Smartlink — A Decentralized Flexible Escrow Solution for Physical and Digital Assets

Whitepaper v2.0

Benoit Constanty[1], Álvaro García Pérez[2], Sara Tucci[2],
Jérémy Martin[3], Diederick Jacobs[4]

[1] Smartlink, Tallinn, Estonia
[2] CEA, List, F-91120, Palaiseau, France
[3] Smartchain, Paris, France
[4] House of Chimera, Rotterdam, Netherlands

Abstract. Trust has been connected to economic activity since the dawn of time. Although the internet and online transactions have had a staggering impact on how we interact with each other, some primary flaws with the system persist. Among these involve rising economic crimes and transaction costs. While traditional security measures provide subtle confidence and protection, fraud and high transaction fees remain two major challenges in day-to-day exchanges.

In this paper, we present a novel method to execute commercial transactions through a decentralized escrow solution that secures online and face-to-face exchanges between parties while eliminating the trust deficit. The aim of our decentralized Escrow is to provide a platform for the exchange of both digital and physical assets supported by escrow accounts. These escrow accounts are implemented in a decentralized way by the means of smart contracts over the Tezos blockchain. The objective of this paper is to lay out a high-level specification of our decentralized Escrow platform and introduce the changes we have made to our initial proposition.

1. Introduction

Electronic commerce (hereinafter: e-commerce) relies almost exclusively on a few financial institutions that process transactions and serve as trusted third-party services. The current online environment where the number of unknown parties increases suffers from fundamental vulnerabilities due to the used trust model. Trust is often regarded as a fundamental concept for understanding economic, financial, and social activities [1-5]. The perception of trust is that it allows parties to perform potential beneficial exchanges while overcoming the presence of moral hazard. It means that one takes a risk, leaving themselves vulnerable to the actions of the counterparty [6].

Additionally, perceived economic distrust depends on various behavioural factors (e.g. trust levels, risk appetite) [7-10]. Hence, the balance of trust and distrust differs for every person, and therefore the accepted threshold is different, influencing the overall will to participate in e-commerce. The perceived risk during an e-commerce transaction is an aggregate factor with three dimensions: risk of functionality inefficiency, risk of information misuse, and risk of failure to gain product benefit [11]. Consequently, the consumers' perceived risk plays a crucial role in the decision-making for purchasing and hedging the involved financial risk through a digital escrow service [12].

E-commerce is characterized by asymmetric

information [13], meaning that transacting parties do not have access to the same information flow [14]. Many significant factors influence the amount of asymmetric information; however, two are closely related to online fraud: the uncertainty of the counterparty's identity and the uncertainty of the product quality [15]. The principal-agent theory is perceived as one of the root causes of economic crime and distrust since self-interest is higher than external interest. The theory claims that the agent can make decisions that impact the principal. However, due to self-interest, the agent will act in their best interests contrary to the principal [16]. This is reflected in a recent study showing that the total costs of global fraud for firms were over 42 billion USD from 2018 to 2020, especially customer fraud and cybercrime are significantly increasing [17].

Considering that economic crime and distrust are perceived with multiple types of transactions, the urgency for a convenient, decentralized, and trustless solution is imminent. This whitepaper proposes a solution for the economic distrust problem by offering a decentralized and trustless escrow service. The system is secured through a robust network of smart contracts built on one of the most secure and scientifically-driven blockchain ecosystems, Tezos. The paper will be developed through a step-wise approach, highlighting fundamental concepts (i.e. smart contracts) to investigate how a blockchain-based escrow service can solve existing financial issues. The paper will highlight how smart contracts work and how these can have a significant effect on the traditional financial industry. Ultimately, the Smartlink block-chain-based escrow service will be high-lighted to contribute to the broader question of how Smartlink will revolutionize the escrow industry.

2. Smart Contracts

2.1 Background on smart contracts

Most modern cryptocurrencies rely on smart contracts, a self-executing contract based on a programming language. Nick Szabo proposed the first concept of smart contracts in 1997 [18]. In this paper, Szabo labeled a purchase from a vending machine as an early form of a 'smart contract'. The owner of the purchased item transfers ownership upon receipt of pre-determined requirements (i.e. money). Szabo also identified that smart contracts needed security to exist; therefore, he mentioned that the currency lockbox and other security mechanisms protect the stored coins and other contents of vending machines from potential attackers [19]. Additionally, he describes a few other potential applications for smart contracts, including automated transfer of digital property and peer-to-peer lending. These previously proposed applications are currently operational and widely adopted by the cryptocurrency community because of smart contract protocols (e.g. Ethereum, Zilliqa, Tezos).

