TradeMap: A FINMA-compliant Anonymous Management of an End-2-end Trading Market Place

Rafati Niya, Sina ; Allemann, Sebastian ; Gabay, Arik ; Stiller, Burkhard

TradeMap: A FINMA-compliant Anonymous Management of an End-2-end Trading Market Place

Sina Rafati Niya, Sebastian Allemann, Arik Gabay, Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH,
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
Emails: [rafati|stiller@ifi.uzh.ch], [sebastian.allemann|arik.gabay@uzh.ch]

***Abstract*—Data leaks and privacy scandals have been a growing concern of the last decade. While most traditional, *i.e.*, centralized, online platforms require users to register with their personal data, they potentially expose the user's identity and data to be used for unintended purposes. This work proposes TradeMap as an integrated architecture, designing and enabling an online end-to-end (e2e) trading market place, while supporting anonymous management features. TradeMap addresses the Swiss Financial Market Supervisory Authority (FINMA) regulations by designing a FINMA-complaint Know Your Customer (KYC) platform. Additionally, TradeMap is based on blockchains and employs Ethereum Smart Contracts (SC). Thus, trust and anonymity between the market place and the KYC system relies on zero knowledge proof-based SCs used for user identification processes. With this management approach proposed, the user authentication is only verified within the KYC platform, providing a legally valid and fully anonymous online trading platform.**

***Index Terms*—Anonymous eCommerce, Blockchain Applications, Smart Contracts, Know Your Costumer (KYC), Swiss Financial Market Supervisory Authority (FINMA).**

I. Introduction

Trading in any form has been and will be an inevitable part of our lives. During the last two decades, especially by the expansion of the Internet and eCommerce universally, new paradigms of Business-to-Consumer (B2C) and Business-to-Business (B2B) trading have emerged, all determining end-to-end (e2e) cases. Referred to electronic or Internet-based trading, eCommerce has adopted by billions of users in last years and estimates predict the eCommerce purchase value of more than 4 billion US dollars in 2019 [23], [20].

One of the most challenging and crucial aspects of designing eCommerce platforms is user privacy [18]. Privacy protection of users' data collecting, preserving, and sharing in centralized and distributed platforms requires a dedicated design with respect to the data flow, especially when leaking of information can lead to the direct or indirect identification of users. As a result of eCommerce management, improvements have been achieved on eCommerce to conform with interactions and the engagement of a vast number of use cases and users globally.

Several privacy-related solutions offer, *e.g.*, Zero knowledge Proof (ZKP) mechanisms, Know Your Costumer (KYC) services, or more recent blockchain-based approaches. However, a combination of eCommerce platforms and these solutions needs to meet legal and technical prerequisites to be addressed by design. While establishing trust between administrators and users of trading platforms by default is getting more difficult due to privacy concerns mentioned, enabling a ZKP-based approach even leads to further challenges. Generally, a user's identification in eCommerce and online trading can be delegated to a third party, *i.e.*, a Certificate Authority (CA) or any other authority that provides KYC services.

Virtual identities and unchecked financial activities have led to huge problems in past [22], [5]. In eCommerce to adhere law have to be met by users (i.e., Businesses), thus, eCommerce platforms require the KYC process to be done by themselves or by a trusted third party. There have been solutions to offer KYC system, especially the recent BC-based approaches. Blockchains (BC) are defined as distributed digital and public ledgers that record transactions immutably and autonomously without the need of a central control [3].

At a first glance, eCommerce approaches relying on BCs, either for KYC or for the e2e trading, suffer from several deficits. These include: **(1)** Lacking a sufficient and reliable user identification, **(2)** neglecting regulations, *e.g.*, the Swiss Financial Market Supervisory Authority (FINMA), **(3)** lacking of ZKP-based mechanisms in support of privacy, **(4)** using fully decentralized BCs, which by default do not bring privacy as data stored by them can be accessed publicly, **(5)** neglecting costs of storing large data on BCs, **(6)** overloading an SC, **(7)** missing the use of standardized interfaces, and **(8)** missing a secure back-end and SC implementation.

