracts that helped verify the authencticity of luxury products, that their sellers want to put up for auction. The research also helps compare the usage of Ethereum, used to build some of the initial blockchain e-auction systems, with Binance Smart Chain. The metrics from the Experiment(6.2), of this paper, clearly indicate why Binance Smart Chain, when used with advanced cryptographic techniques like SMPC, can help build more scalable, efficient and reliable systems, as compared to Ethereum. The experiments showed around 30% reduction in the gas cost and about 80% reduction in processing time when opting Binance Smart Chain for authentication with SMPC involved.

1 Introduction

Luxury products have a promising market in the world for the kind of craftmanship and exclusivity they bring to the table. They interest customers of various strata by motivating them to use the superior quality they offer. Also, the companies that offer these kinds of products, they make sure to build loyalty and trust with their customer, enhancing the want multifolds. However, such kinds of products are mostly targeted for the wealthy population who don't care about the price of the product but instead are more interested in the uniqueness, rarity of the product, be it in terms of the idea behind



Pre-owned Luxury Watches Market Report Scope

Report Attribute	Details
Market size value in 2024	USD 26.52 billion
Revenue Forecast in 2030	USD 45.01 billion
Growth rate	CAGR of 9.2% from 2024 to 2030
Base year for estimation	2023
Historical data	2018 - 2022
Forecast period	2024 - 2030
Quantitative units	Revenue in USD million/billion, and CAGR from 2024 to 2030

Figure 1: Pre-owned Luxury Watches Market Report Scope by Grand View Research

the product, the material used in the product etc. Not more than a year ago, an article about the glocal luxury goods market size valuation was published [1]. The key highlight was the luxury goods market was about USD 272.74 billion in size in 2022 and is expected to grow 1.5 times in size by 2030, concluding a compound annual growth rate (CAGR) of 4.7 percent during the forecast period.

However, it's not just the primary market that has got such traction, the secondary market as well is growing at an unprecedented rate [2] even when the secondhand luxury products' market has not been supported by well by luxury brands. With pre-loved luxury goods sold at a fraction of the retail price, making it accessible to a larger audience, times have changed and demand for secondhand products has increased steeply. Another report by thredUP's 2022 resale report [3], the global secondhand market is expected to grow 127% by 2026. That's 3x faster than the global apparel market overall. The global pre-owned luxury watches market was valued at USD 24.38 billion in 2023 and is expected to grow at a compound annual growth rate (CAGR) of 9.2 percent from 2024 to 2030. In recent years, market for pre-owned luxury watches has experienced astonishing growth, due to which forward-thinking luxury brands are seeing an increase in consumer demand for pre-owned luxury products and are becoming more inclusive of this resale market. For instance, in August 2023 [4], Watches of Switzerland launched a pre-owned selection of luxury timepieces that can be shopped online. Pre-owned watches have been inspected and certified as authentic and come with a twelve-month warranty.

By owning their secondhand market, luxury brands can retain control of their brand in terms of pricing structure and make sure the exclusivity of their products remains intact. While the entering in the resale market is promising to these luxury brands[5], there are also challenges and considerations. One of the major challenge is maintaining brand integrity and authenticity of the products. Counterfeit products and unauthorized sellers pose a significant risk in the pre-owned market. These products, if sold, can impact consumer experience, damage brand reputation and crush the consumer's trust.

As consumer demand for luxury watches continues to rise as stated by a report from

[1] https://www.fortunebusinessinsights.com/press-release/global-luxury-goods-market-10489

[2] https://www.businessresearchinsights.com/market-reports/secondhand-luxury-goods-market-102564

[3] https://www.thredup.com/resale/2022/size-and-impact

[4] https://www.grandviewresearch.com/industry-analysis/pre-owned-luxury-watches-market-report

[5] https://web-assets.bcg.com/img-src/BCG-Why-Luxury-Brands-Should-Celebrate-the-Preowned-Boom-Oct-2019$_{t}cm9-232622.pdf$

Deloitte (2023), luxury brands are working on establishing rigorous authentication processes and partnering with trusted platforms to authenticate and sell their pre-owned items. The sale of counterfeit products, in the resale market, poses a significant threat, to these brands, which is why working to identify these fake products and stopping them from being sold to loyal customers becomes a big challenge to solve. Hence, the need for a robust mechanism to verify authenticity in the secondary market has become increasingly important.

While there are blockchain-based authentication methods as stated in Zimmermann et al. (2023), they lack in terms of scalability, time-consumption and absence of dedicated inbuilt authentication mechanism in auction systems. This opens the door to explore the space for a solution which require less resources to do the authentication. In this research, a modern approach to tackle counterfeiting and build trust within the luxury watch secondary market through the integration of blockchain technology is mentioned. The approach utilises the Binance Smart Chain blockchain for its scalability and efficiency, combined with a cloud based implementation of secure multiparty computation (SMPC) and touches upon Zero-Knowdedge Proof as an idea. These set of technologies involved aim establish a secure, transparent, and decentralized platform for auction systems, where the authenticity of luxury watches can be verified automatically at the time of selling or listing the watch, ensuring genuine products for the buyers.

Objective:

- Design and auction system with focus on an inbuilt blockchain-cloud based watch authentication mechanism using Binance Smart Chain(BSC) and AWS serverless services to prove the authenticity of luxury watch being listed on it.
- Evaluate the proposed smart contracts and utilities to assess their performance through tests.

Research Question: The research is guided by the following question: How can the Binance Smart Chain combined with AWS serverless services and secure multiparty computation, improve the authentication process, in the luxury watch resale market and help in tackling counterfeiting?

Document Structure: The structure of the rest of the document is organized as follows:

1. **Literature Review** - Reviews relevant literature to identify gaps and establish the theoretical ground for utilising Binance Smart Chain with cryptographic techniques.
2. **Methodology** - Elaborates on the proposed methodology, architecture, and model of smart contracts designed for the system.
3. **Design Specification** - Details more around each of the components used in the systems and why those were chosen.
4. **Implementation** - Outlines the implementation details like the relevant methods and what is their significance.
5. **Evaluation** - Details around the tests performed on the proposed system and their results.