Smart contracts allow digital and physical assets to move according to an arbitrary pre-specified set of rules [20]. Smart contracts have a blockchain as an underlying layer, whereby all involved transactions are time-stamped and respectively added. Due to the design of a blockchain, there is no central authority that validates or screens these transactions. In contrast, it is a network of decentralized nodes that validate transactions in the case of Proof-of-Work. Therefore, blockchain technology is a form of Distributed Ledger Technology. Essentially, smart contracts consist of a set of transactions that are stored and updated with Distributed Ledger Technology [21]. Due to the self-executing mechanism of smart contracts, the contract will automatically settle whenever the predetermined prerequisites are met. Once a smart contract is issued, the smart contract's state cannot be altered.

Delmolino, Arnett, Kosba, Miller, and Shi provided a simplified example of a smart contract

and how it might be coded, in the now depreciated Serpent, to achieve its purpose [22]. In this particular example, two parties – Alice and Bob – engage in a simple financial swap. Alice believes the value of the stock will increase, while Bob believes the opposite. Both parties deposit an equal amount of a designated cryptocurrency when the deadline arrives. The stock's current price is queried by interacting with a particular external pricing authority (e.g. oracle). The combined deposit will be given to Alice or Bob based on the given price. The smart contract provides various parameters: the identities of the parties, the reference deadline, prerequisite, and the outcome based on the prerequisite. The smart contract's plain and comprehensible logic makes it relatively easy to understand for consumers with a basic understanding of coding. The highlighted smart contract is relatively simple; it emphasizes the elegance and possibilities of smart contracts to facilitate a broad number of transactions and applications.

2.2 The benefits of smart contracts

Blockchain technology enables smart contracts to operate cost and resource-efficient by providing a fully transparent mechanism to transfer digital property while reducing the dependency on intermediaries. Moreover, with the open nature of a public blockchain, all transactions and data are accessible for the involved parties.

Smart contract technology has a few clear advantages compared to traditional contracts. An example, the perceived risk of transferring property is drastically lowered due to the accessibility of public data of the blockchain. As highlighted earlier, transactions are not validated through a trusted intermediary (e.g. banks) but a consensus method of decentralized nodes.

Public blockchains apply consensus methods to achieve necessary agreements to ensure that every node connected to a particular blockchain is synchronized and its transactions are legitimated. How transactions are publicly verified and added to the blockchain allows a fully transparent ecosystem whereby any involved party can verify transactions. Moreover, smart contracts entirely rely on on-chain data that cannot be altered, assuming the underlying blockchain is robust and fully transparent for any participant.

Smart contracts also may result in lower overhead costs. Since the dependency on intermediaries is significantly lowered, settlements can take place far quicker and without the need of a traditional intermediary. Moreover, smart contracts are self-executing; therefore, fully automated, which decreases human involvement. Consequently, a smart contract's operational cost is drastically lower than a traditional contract. Traditional contract fees are usually service or administrative fees or legal fees associated with preparing, monitoring, and executing written contracts. A typical example of a traditional contract is a purchasing contract whereby a consumer purchases a product online by debit card and pays fees to the credit card company for their services. The blockchain could have similar costs, depending on the consensus method. However, the scale will be much smaller. Additionally, transactions on the blockchain are dependent on the blockchain, evolving to be near-instant. Hence, allowing users to perform cross-border transactions with negligible transaction times.

The simplicity of smart contracts allows for a unique opportunity to decrease language ambiguity. Ambiguity occurs when there is a lack of clarity or a sense of uncertainty about applying a particular term [23]. A word may have multiple definitions in a sentence structure, allowing for different interpretations. There have been numerous issues whereby ambiguity led to severe economic and social damages in the past. The case of Raffles v. Wichelhaus must be one of the most famous cases regarding mutual misunderstanding. This case took place in 1864, where the accuser, Mr Raffles, offered to sell a certain amount

of cotton to the defender, Mr Wichelhaus [24]. It was agreed that the cotton would be transported to Liverpool by ship, called Peerless, from Bombay. At the time, two ships were sailing under that name, and the contract did not specify which ship had the goods. Both parties believed that the agreement covered different ships since Wichelhaus assumed that the goods would be delivered in October, while Raffles gave the goods to the Peerless boat that would arrive in December. Wichelhaus refused to pay, as the goods were dispatched too late, whereupon Raffles sued him. Was there an enforceable contract between the two parties? The court ruled that there was not. There was ambiguity in Peerless and which ship was understood. There was no consensus on what the parties had in mind, so the contract was nonbinding. An outsider could not determine which boat was referred to in the agreement. Mutual misunderstanding can be characterized as a problem of contract where customary law falls short [25].

In summary, smart contracts have the following advantages compared with traditional contracts [26]:

Lower perceived risk. Due to the design of an open blockchain, issued smart contracts cannot be altered. Additionally, the transparency of an open blockchain forces participants to be accountable for their potential malicious intent.

Lower overhead costs. The decentralized public ledger substitutes brokers and mediators due to the trustless nature of an open blockchain. Smart contracts are decentralized self-executing contracts stored in a blockchain; therefore, administration or additional services are redundant.