This work introduces as a solution termed "TradeMap", the ZKP-based design of an e2e trading market place. It enables anonymous eCommerce for customers and businesses, who can sell and purchase goods. TradeMap combines the two main parts as of KYC and eCommerce, based on BCs, which not only manage the user identification in a FINMA-compliant fashion, but also employ a novel approach to use SCs for managing all user interactions with a single platform. As such TradeMap prevents any system administrator of a trading market to reveal or even know the user's identity. The user identification and registration in TradeMap are managed by SCs for all identity verification requests, thus, leading to the anonymous management capability.

This paper is organized as follows: Section II overviews related work and leading to the requirement analysis of TradeMap within Section III. While Section IV discusses the design and prototypical implementation details, and Section V provides a discussion and an outlook.

II. Related Work

While the Technical Report [15] details all relevant related work on KYC systems and blockchain-based decentralized trading platforms, this section here summarizes key observations, which the TradMap design is based on as a fully decentralized, yet anonymous management approach enabling e2e e-trading.

A. Know Your Customer (KYC) Verification

Performing a Know Your Customer (KYC) verification is key to interact with new customers, especially within the financial domain [17]. Since the traditional KYC process carries high costs, it is in the interest of both parties (consumer and supplier) to reach an efficient outcome. Amongt others, the following systems had been developed to optimize KYC processes:

IDnow: IDnow is an identity verification platform, which provides a wide range of KYC services which comply towards Anti-Money Laundering (AML) as well as the regulations of the corresponding authority [10].

VideoIdent: VideoIdent verifies using a P2P video chat with a responsible person. Within the video chat the customer will be asked questions and to hold his/her ID into a camera such that a tilting of it enables a verification as in a face-to-face setting [11].

CB Financia:l Services AG (CBFS) CBFS also provides a platform for online identification and the conclusion of contracts. The identification solution CBFSIdent applies secure video streaming to verify identities [6].

Shufti Pro: Shufti Pro provides efficient and accurate digital KYC verification services via an artificial and human hybrid technology [19].

Tradle: Tradle allows financial institutions to onboard their customers with blockchain-based bots. A chat and snapshots of identity documents verifies the client [7].

KYC-Chain: KYC-Chain enables businesses to handle the KYC processes for individuals and corporations by applying a B2B-managed workflow application [12].

KYCstart: KYCstart is a Proof-of-Concept of a KYC-as-a-service using blockchains [13].

Table I compares per column the KYC identification alternatives used, the application of an underlying BC, service access options, and practical usage.

B. Decentralized Trading Systems

Blockchain Platform for Industrial Internet of Things (BPIIoT): [21] proposes the creation of a blockchain-based market place for industrial manufacturing services, enabling an interaction directly with manufacturing machines through a dApp.

Exergy: [14] supports prosumers and consumers of energy to trade energy directly and process payments through a specifically developed blockchain and ERC20 compliant tokens used.

Blockchain P2P Marketplace: [16] proposes an Android application (app) running with Ethereum to allow users to buy, sell, rent, or lend out physical objects using SCs and the Ether cryptocurrency on a Peer-to-Peer marketplace. To use this app users need to meet in person and there is no eCommerce market place where users can refer to buy/sell goods in there.

Decentralised Sharing App: [4] outlines objects being registered via a QR (Quick Response) code that can be rented out to other parties having access to the application.

Table II compares the use of cryptocurrencies, the dedicated use case, the anonymity level achieved, and the usage.

TABLE I
Comparison of KYC Systems

Company	Identification	Blockchain	Access	Usage
IDnow	Video, Auto	x	API	Mobile/Web
CBFS	Video	x	SaaS or License	Web
Shufti Pro	Auto	x	API, Integration	Mobile
Tradle	Chat	✓	App, Web	Mobile/Web
KYC Chain	n/a	✓	Solution	Web
KYCstart	n/a	✓	n/a	n/a
TradeMap	Video	✓	Smart Contracts	Web

TABLE II
Comparison of Distributed Trading Approaches

Project	Crypto-currency Oriented	Use Case	Complete Anonymity	Usage Environment
BPIIoT	yes	Industry	no	Web App
Exergy	no	Energy	no	Mobile App
P2P Marketplace	yes	Private Marketplace	no	Android
Decentralized Sharing App	yes	Private Marketplace	no	Web App

III. Requirements

Based on the identification of major security requirements to be met, the TradeMap's design requirements are outlined below, including the Swiss FINMA-compliant video identification requirements and relevant SCs.