6. **Conclusion Future work** - Details around the future scope and directions of the work.

2 Related Work

This section outlines different fronts that were explored before building the proposed system. It is starts with discussing the traditional techniques of E-Auction systems in order to provide some background for the present work in this field. Continuing, The idea around how blockchain technology can be used to create e-auction platforms has been discussed. Then there has been a discussion on blockchain based auction systems, blockchain usage in supply chain for counterfeit prevention and the integration of advanced cryptographic techniques in blockchain. This approach of reviewing was considered important to address each critical component of the research question.

2.1 Traditional E-auction Systems: Integrating Blockchain Technology

In early blockchain-based auction systems, in order to improve transaction security, auction procedures, and guarantee the integrity of each sale, Ethereum's smart contract technology was used. The following sections talks about how these early implementations have helped gather the foundational idea on how to use blockchain technology for auction systems, focusing on both the areas that were explored and the limitations that was faced.

Research such as Qusa et al. (2020), Chen et al. (2018), and Omar et al. (2021) helped identify blockchain's potential to secure transactions and automate elements of auction workflow like placing the bids, choosing highest bidder etc. This further improves the performance and trust in the auction ecosystem. The work by Galal and Youssef (2019) which was an Ethereum-based solution for sealed-bid auctions suggested that blockchain can be used to maintain auction's integrity by blocking bidders from knowing competing bids, hence helping securing the bid confidentiality. This solution made blockchain to be a fair choice in improvising auction frameworks to ensure fairness and security.

While these advancements are optimistic sight to look at, there is no second thought on that Ethereum has it owns scalability and performance challenges. The studies by Chen et al. (2018) and Omar et al. (2021) both inform about the scaling issues that Ethereum-based systems have when there is high volume of transactions to handle. This highlights that on a long run, when the scale increases or when auction systems become more complex, Ethereum might not be the fair choice to handle real time bidding for example. Moreover, Chen et al. (2022) explores the idea of combating counterfeit luxury goods using blockchain technologies. Hence, these studies suggest that it's now time to explore solutions which can handle transactions quickly and possibly at lower costs.

To address the performance challenges, an alternative to Ethereum is Binance Smart Chain[6]. Binance Smart Chain is highly scalable, managing more number of transaction than Ethereum and is Ethereum Virtual Machine compatible meaning that it is very convenient to move Ethereum Applications to Binance Smart Chain with minimal changes. This is important to quickly build upon the understanding gathered from the studies

[6] https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md

by other researches in the Ethereum space and port those understanding fairly easily to Binance Smart Chain.

Overall, There has been a considerable amount of work in the space of building ethereum based auction systems, keeping in mind that bidder stays anonymous and there is transaction security to ensure the user experience is preserved. However, the scalability concerns shed light on the need for a more efficient solution that is more than just security. The idea that has been discussed in this paper tackles the scalability concerns, adds efficiency to the system as well as gives a fair starting direction for an integrated cloud based off chain authentication mechanism with advanced cryptography method, which serves as an anti-counterfeiting layer.

Hence, it is necessary to explore relevant advanced cryptographic methods, to improve the security and privacy of blockchain-based luxury watch auction platforms. But discussing on the cryptography front, it is important to understand blockchain's impact on maintaining integrity in supply chain and anti-counterfeiting as these two features are critical for any e-auction system.

2.2 Blockchain's Impact on Supply Chain Integrity and Counterfeit Prevention

Usage of blockchain technology in the supply chain management space had led to significant decrease in the number of counterfeit goods as it helps track the history of any product, starting from the stage of raw material collection to till the hands of the consumer. Such application of blockchain is very important in case of luxury items where the products can be extremely expensive and exclusive.

The study by Thakkar et al. (2021) suggested a blockchain-based framework that serves as great example supporting the theory of blockchain technology improving supply chain management systems . The system, mentioned in Thakkar et al. (2021), guarantees the integrity of supply chain records. This system maintains a verifiable record of commodities, from manufacturing to sale, by utilising the immutable characteristics of blockchain transactions, which is essential for verifying the legitimacy of things in auction systems. Stakeholders may safely confirm the legitimacy of the things up for sale by having a transparent perspective of the product's route, which lowers the danger of selling counterfeit goods.

In a similar vein, Sun et al. (2023) describes a decentralised application that authenticates products, using QR codes connected to blockchain entries, making the whole authentication process more efficient and secure. This method not only helps in performing verification of good but also increases user engagement, by making the authentication procedure much simpler. However, while these developments are significant accomplishments, they mostly concentrate on basic security features and transparency. They do not entirely utilize the cutting-edge cryptographic approaches, such as zero-knowledge proofs (ZKP) and secure multi-party computing (SMPC), that offer further levels of security and privacy.

These research show the importance of blockchain in helping secure the entire supply chain pipeline and help keep the authenticity of the product intact. However, these studies also provide details around the gaps that are there. The idea of integrating advanced cryptography techniques, such as SMPC, points towards the next step in developing more secure and transparent auction platforms. This research addresses these gaps by integrating cloud based cryptographic components in the auction system to do off chain authentication of the listed products on auction systems, particularly those dealing with the resale of luxury items.

2.3 Cryptography's Role in Auction Security and Privacy

Integrating cryptography in the pipeline of luxury products resale helps in solidifying data privacy and integrity in blockchain based e-auction systems. The application of SMPC, within blockchain, helps in creating a collaborative computation environment, where multiple parties compute a function over their inputs, while also maintaining that the inputs are not leaked. Zhu et al. (2018) mentions about the using SMPC to protect the bidding process in an auction system. It discusses that for a fair auction system, it is important to keep the bid values as well as the bidders identity confidential and how SMPC can be used to achieve that. However, it strongly puts forward the need for better SMPC integration, possibly the ones that don't compromise on transaction speeds or system scalability.