Lowered language ambiguity. Language is one of the most complex outcomes of evolution, whereby ambiguity plays a considerable role [27]. Ambiguity is also found in policy frameworks and legal contracts, making it burdensome for contractors and lawyers. The perceived ambiguity in programming languages is lower due to the execution, allowing only one interpretation of a specific sentence.

Improving operational efficiency. The elimination of intermediaries lowers the needed resources and therefore can significantly improve the efficiency of business processes. The self-executing nature of smart contracts lowers the turnaround time, for example.

2.3 Smart contracts: A financial innovation

The traditional innovation-growth perspective assumes that financial innovations help improve the quality and variety of financial instruments [28, 29], facilitate risk sharing [30], and ultimately improve allocative efficiency [31, 32]. However, financial innovation also has a considerable negative effect; one of the root causes of the global financial crisis of 2008 was innovative financial instruments by dramatically increasing credit expansion, leading the world into one of the worst financial recessions in decades. The thin line between positive and negative financial innovation makes it complex and, in foresight, burdensome to classify financial innovations due to ever-changing political and financial frameworks and overall risk acceptance by institutions. However, there is supporting evidence that financial innovation allows countries to grow faster by growth opportunities [33]. An example of a financial innovation that could increase the growth opportunities for countries is digital escrow services. "Online escrow services are fundamental to facilitate and accelerate e-commerce, by securely assuring settlements" [34]. The perceived risk significantly decreases by protecting the involved parties from asymmetric information and self-interest. Consequently, the consumer is more willing to engage with e-commerce, leading to higher business revenue.

However, the intensity of competition is relatively low for the digital escrow industry due to the high financial barriers for entrants. Addition-

ally, a significant entry obstacle is a complex and expensive infrastructure for a scalable escrow service. Monopolies can be seen as a crucial issue that potentially impacts the overall quality and pricing of the service [35]. As a result, there is a lack of participants, and therefore, the industry is relatively monopolized by a few market participants, leading to high transaction fees and industry stagnation. Furthermore, the processing times of traditional escrow services can take up to five business days, depending on the used payment method [36]. The current centralized design of escrow services is transferring the perceived risk from a consumer to a third-party intermediary instead of eliminating the risk. The usage of smart contracts can minimize the perceived risk due to the lower language ambiguity and increased overall operation efficiency.

The means of payment of a blockchain escrow service is, in general, a native cryptocurrency with an underlying blockchain layer. The significant difference between traditional escrow services is that a public blockchain is immutable; once verified, data cannot be altered [37]. The involved parties can verify if transactions have taken effect without trusted third-party intermediaries through the public blockchain. It allows blockchain escrow services to operate more efficiently by decreasing overhead costs while increasing operational efficiency [38]. The precision of cryptographic identifiers can minimize future conflicts over contract terms; due to that, the ambiguity of programming languages is less than traditional real-world languages [39].

3. Smartlink

Smartlink intends to create a decentralized and secure ecosystem that eliminates the need for trust during a commercial transaction by providing different tools to solve Trust Conundrum for Web3.0 and off-chain appli-cations, emphasizing rapid settlement time enterprise-grade security and a convenient interface. Smartlink does this by removing many significant intermediaries, lowering overhead costs and perceived risk while increasing the user's flexibility. Users are provided with a set of secure, standardized smart contract templates to ensure the accessibility and security of the protocol. However, users can also customize or create new contracts based on their own needs. By promoting an intuitive user experience and design, the ecosystem allows anyone to use the product with ease without any complexity constraints. Furthermore, Smartlink will implement a robust KYC and AML protocol that safeguards its users' information without compromising the network's security. The users' data will be stored on a local database or a decentralized data storage protocol. The advantage of a decentralized data storage protocol is lower overhead costs than centralized cloud-based storage and it removes the vulnerabilities of centralized authority. However, the overall required infrastructure for decentralized data storage is more complex, due to supervision, and it is expensive.

The utilized blockchain layer of Smartlink is Tezos, an open-source, community-governed blockchain network. Tezos utilizes a Proof-of-Stake (i.e. Liquid Proof of Stake) mechanism as consensus method, that utilizes baking and features optional delegation, allowing any stakeholder to participate in consensus without giving up custody of their tokens [40].

3.1 Decentralized escrow

The Smartlink escrow service eliminates the perceived risk during a digital property transfer through leveraging smart contracts. The user can utilize the Smartlink smart contract library (hereinafter: Sscl) or create their smart contract based on their needs. The Sscl are enforceable, legally valid, and audited smart contracts; thus, contracts are legally binding. Consequently, it minimizes the overhead costs of legal research and developments of smart contracts for users. The smart

contracts are scalable, allowing multiple stakeholders and complexity. The involved parties of a smart contract can allocate an inspection period before the closure of a deal to ensure that the involved parties can inspect and confirm if the smart contract accommodates the prerequisites. By defining specific rules and requirements for the smart contract, the smart contract can self-execute based on these prerequisites. The smart contracts have a multi-step agreement mechanism, allowing involved parties to create payment milestones.