A. Video Identification Requirements of KYC Systems

For the video identification process the platform must comply with the regulations FINMA has published [15]. Hence, the technical aspects of the FINMA publication were considered carefully. [8] lists all relevant articles, which had been considered. To meet the key requirements of (a) all relevant data need to be submitted, (b) consent to use those, and (c) pictures are taken, the following design was prepared: A user friendly form was designed to collect relevant data to be stored in the data base making it available for users at any time. To prevent users from spamming the platform, an email-based verification is executed, once the user registers proving that (a) the user knows her/his email address and (b) the user is in possession of the password to access the respective account. For the video identification itself the usage of WebRTC APIs (Application

Programming Interface) is proposed, because the APIs provide secure and interrupt-less RTC (Real-Time Communication) capabilities. Security concerns can be eliminated by using *CSRF* tokens via a valid user id to authenticate. In this way, no not-entitled user can access a channel. As described in FINMA Art. 16 [8], the platform can make use of an email-based verification.

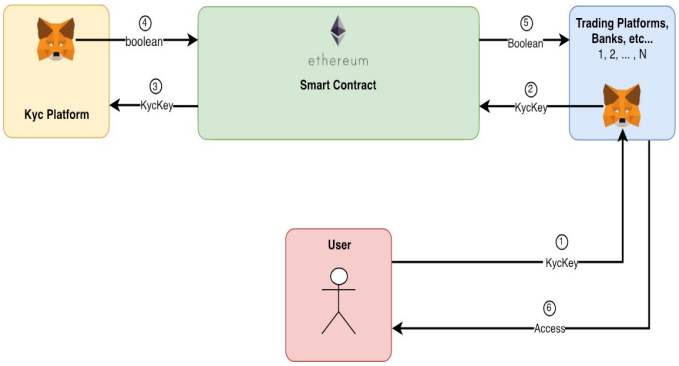

Fig. 1. Trading Platform's Identity Verification Requests to the KYC Platform Through Smart Contract

B. Smart Contracts' Requirements

The Smart Contract (SC), which has to be developed brings requirements such as accessibility, anonymity and usability. The accessibility requirement for users could be met by having a browser extension installed allowing the user to create a new wallet. Since sending transactions to the Ethereum network always cost an amount of Ether, it is important that the browser extension has access to the user's wallet to transfer the funds. Blockchain transactions are transparent and visible for all users in the network. Since the goal is to allow user's complete anonymity, it must be considered to make SC requests anonymous. A design proposal is to use a unique hashed key (*KYC key*) with which users could register themselves at connected platforms anonymously while providing consent that the user's data could be shared with the platform. To prevent that the *KYC key* is copied once a SC request was processed, it is suggested that the mentioned key be hashed.

As mentioned above, each transaction made to the Ethereum network requires a small payment of Ether amount. This amount is called *gas*. Another aspect, which has to be considered, is the block time of the Ethereum network. It takes some time to process the transaction because every transaction has to wait for a new block to be created. In a system enabling user-interaction with the BC this can decrease the usability due to long transaction times. If the amount of Ether the user is willing to pay per unit of *gas* increases, it could ensure that the transaction is mined quicker. Unfortunately, this results in a trade-off between costs for transactions, the so called *gasPrice*, and block time of transactions meaning the usability decreases when the costs are reduced and vice versa. Therefore, the goal is to find a well balanced *gasPrice*.

IV. Design and Prototyping

TradeMap consists out of the KYC platform, the e-trading platform, and their respective SCs. These together provide the anonymous management features needed to ensure that trust can be provided, too.