Similarly, using ZKPs enable a party to prove the truth of a statement without revealing any important information, beyond the statement's validity. In auction systems, for verifying the authenticity of luxury watches, this is quite advantageous as it this technique doesn't expose sensitive items or seller details. Yang et al. (2020) fairly discusses at length about the extent of ZKPs applications, in combination with SMPC, to boost privacy in blockchain networks. However, there has been no evidence on directly using ZKPs with luxury resale auctions, providing the ground for exploration and assessing it's potential in authenticity verification.

It is also important to note that from the discussions by de Boissieu et al. (2021) and Klöckner et al. (2023), it is evident that blockchain's is quickly rising in popularity in the luxury watch sector space. It tells about how blockchain easily integrates with other technologies and has helped in combating the issue of counterfeiting and product verification, directly pointing to the importance of cryptography solutions in the luxury watch market or luxury watch auction ecosystem.

Apart from the industry specific insights, Yang et al. (2020) discusses that there is still a gap, both theoretical and practical, in understanding the capabilities of advanced cryptographic method within the luxury watch auction systems, even when there are relevant advancements done in works like Zhu et al. (2018). As different industries have different requirements, it is still challenging to customise cryptographic solutions as per specific privacy necessities without complicating the system and making them difficult to implement.

Although Zhu et al. (2018) made significant advancements, theoretical and practical, a gap continues to exist in fully utilising SMPC and ZKPs within luxury watch auction systems, as examined in Yang et al. (2020) in addition to industry-specific insights. Due to lack of research and exploration, it is still challenging to customise these cryptography solutions to the specific security and privacy necessities, of these auction systems, without excessively increasing their complexity and making them difficult to implement.

Overall, these different set of studies show that overtime blockchain technology has established itself as a great option to build a secure and reliable e-auction systems. There have been some attempts to use advanced cryptographic methods to address privacy and security concerns. The present study uses a variety of cryptographic techniques to improve the authentication and verification processes for premium commodities. This research provides the foundation for using Binance Smart Chain as a blockchain platform that can handle advanced cryptography procedures. This helps tackle the limitations that come Ethereum based auction systems. The scalability and performance issues, that act as a bottleneck, can be handled using Binance Smart Chain, helping build a scalable system that can provide secure seamless transactions, along with features that will combat counterfeiting like an inbuilt product authentication mechanism.

2.4 Research Niche

As talked about in the last sections, the range of researches which were explored helped in getting a clear view of the potential of blockchain technology in the e-auctions systems space. It helped identify the constant pain points of scalability, efficiency and authencity in these auction systems. As established from the research that there has been significant role of blockchain in helping prevent counterfeiting, however it is concluded that using advanced cryptographic techniques in combination with blockchain and cloud can help build a solution which tackles the limitations mentioned before.

Expected Contribution of the Research: The core contributions of this research are:

- **Scalability and Efficiency:** Smart contracts for the Binance Smart Chain that support cloud based off chain luxury watch authentication mechanism.

- **Auction Workflow Architecture** A detailed system diagram as well as interaction details so that it serves as an initial pointer for further research and extensions.

3 Methodology

Considering the gaps that have been identified in the related works, this method uses Binance Smart chain, which essentially support fast processing of transaction at a low price. This is needed to build and support systems that are supposed to handle multiple transactions at the same time, like auction systems. Another important benefit of using Binance Smart Chain is that it provides cross-chain interoperability, which means that it supports working with different chains using bridging protocols and enables user to transfer their assets between them. This brings in the dimension of extensibility to our solution. It is not just using a better chain that solves the existing problems by making the systems faster, but it is also using the advance cryptographic techniques like SMPC etc., that makes the system more secure. These cryptographic techniques helps automates and decentralise the authentication process of the auctioned watch, making it significantly more difficult to list any fake watches on the platform. A high level depiction of the workflow can be seen Figure 2 and below is the details around the workflow:

1. **Register watch for Auction :** End users, who want to auction their luxury watches, initiate the process by registering their luxury watches on the platform. This step involves providing essential details such as serial number. This particular call is being handled by *Watch Smart Contract* which contains methods to take this information and send it for verification. The verification request is submitted to the *Authentication Smart Contract* to initiate the validation of authenticity of the watch. Sellers need to follow this step for every product they want to auction, and the system doesn't support adding details of multiple products at once. This ensures