The Smartlink escrow service will allow digital and physical property transfers through leveraging smart contracts, Smartlink API and Decentralized Oracle Networks (DONs). DONs are a group of independent nodes that provide data to a blockchain. Every independent node retrieves data from off-chain sources and stores it on-chain. The data is then aggregated to a system to determine the validity of the data. The transfer of digital property (e.g. Tezos tokens, synthetic assets, NFTs) is fully on-chain, allowing users to track transactions through the blockchain. In an escrow exchange, the Seller and the Buyer first agree on the terms of the exchange collected in an 'escrow proposition'(hereinafter: proposition), which is captured by an escrow smart contract on Tezos. The acceptation of the proposition by the two parties entails that the escrow smart contract withholds some stipulated amount of money from the Buyer. After the acceptation of the proposition, the Seller delivers the product to the Buyer, and when both parties have verified that all the conditions of the exchange are satisfied, the escrow smart contract releases the amount to the Seller. If the conditions are not met, both the Buyer and the Seller could start a dispute, which would escalate through several phases according to certain time ranges and which may eventually involve a Mediator. The Mediator would collect the evidences presented by the Buyer and the Seller and would eventually emit some verdict in favour of one of the two parties.

The current implementation of Decentralized Escrow covers the use cases for the exchange of digital assets [91, 92] and present detailed workflows for the "creation of an escrow proposition", "acceptation of a proposition", "cancellation of a proposition", and "dispute of a proposition". The actors in this workflow define a system architecture that resembles that of the Decentralized Applications (DApp) pattern[1] where a Smartlink web service simplifies the interactions between the final users and the smart contracts on the blockchain, via an application program interface (API) which may store relevant data in an off-chain database, and whose operations are available to the users through an internet browser (see Figure 1).

Among other activities, the Smartlink API is in charge of the following:

(i) Authenticating the final users through Smartlink's log-in service, which, among other attributes, registers the Tezos wallet address and the email address of each user [92]).

(ii) Validating and preparing the data to be included in the blockchain transactions, which are sent to the final users in order to be signed with the user's wallets thus invoking the corresponding smart contract(s).

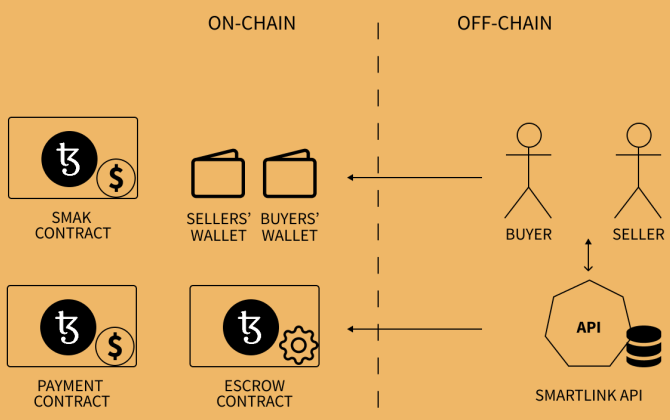

Figure 1: System architecture of the Decentralized Escrow.

[1] https://research.csiro.au/blockchainpatterns/general- patterns/deployment- patterns/dapp/

(iii) Notifying the users of the results of their operations by exchanging emails with the registered email addresses.

Even though the authentication of final users presents a certain degree of centralization, this is however adequate for Smartlink's business model for the exchange of digital assets. Smartlink keeps an off-chain register of all the escrows in the platform and generates all the invocations of the smart contracts, which are to be signed by the final users. The final users pay the tez gas fees for including these transactions in the Tezos smart contract.

In its current implementation, Decentralized Escrow is optimized for the exchanges of digital assets. In this kind of exchanges, the real-world entities and objects involved are limited and known beforehand (since there are no intermediaries), and the conditions of a given escrow can be checked automatically in an easy way, since the exchange of such products lays exclusively on electronic transactions. However, the exchange of physical assets involves interactions between real-world entities that pose a whole new brand of challenges, which are to be addressed by future versions of the Decentralized Escrow. Some of these challenges are investigated in this technical report.

The escrow for digital assets allow efficient Over-The-Counter (OTC) trades in one-on-one transactions, removing the need for any trusted third-party intermediaries. Through the use of the FA 1.2 standard on Tezos, tokens can be used besides the native Smartlink token, SMAK. The FA 1.2 Tezos standard is Tezos fungible token standard that includes a ledger that outlines identities to token balances. It provides a standard API for token transfers and authorizes external contracts or accounts to transfer users' tokens [41]. The FA 1.2 Tezos standard is a leap in consumer accessibility due to the multiple native Tezos cryptocurrencies and compatibility of wrapped ERC-20.