A. TradeMap's Design Overview

TradeMap enables accessing anonymous interaction in an e2e trading manner, being managed by legally accepted schemes. Thus, TradeMap designs two interconnected systems. On one hand, the FINMA-compliant KYC system and, on the other hand, a secure trading platform enabling BC-based e2e trading. These inclusive platforms are only interconnected via the SC (cf. Fig. 1). This enables other trading platforms to connect to the KYC system without any need for modifications of existing system. As illustrated in Fig. 2, users enter the registration phase and verify their email address. In the third step beneficiaries of the KYC key, *e.g.*, managers of the company, will be declared. Terms and conditions, which are determined based on FINMA regulations, have to be accepted by the user within the fourth step. Followed by the video verification and a One Time Password-based (OTP) activation the KYC user is approved and registered. Finally, the user KYC key can be stored in the SC for future use.

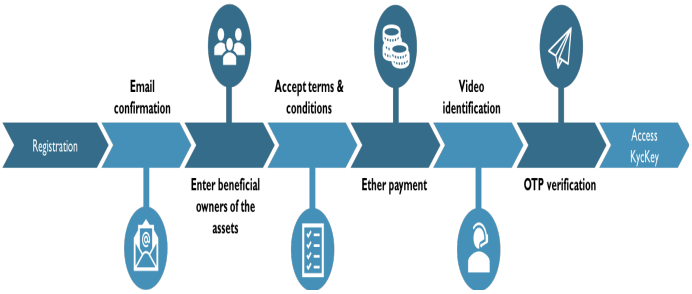

Fig. 2. KYC System Interactions for a Verification Request

The e2e trading is designed to be used as a market place for trading objects and products. Secondly, it can be used as an inventory for registered products. With TradeMap, the history of objects' past owners can be verified. Smart Contract preserves all information needed to identify one object. This approach empowers the anonymous management of the entire system and protects against fraud by enabling buyers with a pre-purchase checking option of the objects' history, all based on the BC.

B. KYC Platform Implementation

For the video identification process, all requirements of the FINMA circular 2016 [8] such as "The financial intermediary structures the online onboarding process in such a way that the contracting party fills out the details required under Articles 44 and 60 AMLO-FINMA electronically and transfers them to the financial intermediary before the audio-visual identification interview takes place. In addition, the financial intermediary checks the information gathered during the onboarding process against the information contained in the contracting party's

identification document." and "The financial intermediary must obtain the contracting party's explicit consent to conduct the video identification and audio recording before starting the video interview." have to be met. Also the Anti-Money Laundering Ordinance [2] was considered. Figure 1 shows each step a user has to go through to claim his KYC key. The smart contracts developed for the KYC part can be accessed from [1].

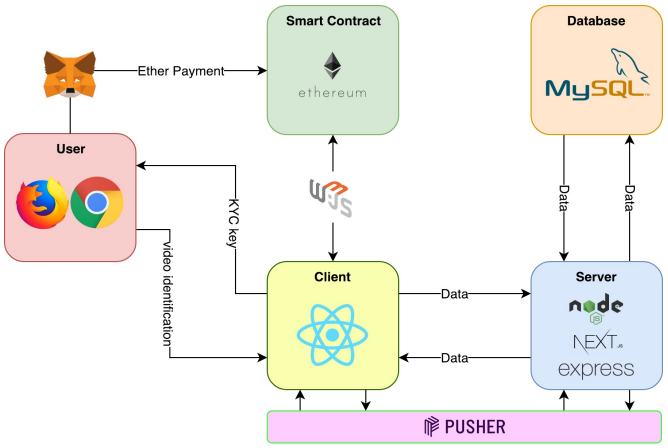

Fig. 3. KYC Platform Implementation Architecture

C. Trading Platform Implementation

Figure 4 shows the three possible data flows and their chronological execution. The green arrows indicate the data flow occurring when an object is being listed on the platform. Step 1 is triggered by the seller (user) clicking the "*Sell*" button in the front end, thereby sending data to the client. The client sends this data to the server (step 2), which finally writes it to the database (step 3). Concurrently to the data being sent to the server, it is also persisted on the BC (step 2, copy). Arrows colored in red show the order in which the components operate to display existing data to a user. At first (step 1), the data is read from the database by the server and forwarded to the client (step 2). The process in concluded by displaying the data retrieved to the user (step 3).