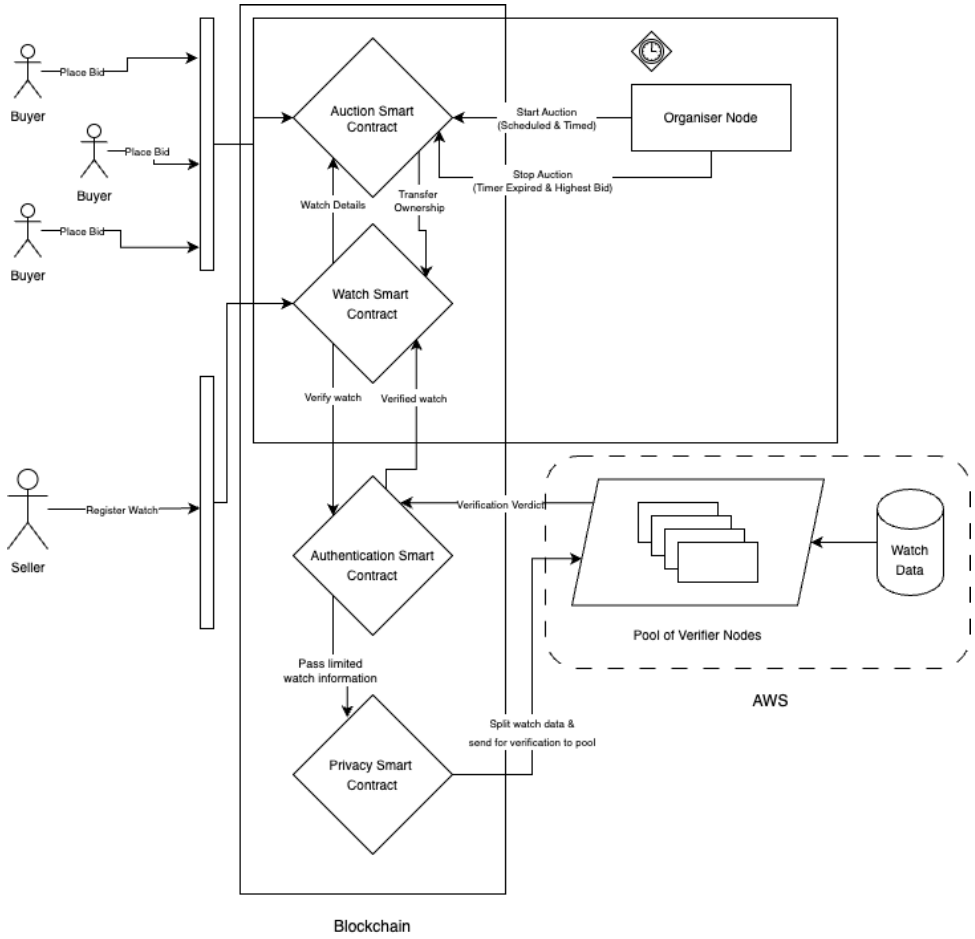


Figure 2: Proposed Workflow

that every process/request verifies and authenticates a single product eliminating any chance of error.

2. **Authentication:** When the request for verification of the product, is submitted by the seller, *Authentication Smart Contract* works as a mediator between the watch smart contract and the privacy smart contract. It is essential to pass in the serial number to the privacy smart contract to use SMPC and verifiy that the watch is genuine or not.

3. **Listing Creation:** Once the product is successfully verified, i.e. it is genuine, the watch details are stored within the *Watch Smart Contract*. An auction listing can then be created in the *Auction Smart Contract*, specifying critical parameters, such as auction start and end times, and minimum bid price.

4. **Auction Process:** During the auction period, participants submit their bids through the *Auction Smart Contract*. The smart contract ensures that all bids are securely and transparently recorded. The highest bid is regularly tracked, and participants are notified on their bid status.

5. **Auction Conclusion:** When the auction ends, *Auction Smart Contract* checks the highest bidder. The contract then handles the automatic transfer of ownership,

updating the *Watch Smart Contract* to reflect the new owner. This transaction is securely recorded on the Binance Smart Chain blockchain.

6. **Ownership Transfer:** The new owner, identified as the highest bidder, gets a confirmation of the ownership transfer. The system ensures that the ownership transfer is accurately handled on the blockchain.

4 Design Specification

As per the discussion in section 3, the proposed solution uses a blend of latest blockchain technology and modern cloud serverless compute storage solutions. Incorporating serverless compute and storage solution is important to make the system robust as it shifts the infrastructure responsibility to the cloud service providers. Any increase in number of requests is also seamlessly handled. This kind of approach is very ideal for an auction system where the number of authentication requests can change depending on the market needs.

The user interface layer, the blockchain layer, and the cloud layer represent the three main layers that make up the system's core architecture. The user interface layer is necessary to communicate with end users, like bidders and sellers. It provides an interface through which one can register watches, place bids, and perform other tasks. This layer communicates with the smart contract layer, which reveals crucial techniques for maintaining the auction system.

The core component of the system is the smart contract layer, which implements the main smart contracts needed for watch registration and verification, privacy-preserving computations, and auction management. These Solidity-developed smart contracts are implemented on the Binance Smart Chain Testnet blockchain.

The cloud layer represents the decentralized compute and the storage layer which provides workforce to execute secure multiparty computation on the watch data and central watch database respectively. The Binance Smart Chain blockchain's high throughput and low latency make it suitable for real-time auction applications, ensuring that the system is able to scale well for decent workloads.

The proposed solution as can be seen Figure 3 has a critical middleware design approach to act as a bridge between the blockchain and the cloud layer. The term "Middleware" describes software that acts as a link between multiple parts or applications in a computer environment. It acts as a link between various systems, apps, or services, allowing data exchange, communication, and interaction. In order to make the complex process of integrating various technologies easier to understand and facilitate their seamless operation, middleware is essential. The main functions of middleware are load balancing, data management, integration support, communication facilitation, and security implementation. These features offer benefits like improved interoperability, scalability, and streamlined development and maintenance procedures. SDKs and libraries are frequently used by middleware to add new functionalities on top of preexisting ones. Similar to the current study, middleware is occasionally created to create an abstraction or wrapper around heterogeneous systems or APIs. A NodeJs-based middleware is created in this study in order to communicate with Binance Smart Chain and the AWS Cloud. The script is created separately for prototyping purposes and uses pre-defined variables for the credentials for the cloud accounts.