Furthermore, Smartlink will utilize the FA2 Tezos standard to transfer Non-Fungible Tokens. A Non-Fungible Token is a non-interchangeable unit of metadata with unique identification codes and metadata publicly verifiable through a public blockchain. The critical factor that distinguishes the FA2 standard from the FA1.2 standard is the standardization of transfer semantics, meta-data, accessing balances, total supply, and permission rights [42]. These implementations significantly increase the degrees of freedom of token contracts by allowing configuring token types, token management, supply operations, authorizing architecture and questions on contract upgradeability [43]. Finally, participants must have a compatible wallet to store the acquired digital property to transfer digital property.

3.2 Digital Marketplace

Cryptocurrencies are increasingly being used for day-to-day payments; due to technological advancements, the transaction fees of specific blockchain networks are negligible (e.g. Zilliqa, Tezos). Traditional payment processors are gradually entering the crypto-currency market (e.g. PayPal, Square). The profitability of cryptocurrency services are considered high, consequently, newly entering traditional companies are reporting significant revenue growth numbers [44]. One of the frontrunners of the cryptocurrency payment industry, Bitpay, reported a 50% revenue growth in 2021 [45]. The growth is expected to increase in the next few years due to the consumers' increased interest in cryptocurrency services [46].

The synergy between a cryptocurrency marketplace and an escrow service is significant due to the complementary nature of the products. Consequently, the overall overhead costs of both products are potentially reduced through economies of scale. Thus, Smartlink plans to launch a marketplace for Web 3.0 that distinguishes itself from existing solutions through ad-

vanced functionalities, including a crypto wallet browser integration, escrow smart contract, multi-cryptocurrency support, significantly lower fees, a built-in reward system and a user-friendly interface. The perceived risk is reduced for the involved parties through an on-chain review system. Smartlink provides an option to settle payments immediately or use escrow smart contracts for the transaction.

According to a recent study, new users perceive the cryptocurrency industry as complex, preventing potential user adoption [47].
Hence, Smartlink emphasizes the user experience by adopting accessible concepts and interfaces. Additionally, Smartlink plans to provide its services through mobile applications that support initializing and executing the main functionalities, including the contract template library, escrow service, milestone payments, tracking transactions, and sending offers. The mobile application will be a significant gateway to the Smartlink Marketplace, allowing consumers to purchase products and services directly with an auto-connect feature for compatible wallets. Additionally, the Smartlink app features dispute resolution services, allowing users to raise tickets
and follow-up on the arbitration process through the app.

3.3 Transferring Digital Property

The blockchain is perceived as a potentially revolutionary solution for transferring digital property efficiently, safely, and in a relatively easy way [48]. The benefits of smart contracts and the underlying blockchain layer can serve to be the catalyst for a new era of e-commerce. Additionally, some features will require users of the Smartlink platform to go through a KYC and A.M.L. process to comply with Financial Action Task Force (FATF) guidelines. The buyer and seller must connect their Tezos compatible wallets to the Smartlink escrow services through the Smartlink API, and the data will be written to a database to create an escrow contract.

In order to execute any transfer of property through the smart contract, the buyer and seller have to agree on the set of rules of the contract, which will be executed after signing a particular transaction. Typical examples are the price of the exchanged digital property and the delivery timeframe. As shown in figure 2, the general smart contract process flow for transferring digital properties involves two stakeholders: a buyer and seller, whereby three smart contracts will be utilized to establish a robust escrow contract. The stakeholders connect through a compatible wallet with the Smartlink-API to validate the escrow and milestones written to a local database. The transaction data will be sent to the stakeholders to validate and sign if the stakeholders agree with the payment contract. Consequently, the type of preselected and approved means of payment (i.e. cryptocurrency) will be sent to the Payment Smart Contract. Additionally, the required amount of the preselected cryptocurrency will be calculated and verified through the Smartlink API. If the stakeholders agree and validate the transaction, the smart contract will create the payment and permit, and the Smartlink API will verify the payment data. The stakeholders will be notified of the created payment through email and form a consensus if the created payment complies with the preset requirements.

The escrow can be made through the escrow smart contract if both stakeholders comply. Finally, the permit is verified by connecting with the Payment smart contract and the escrow validity by the Smartlink API. The involved stakeholders will be notified by another email that the escrow is successfully launched, therefore legally binding the participants to the smart contract.