Black arrows depict the item purchase process, which is triggered as soon as a buyer (user) clicks the "*purchase*" button and pays for an item (step 1). Subsequently, the client sends the funds to the BC (step 2), which will then prompt the seller (step 3) to ship the item to the buyer (step 4). Once the buyer receives the item, he/she confirms the receipt, which will release the funds to him/herself and the seller (step 5). Meanwhile, the BC sends a confirmation back to the client, which passes all relevant data through to the database via the server in order to update it (steps 6, 7 & 8). The main function of the SC [9] is to handle the verification requests for users registering with an external platform using their KYC key. The user will, once verified, have access to his KYC key through the profile page. With this KYC key the user registers at a platform. Figure 2 outlines the respective verification request. Thus, SCs enable the tracking of these requests back, which is important for analyzing unauthorized user accesses from external platforms.

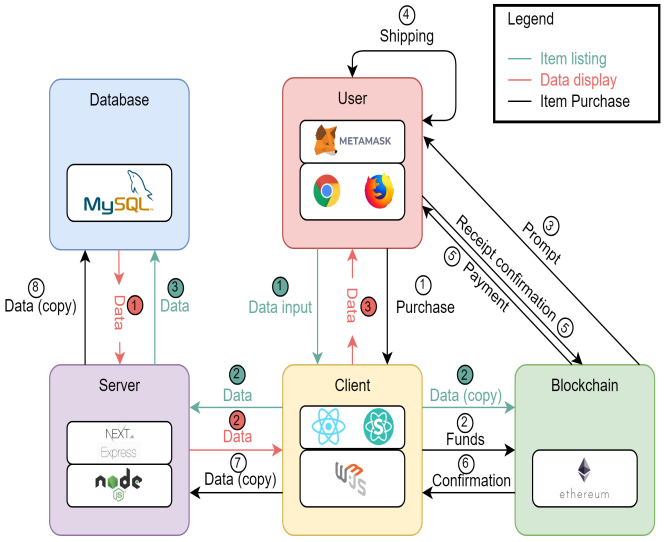

Fig. 4. E2E Trading Platform Architecture

V. Discussion and Outlook

Designing multi-component systems based on blockchains (BC) can only make IT systems better, if all features supported by traditionally centralized applications, such as KYC or eCommerce, are offered unchanged and improvements as of new features and functionality is being added. From a governance perspective of managing user interactions with centralized systems, especially with respect to the case of relying on a decentralized trust factor of BCs, TradeMap propose a novel design, that meets facilitating traditional eCommerce as a marketplace of e2e trading. In this sense TradeMap integrates the BC with care, undertaking several steps to meet FINMA regulations of user registrations.

TradeMap performs such a registration without storing all user data in the BC. With respect to the trading platform, the permission for verifying the user's identity is only done by a method, which itself does not need any identity disclosure. Thus, before and after the identity verification, the trading platform's administrator will not receive any identity-related information. In that sense the anonymous management feature had been achieved for the e2e trading market place.

TradeMap enables data management for users, *e.g.*, businesses, to trace back the history of products before purchase. With TradeMap each product is now traceable, safe trading is enabled, and a healthy and ethical market place is designed to offer full independence to users from trusted third parties, such as banks.

VI. Acknowledgements

This paper was partially supported by (a) the University of Zürich UZH, Switzerland and (b) the European Union Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, namely the Concordia project.

REFERENCES

[1] S. Allemann, "TradeMap's KYC Platform Source Code," https://github.com/sealle/BA-S.E.A, August 19, 2019.

[2] AMLO-FINMA, "Verordnung der eidgen ossischen finanzmarktaufsicht über die bekämpfung von geldwäscherei und terrorismusfinanzierung im finanzsektor," https://www.admin.ch/opc/de/classified-compilation/20143112/index.html, January 24, 2019.