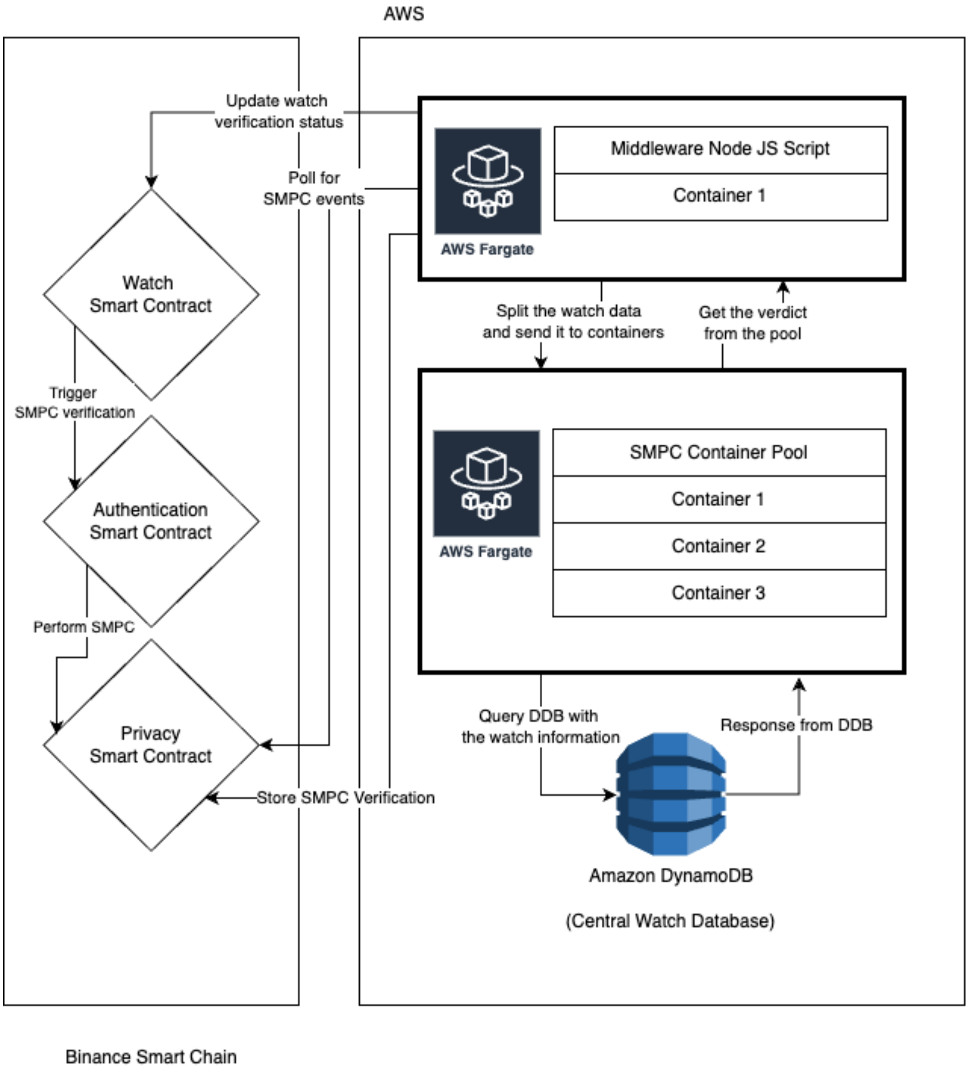


Figure 3: Interaction between the blockchain and the cloud layer using AWS Fargate Poller

There are multiple design consideration which are important to be taken care. First pointer on this is that we are required to work with a chain which has better transaction processing times and provides a fairly decent transaction cost. Solana was considered as a choice earlier as fits the needs required for our system but the problem was solana-test-validator tool has incompatibility with recent Mac Chip and hence, becomes difficult to test solana smart contracts locally before deploying it on the test network. The second best option was the Binance Smart Chain which let's us stay with Solidity for writing the smart contracts. Also, it's easier to test the contracts locally using the Ganache personal blockchain running.

Another vital aspect of the design is to bridge the gap between the blockchain and the cloud layer. This is needed because the smart contract needs to verify the data using the SMPC nodes deployed on AWS Cloud. As we don't have a way in Solidity AWS SDK i.e. smart contracts can't directly invoke something outside the blockchain environment. This led to look for a polling method which can monitor changes in the blockchain environment where the smart contract is deployed and accordingly act on it.

This is aligns well with the characteristic of a middleware. The middleware in our case is a Node.Js script running on a container deploying on AWS Fargate. The smart contracts have been setup to emit signal to notify the polling script to fetch the information from the blockchain. This allows our middleware to take the control from the blockchain environment to the cloud environment.

Once the middleware has been notified, it can pass on the information to containers deployed on the AWS fargate to do the SMPC computation. At this point, the AWS Fargate containers can easily interact with the Amazon DynamoDB service where the central watch database is stored. The key idea around opting for a NoSQL Database like Amazon DynamoDB was that the watch details gathered from different authentic sources might have different fields and also it's just not the information that is being gathered from different sources but also as the watches have different designs, they have some core properties linked to them and some extra ones which might be missing for a standard watch for example number of diamond pieces, weight of each diamond piece etc. Another reason why Amazon DynamoDB is a perfect fit for our system as It can be easily concluded that the database needed for the use case is going to be ready-heavy and Amazon DynamoDB can autoscale as per the increase in the load.

It is important to also talk about why containers are being used for doing the SMPC. To be as much fair, it is important for all the SMPC participating components to have a similar environment, setup etc. For such a requirement, containerisation is a good solution as it provides the isolation needed for the components to not interact or impact the computations done by each nodes. It also provides consistency, ease of deployment which means can be quickly distributed across various infrastructures, scalability to name a few benefits in keeping the system reliable and available.

5 Implementation

5.1 Auction Smart Contract

This smart contract is created to handle the auction process for watches and uses olidity 0.5.16. The smart contract includes a structure named Auction which stores vital details of each auction such as the seller's address, starting price, auction end time, highest bidder's address, etc. To track the current auctions, a map has been used which used the watch serial number as the key and entire auction data as the value. The smart contract has four methods to carry out the auction process. The first *startAuction* function starts a new auction. A unique watch serial and parameters like the start price and auction duration are sent to it to link the watch with corresponding auction data. The second *placeBid* method helps the participants to place bids, implementing rules like bids must exceed the current highest bid etc. The third method *endAuction* is used to end an auction. The method also ensure that the seller can end it and transferring the highest bid amount to the seller if there is a highest bidder. Events such as `AuctionStarted`, `BidPlaced`, and `AuctionEnded` have also been added to for now just log actions in the auction environment and can be later extended for needed event based actions. Also, *getAuctionDetails* function provides public access to view auction elements. Overall, the Auction smart contract helps the the entire auction lifecycle by providing all the necessary methods to correctly manage all the interactions during the auction process.

5.2 Watch Smart Contract

This smart contract is for keeping the record of all the genuine watches in the auction environment. It uses Solidity 0.5.16 and is deployed on the Binance Smart Chain blockchain. The core idea of this smart contract is to provide all the needed methods for interaction with the watch data like what all watches are there in the environment, any details about a specific watch etc.

A custom structure called the `WatchDetails` is used to store the watch data. It contains fields like serial number, manufacturer signature, and verification status encapsulated in it. This ensures that each watch is tracked in the auction system correctly. This is the smart contract that contains the method for invoking the off-chain cloud based verification of the watch. The method is called *registerWatch*. As the name suggests, it is called to register any watches in the auction system. The moment it is invoked, it also triggers a verification of the watch by contacting with other relevant smart contracts like Authentication smart contract.