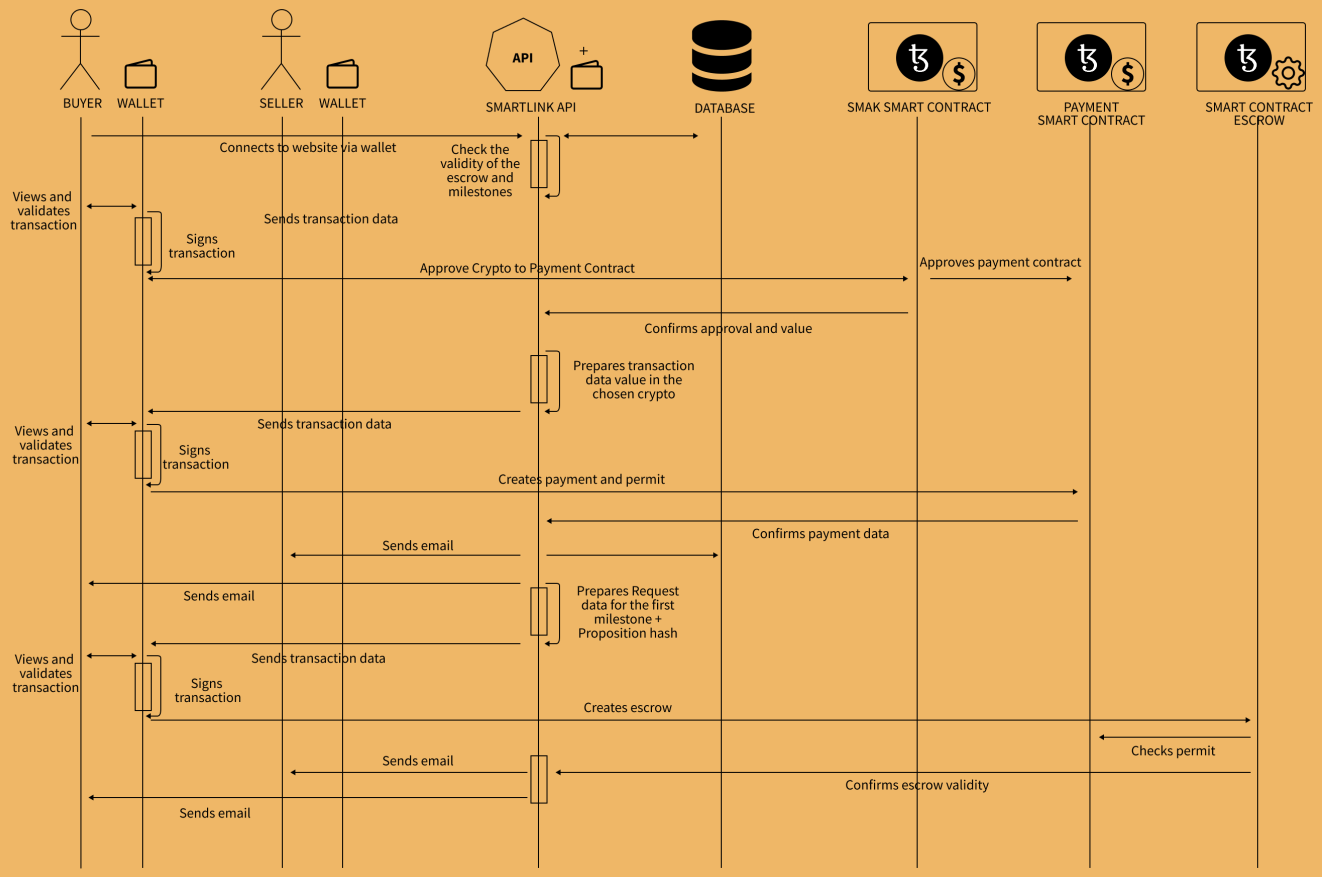

Figure 2: Workflow of a Digital Asset transaction using the Smartlink Escrow module

3.4 Transferring Physical Property

The main challenge for tracking physical products on a blockchain is the feature to be individually recorded. The scalability of blockchains can be a limitation due to the required amount of transactions. Additionally, preserving off-chain data in an integer, privacy-friendly, and equal manner can be perceived as complex. A typical example is the blockchain certifications of the Marine Stewardship Council (hereinafter: M.S.C.), which acts as a neutral, trusted third-party that can track the commercial journey of seafood. However, the transportation path is inaccessible for the consumer, and the application is running on a permissioned blockchain. The primary purpose of M.S.C. is to set a standard for sustainable fishing. A recent report has shown that the M.S.C. certifications are not as sustainable as supposed due to laxity and inconsistencies [49]. The leading causes are that the M.S.C. label rules are too lax due to information asymmetry.

The consumer must trust manufacturers or third parties that the data hosted on the permissioned blockchain has not been altered. Therefore, the blockchain certifications of M.S.C. are as inefficient as non-blockchain supply chain solutions. Additionally, the certifications suffer from the principal-agent problem, whereby the clients' interests of M.S.C. and M.S.C. itself are not aligned. Smartlink recognizes the implications of information asymmetry and eliminates any information failures. The Smartlink escrow service utilizes various on and off-chain mechanisms that verify the counterparty's identity and allow end-to-end tracking of the physical property. A built-in KYC process will hold potential malicious actors responsible for any harmful behaviour by verifying the involved participants. Furthermore, by strengthening the verification aspect of the

off-chain component of the product, asymmetric information for the involved parties is reduced.