[3] T. Bocek and B. Stiller, *Smart Contracts - Blockchains in the Wings*. Tiergartenstr. 17, 69121 Heidelberg, Germany: Springer, jan 2017, pp. 169–184.

[4] A. Bogner, M. Chanson, and A. Meeuw, "A Decentralised Sharing App Running a Smart Contract on the Ethereum Blockchain," in *Proceedings of the 6th International Conference on the Internet of Things*, ser. IoT'16. New York, NY, USA: ACM, 2016, pp. 177–178. [Online]. Available: http://doi.acm.org/10.1145/2991561.2998465

[5] R. Campbell, "Block Explorer News; The Silk Road: A Story of Bitcoin, Drugs, and the DarkWeb," https://blockexplorer.com/news/silk-road-timeline-bitcoin-drugs-dark-web/, December 1, 2018.

[6] CB Financial Services AG, "Cbfsident," https://www.c-b-f-s.com/services/cbfsident/, November 27, 2018.

[7] R. De Feniks, "Tradle: KYC on Blockchain," https://urlzs.com/YL9nU,.

[8] FINMA Circular: Video and Online Identification, pp. 07–16, November 2018. [Online]. Available: https://www.finma.ch/en/~/media/finma/dokumente/rundschreiben-archiv/2016/rs-/finma-rs-2016-07.pdf?la=en

[9] A. Gabay, "TradeMap's eCommece Platform Source Code," https://github.com/Aeregabay/BA, August 19, 2019.

[10] IDNow, "IDNow: Regulation," https://www.idnow.io/regulation/identification-kyc/, November 27, 2018.

[11] IDNow.io, "IDnow, VideoIdnent, Seamless Online Identification Using an Agent-assisted Video Chat Process in Compliance with The Money Laundering Act," https://www.idnow.io/products/video-verification/, November 27, 2018.

[12] KYC-Chain, "Efficient KYC Management," https://kyc-chain.com/, November 27, 2018.

[13] A. Lielacher, January 24, 2019. [Online]. Available: https://urlzs.com/ehWUM

[14] LO3 Energy, "Exergy Business Whitepaper ," https://exergy.energy/wp-content/uploads/2018/04/Exergy-BIZWhitepaper-v10.pdf, January 4, 2019.

[15] S. R. Niya, S. Alleman, A. Gabay, and B. Stiller, "A Blockchain-based Anonymous P2P Trading System," in *IfI Technical Report No. 2019.04, Department of Informatics IfI, University of Zuerich UZH*. Zürich, Switzerland: UZH-IfI, June 2019.

[16] S. R. Niya, F. Schüpfer, T. Bocek, and B. Stiller, "A Peer-to-peer Purchase and Rental Smart Contract-based Application (PuRSCA)," *it- Information Technology*, Vol. 60, No. 5, pp. 307–320, oct 2018. [Online]. Available: https://urlzs.com/uMzDg

[17] NorthRow, https://www.northrow.com/kyc-checks/, November 26, 2018.

[18] Shazia W. khan, "Cyber Security Issues and Challenges in E-Commerce," in *Proceedings of 10th International Conference on Digital Strategies for Organizational Success*, 2019, http://dx.doi.org/10.2139/ssrn.3323741.

[19] shuftipro.com, "Shufti pro," https://shuftipro.com/, November 27, 2018.

[20] Statistica Research Department, "Retail e-commerce Sales Worldwide from 2014 to 2021 ," https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/, November 27, 2018.

[21] M. V.K and A. Bahga, "Blockchain Platform for Industrial Internet of Things," journal of Software Engineering and Applications,Vol.9 No.10, October 2016, 2016.

[22] Wikipedia, "Silk Road (Marketplace)," https://en.wikipedia.org/wiki/Silk_Road_(marketplace), June 13, 2019.

[23] C. Yang, Y. Chen, S. Chen, and S. Wu, "A Reliable E-commerce Business Model Using Blockchain Based Product Grading System," in *2019 IEEE 4th International Conference on Big Data Analytics (ICBDA)*, March 2019, pp. 341–344.