Continuing on the process of verification, the contract contains a method called *updateVerificationResult*. It is important to mention this is because it is responsible for updating the verification status of a watch asynchronously i.e. it is called by a cloud based poller script to update the watch details with the verification verdict from the SMPC nodes.

For getting the watch information, the contract provides the *getAllWatches* method, to get information on all the verified and genuine watch in the system.

As mentioned earlier, Watch Contract starts the verification but the verified method is a part of the authentication contract so watch contract interacts with another smart contract to pass the watch data to it so that it can be used for further verification.

Overall, the watch smart contract plays a vital role as it is fundamental to the auction systems as everything revolves around the watch like the bidding, the authentication etc.

5.3 Authentication Smart Contract

A smart contract to work as a mediator between the watch contract and the privacy contract. Again, it is written in Solidity. The primary method, *triggerSMPCVerification*, starts the verification by passing the serial number of the watch to the Privacy Contract, which has the SMPC method.

Secure Multi-Party Computation also known as SMPC, is mainly used for verification in smart contract. In order to verify the entered information, of the luxury product, in a decentralized manner, SMPC is used. It distributes this computation, the process of authentication, across multiple nodes, improving the security and reliability and eliminating any single point of failure. Every single verifier node, receives a part or subset of the input data, containing the information of the watch, and it then verifies the received information against the watch database. This helps in ensures that the nodes work fairly and reach a conclusion, above a certain threshold, for the watch to be considered authentic or genuine. This decentralized computation is managed through the *performSMPC* method in the Privacy Contract, which the Authentication Smart Contract triggers using the *triggerSMPCVerification* method.

After the verification of the watch, *confirmAuthenticity* method is used to check the result of the SMPC process by sending in the serial number. If the verification is successful, this means that the watch was genuine and this smart contract will return a positive result.

In nutshell, the Authentication Smart Contract comes into picture to ensure the security and integrity of the watch verification process. Using the cryptographic techinque called SMPC, this contract avoids revealing the confidential watch information while also ensuring the authenticity of each watch listed for auction.

5.4 Privacy Smart Contract

This contract is important as it emits the event to perform SMPC which the off chain poller on the cloud is monitoring. The moment the perform SMPC is emitted, the poller fetches the data from the smart contract to process it.

The data structures, used by this contract, helps in storing the SMPC verification results. The contract, using the `SMPCData` structure, contains the serial number of the watch and the verification result, that whether the watch is validated and is genuine. This data is stored as a Map.

Once the event is emitted and the SMPC process is successfully completed, the method named *storeSMPCVerification* is used to store the results of the verification, in the above mentioned data structure. Both the details - the watch's serial number and a boolean value, suggesting its authenticity and whether the watch has passed the SMPC verification, are passed as inputs to this method or function and is then stored in the contract's mapping data structure, as mentioned earlier. Once this data is stored, an `SMPCVerificationStored` event is emitted to record this action on the blockchain.

At the end, *verifySMPC* method handles the last step of the verification process. The result of the verification check, using SMPC, and whether a watch is genuine or not, this information can be accessed or viewed by other contracts or users, with the help of this method. The entity that wants to check the verification result of a particular watch, can simply provide its serial number and this method will return whether the watch is authentic or not, by returning a boolean value. 0 for false(fake) and 1 for true(genuine).

Overall, privacy contract is the end of the blockchain layer and is read by the cloud poller for events. By implementing and managing the SMPC operations, this contract plays a vital role in confirming the authenticity of watches while maintaining the confidentiality of their data.

5.5 Cloud based polling script

This is a Node JS script which has been deployed on AWS Fargate to act as a bridge between the blockchain and the cloud layer. As smart contracts cannot directly invoke an AWS service, it was important to add a middleware that could take care of this.

This script runs on AWS Fargate and monitors the privacy smart contract for the perform SMPC event. The moment a perform SMPC event is emitted, it picks the watch information on which it needs to do the SMPC and further moves this data to the SMPC nodes that verify this data using the central watch database on DynamoDB. It is important to mention that the script uses the node real websocket connection to poll the smart contracts for event as it is not possible with the regular BSC testnet which only provides HTTP connection so subscription of events is not possible with that.

5.6 SMPC Script

This is a fairly simple node JS script running as a container on AWS Fargate. It checks the input data with the central database table on the DynamoDB and provide a true verdict if the inputted data was found in database else false will be returned.

5.7 Central Watch Database

This is a Amazon DynamoDb table that contains a dump of watch dataset collected from resources online like Kaggle. The data was free to use and modify. Also, it was created using AWS CLI and a python helper script was used to dump data into it. An important aspect of choosing DynamoDB was it's scalability advantages which help in avoiding bottlenecks in the system.

6 Evaluation

This section is to talk about the results that have been obtained after creating the luxury watch authentication mechanism on Binance Smart Chain. The aim is to check the system in terms how much time it takes to confirm the authenticity of the watch, the average amount of gas used during a typical verification, scalability and reliability.