3.4.1 Challenges with the exchange of physical assets

The exchanges of goods in the physical world involve entities and objects that may not be known in advance, and which interact with each other in ways that are difficult to verify by mechanized means. To wit, in any exchange in the real world there is necessarily an entity who is in charge of delivering the goods (whether a company or an individual, in which case it could be one of the Buyer or the Seller themselves). This shipping entity could in turn externalize its functions and rely on other subsidiary shipping services or intermediaries, depending on circumstances that involve human activities which cannot be foreseen a priori (supply sources, transportation, weather conditions, legal and customs regulations etc.). The problem that arises is how to authenticate these intermediaries, which may be dynamically involved in the shipping process, and how to collect the accord from the final users for them to participate, and the proofs that each intermediary complied with its corresponding function as to ensure the chain of custody of the goods being shipped, which is a required in order to establish liabilities of the different intermediaries in case of disputes.

In order to support these tasks and provide the required guarantees, other entities such as identity providers and/or know-your-client companies (KYC) may be involved as well, specially in the authentication of the intermediaries and in the establishing of a reputation system that would reflect on the trustfulness of each participant. The system architecture for the exchange of physical assets includes additional off-chain entities and an increased coordination complexity between themselves and the system, as depicted in Figure 3. This increased coordination complexity must be handled in an open and decentralized way and reflected on the blockchain, in order to keep up with the goals of Decentralized Escrow.

One well-known solution to introduce the state of an external system into a blockchain is to use the Oracle pattern[2]. This pattern consists in designating a trustful party, conventionally called an oracle, which is in charge of collecting information from the external entities, and of regularly posting a curated state of the off-chain world into the blockchain by calling an associated smart contract. The oracle may process data received from several sources before signing and posting it on chain. A relevant example of the application of this pattern in the Tezos ecosystem is the Harbinger Price Feed for digital assets[3].

From all the many issues that the exchange of physical assets pose, we focus on identity management and the shipping process. Our next sections explore solutions for decentralized identity management based on variations of the Oracle pattern alongside detailed workflows for authentication and for the transfer of custody of physical assets.

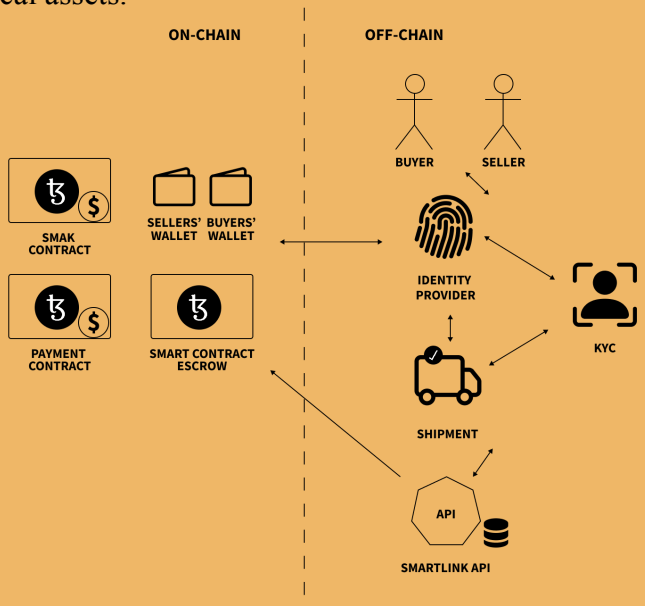

Figure 3: System architecture for the exchange of physical assets.

3.4.2 Decentralized identity management

In the current version of our Decentralized Escrow, identity management and authentication is

[2] https://research.csiro.au/blockchainpatterns/general- patterns/interacting- with- the- external- world/ oracle/

[3] https://harbinger.live/

carried out by the Smartlink API in a centralized way through its log-in service, and with the support of the off-chain data collected and stored by Smartlink. We now propose a decentralized model for authentication that overrides the Smartlink API log-in service and stores the identities of the registered users directly on-chain. Our objective is not to remove the current log-in service but to enable secure and heterogeneous methods (not necessarily controlled by Smartlink) to interact with it by dynamically providing identities from the off-chain world. These identities will be stored on chain, and the log-in service will act as a proxy to those identities. To truly replace Smartlink's log-in service by a decentralized solution could be an interesting endeavour in the long term, which goes further in the direction set by our proposal. For the moment, we aim at the more modest objective of allowing third parties to provide the identities of the subjects that could take part in the Decentralized Escrow.

We propose the use of the Identifier Registry pattern[4], which consists of a smart contract that maintains a list of mappings from identifiers to identities. In our case, an identifier is a public key from an asymmetric pair controlled by the subject relative to the identifier, and an identity is a tuple of attributes relative to the subject that includes the three compulsory attributes of Name, Email, and Tezos wallet Address, as well as the optional attributes of Postal Address and Birth Date (or Registration Date if the identity corresponds to a non-physical person), together with additional attributes that would describe the role of the subject in the system, and if it applies, its reputation according to some reputation schema provided by some KYC, or any other information required for establishing the legal liability of the subject. These attributes generalize the data model for Users in the Technical specification of the Decentralized Escrow [91].
The identifier (the public key) uniquely identifies each subject and enables the authentication of any message or event issued by the subject, via cryptographic signatures. The Tezos wallet address helps to verify the blockchain transactions and smart-contract invocations issued by the subject, and the Email provides a channel for notifying the result of the various operations performed by the subject.