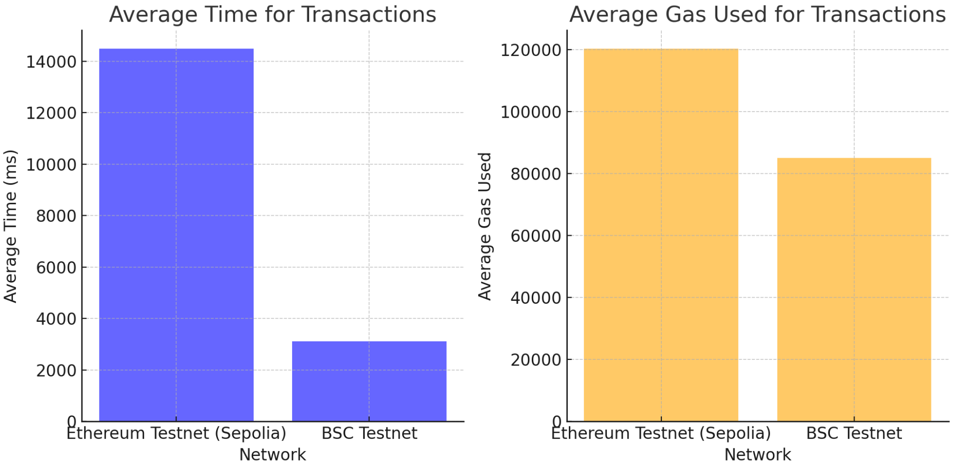
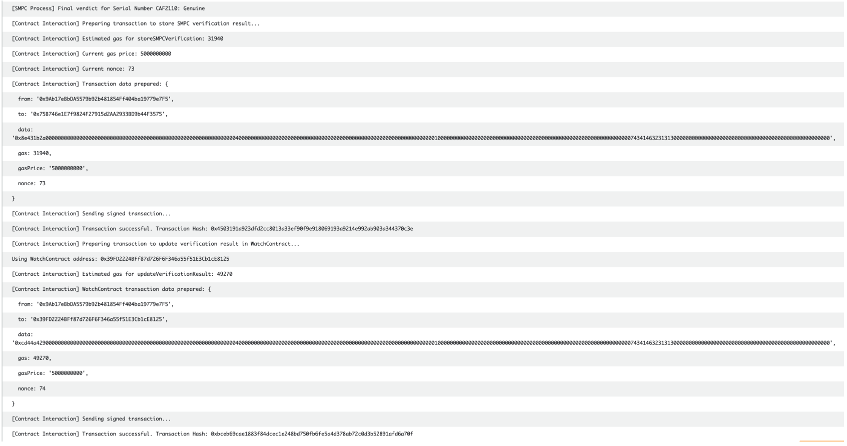


Figure 4: Performance metrics for deployed contracts on Ethereum Testnet and Binance Smart Chain Testnet

6.1 Experiment / Deploying on the Ganache

The primary evaluation for the smart contracts was done using Ganache, which is a personal blockchain to test Ethereum based smart contracts locally. After deploying the smart contracts locally using truffle migrate, the smart contracts were deployed firstly on the Sepolia testnet. It was important to review the performance on Ethereum Testnet Sepolia so that there can be a clear picture about the performance improvements switching from one chain to another can bring. As in the system, we have a poller to fetch and act upon events that the smart contract emits, a websocket connection was needed poll the information to the cloud. This was done using the Infura websocket for Ethereum Testnet Sepolia. Similary, for the Binance Smart Chain testnet, a websocket provided by Node Real was used.



```
[SMPC Process] Final verdict for Serial Number CAF2110: Genuine
[Contract Interaction] Preparing transaction to store SMPC verification result...
[Contract Interaction] Estimated gas for storeSMPCVerification: 31940
[Contract Interaction] Current gas price: 5000000000
[Contract Interaction] Current nonce: 73
[Contract Interaction] Transaction data prepared: {
  from: '0x9Ab17eBbDA5579b92b481854Ff404ba19779e7F5',
  to: '0x75B746e1E7f9824F27915d2AA2933BD9b44F3575',
  data:
'0x8e431b2a00000000000000000000000000000000000000000000000000000000000000400000000000000000000000000000000000000000000000000000000000000001000000000000000000000000000000000000000000000000000000000000000743414632313130000000000000000000000000000000000000000000000000',
  gas: 31940,
  gasPrice: '5000000000',
  nonce: 73
}
[Contract Interaction] Sending signed transaction...
[Contract Interaction] Transaction successful. Transaction Hash: 0x4503191a923dfd2cc8013a33ef90f9e918069193a9214e992ab903a344370c3e
[Contract Interaction] Preparing transaction to update verification result in WatchContract...
Using WatchContract address: 0x39FD2224BFf87d726F6F346a55f51E3Cb1cE8125
[Contract Interaction] Estimated gas for updateVerificationResult: 49270
[Contract Interaction] WatchContract transaction data prepared: {
  from: '0x9Ab17eBbDA5579b92b481854Ff404ba19779e7F5',
  to: '0x39FD2224BFf87d726F6F346a55f51E3Cb1cE8125',
  data:
'0xcd44a42900000000000000000000000000000000000000000000000000000000000000400000000000000000000000000000000000000000000000000000000000000001000000000000000000000000000000000000000000000000000000000000000743414632313130000000000000000000000000000000000000000000000000',
  gas: 49270,
  gasPrice: '5000000000',
  nonce: 74
}
[Contract Interaction] Sending signed transaction...
[Contract Interaction] Transaction successful. Transaction Hash: 0xbceb69cae1883f84dcec1e248bd750fb6fe5a4d378ab72c0d3b52891afd6a70f
```

Figure 5: Logs from the Poller Container after successful SMPC computation with 3 containers on AWS Fargate

6.2 Experiment / Deploying on the Binance Smart Chain Testnet

After the successful deployment of smart contracts on both of the testnet, A node Js script was run using the truffle exec command which registered around 1000 watches on each of the network to understand the performance different and utility of the idea. The obtained average time for completing the registration, which means sending for verification to cloud, performing SMPC and giving a verdict around if it's genuine or not and if genuine, adding it to the watch smart contract list of genuine watches, and the amount of gas used in this process can be seen in Figure 4. As a conclusion, moving to a different chain while reusing the ethereum based smart contracts led to around 30% reduction in the gas cost while also decreasing the process time to about 80%.

6.3 Experiment / Testing AWS Fargate Poller SMPC containers

Keeping scalability in mind, AWS Fargate is used to host the SMPC containers, so adding new SMPC containers in the system is fairly easy to do based on the CPU load that the container has. The testing in terms of scalability was done with Amazon Dynamo DB to handle concurrent read requests from the SMPC containers and as the DynamoDB is set to On-Demand, it is able to scale well with multiple watch registration request. One of the fallbacks that was seen was that there is currently no mechanism to scale the poller so if there are a multiple events that needs to be picked up from the smart contract, there is currently just single poller processing requests sequentially. Please refer to 5 showcasing successful blockchain event tracking and SMPC on the cloud.

6.4 Discussion

Based on the findings, gathered while building the system, are that the system was able to perform better than the Ethereum testnet, as stated in the previous section. The research focused more around creating an inbuilt off-chain authentication mechanism with the help of serverless cloud technologies. The major takeaways from the research and creating of the prototype are that it created a middleware approach for successfully executing an asynchronous verification of listed watches on cloud, contrary to the synchronous nature of smart contracts. It also used a different blockchain to validate performance improvements that can happen in the authentication of watches. However, there were certain design challenges that were faced like the current approach with the poller can support limited concurrency, and to increase the supported concurrency, there should be a container management system on top the containers which are running. For example, there needs to be certain design considerations around not processing the same event twice when there will be multiple pollers etc. Overall, this idea is a Proof-of-Concept that worked fine during the initial run but requires a range of refinement to be called as a product. Also, the idea of ZKP and auctioning was not thoroughly touched upon to create a fully working end-to-end application, but a core component of the system was created, using SMPC and cloud based services, and tested for real-life application.

7 Conclusion and Future Work

This research aimed created a mechanism for authenticating luxury watches in the secondary market using SMPC on Binance Smart Chain. The objective was to create an automated authentication mechanism for a secondary market auction system for luxury watches which can help validate the genuinety of watches that are being listed. The primary challenge was that there were no automated authentication system, using advanced cryptographic techniques, as well as there were scalability challenges of the used blockchains. The proposed design overcomes these challenges of authentication, by using SMPC, and does decentralised verification of a watch and uses an alternative to Ethereum, named Binance Smart Chain(BSC). The BSC provides a fast, low-cost, and scalable blockchain platform for decentralised application.

There are a range of directions that can be explored to further the research. First would be to test the idea for concurrency thoroughly. Second would be to update the SMPC implementation, which would mean using more data, more number of nodes and also adding the element of Zero Knowledge Proof(ZKP), by restricting what the user provides at the time of registering the watch.

References

Chen, C. L., Guo, L.-H., Zhou, M., Tsaur, W.-J., Sun, H., Zhan, W., Deng, Y.-Y. and Li, C.-T. (2022). Blockchain-based anti-counterfeiting management system for traceable luxury products, *Sustainability* **14**(19): 12814.
URL: *https://doi.org/10.3390/su141912814*

Chen, Chen and Lin (2018). Blockchain based smart contract for bidding system, *2018 IEEE International Conference on Applied System Invention (ICASI)*, IEEE, Chiba,

Japan, 13 - 17 April 2018, pp. 208–211.
URL: *https://doi.org/10.1109/ICASI.2018.8394569*

de Boissieu, E., Kondrateva, G., Baudier, P. and Ammi, C. (2021). The use of blockchain in the luxury industry: Supply chains and the traceability of goods, *Journal of Enterprise Information Management* **34**(5): pp. 1318–1338.
URL: *https://doi.org/10.1108/JEIM-11-2020-0471*

Deloitte (2023). The deloitte swiss watch industry study 2023, Available at: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/consumer-business/ch-deloitte-swiss-watch-industry-study-2023_EN.pdf. Accessed 10 April 2024.

Galal, H. S. and Youssef, A. M. (2019). Verifiable sealed-bid auction on the ethereum blockchain, *International Conference on Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC*, Springer, Nieuwpoort, Curaçao, 2 March 2018, pp. 265–278.
URL: *https://doi.org/10.1007/978-3-662-58820-8_18*

Klöckner, M., Schmidt, C. G., Fink, A., Flückiger, L. and Wagner, S. M. (2023). Exploring the physical–digital interface in blockchain applications: Insights from the luxury watch industry, *Transportation Research Part E: Logistics and Transportation Review* **179**: 103300.
URL: *https://doi.org/10.1016/j.tre.2023.103300*

Omar, I. A., Hasan, H. R., Jayaraman, R., Salah, K. and Omar, M. (2021). Implementing decentralized auctions using blockchain smart contracts, *Technological Forecasting and Social Change* **168**: 120786.
URL: *https://doi.org/10.1016/j.techfore.2021.120786*

Qusa, H., Tarazi, J. and Akre, V. (2020). Secure e-auction system using blockchain: Uae case study, *2020 Advances in Science and Engineering Technology International Conferences (ASET)*, Dubai, United Arab Emirates, 4 February 2020 - 9 April 2020, pp. 1–5.
URL: *https://doi.org/10.1109/ASET48392.2020.9118213*

Sun, F., Yang, Y., Zhou, L., Yao, Y. and Wang, G. (2023). Multi-point mosaic fusion authentication: A strategy for luxury goods authentication, *2023 8th International Conference on Computational Intelligence and Applications (ICCIA)*, Haikou, China, 23 - 25 June 2023, pp. 154–160.
URL: *https://doi.ieeecomputersociety.org/10.1109/ICCIA59741.2023.00036*

Thakkar, A., Rane, N., Meher, A. and Pawar, S. (2021). Application for counterfeit detection in supply chain using blockchain technology, *2021 International Conference on Advances in Computing, Communication, and Control (ICAC3)*, Mumbai, India, 3 - 4 December 2021, pp. 1–6.
URL: *http://dx.doi.org/10.22667/ReBiCTE.2021.07.15.003*

Yang, Y., Wei, L., Wu, J. and Long, C. (2020). Block-smpc: A blockchain-based secure multi-party computation for privacy-protected data sharing, *CBCT'20: Proceedings of the 2020 the 2nd International Conference on Blockchain Technology*, Association for

Computing Machinery, Hilo, HI, USA, 12 - 14 March 2020, pp. 46–51.
URL: *https://doi.org/10.1145/3390566.3391664*

Zhu, Y., Song, X., Yang, S., Qin, Y. and Zhou, Q. (2018). Secure smart contract system built on smpc over blockchain, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 30 July 2018 - 3 August 2018, pp. 1539–1544.
URL: *https://doi.org/10.1109/Cybermatics_2018.2018.00259*

Zimmermann, R., Udokwu, C., Kompp, R., Staab, M., Brandtner, P. and Norta, A. (2023). Methods to authenticate luxury products: Identifying key features and most recognized deficits, *SN Computer Science* **4**: 747.
URL: *https://doi.org/10.1007/s42979-023-02201-5*