We next propose two solutions for identity management in which the identity providers and the methods used for validating the identities correspond to opposed cases between authoritative identity sources and self-sovereign identity: the first solution uses certificates issued by a certification authority; the second solution uses the Blockchain and Social Media Account Pair pattern[5], which allows for the verification that a blockchain address and a social media profile are controlled by the same subject, thus lifting the trustworthiness of the social media.

Identity provided by a Certification Authority
Figure 4 below depicts the workflow for the registration of a new identity into the Identifier Registry using a Certification Authority (hereinafter: CA) as the identity provider. A subject that wishes to be registered using this method first requests a digital certificate from the CA. This certificate certifies the ownership of the pair of asymmetric cryptographic keys associated to it (we write KS and PK S respectively for the private and public key of subject S). This certificate can be validated by anyone in possession of the public key of the CA. After receiving the certificate, the subject forwards the certificate and the signed identity (notice that the identity may contain information not included in the certificate) to an Adapter smart contract. Communicating these credentials first to the on-chain Adapter serves the purpose of binding them to the Tezos wallet address controlled by the subject. The Adapter in turn forwards the identity and the credential to an Oracle by issuing some transaction that signals a query to the Oracle to validate the newly received

[4] https://research.csiro.au/blockchainpatterns/general- patterns/self- sovereign- identity- patterns/ identifier- registry/

[5] https://research.csiro.au/blockchainpatterns/general- patterns/self- sovereign- identity- patterns/ bound- with- social- media/

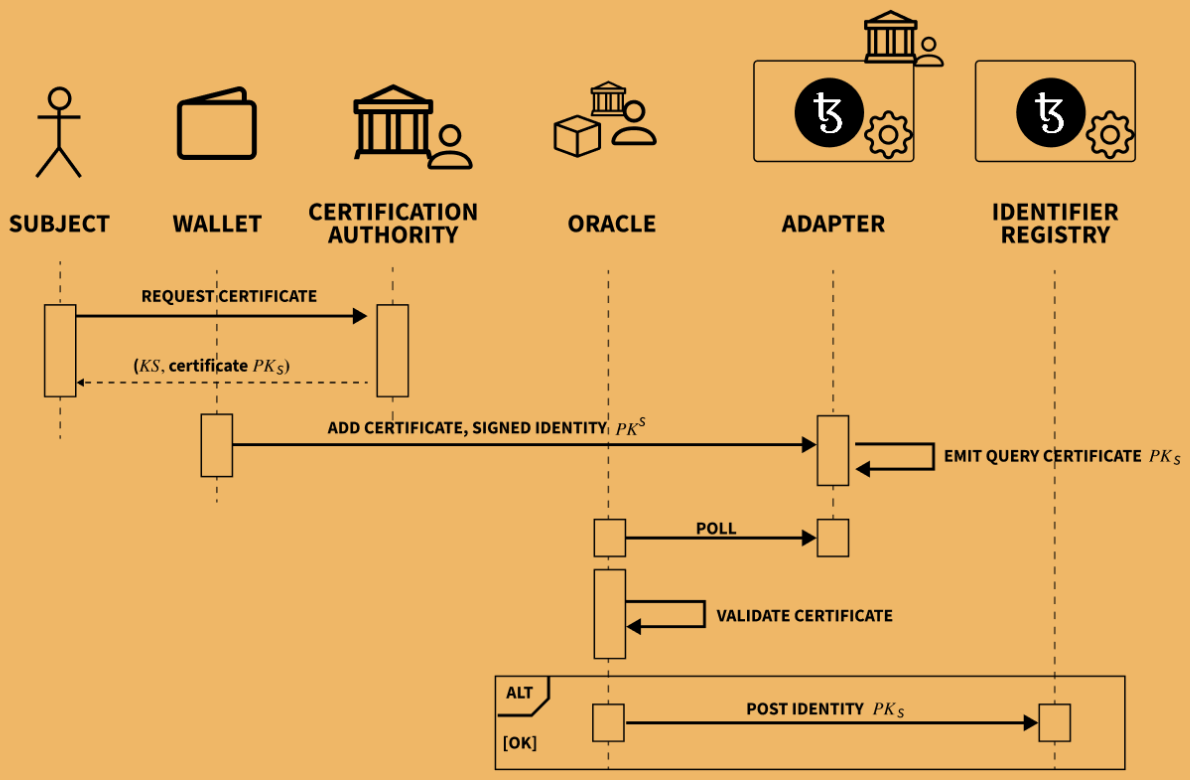

Figure 4: Workflow for registration using a Certification Authority.

identity.[6] Once the Oracle retrieves the certificate and the signed identity from the Adapter, it checks the validity of the certificate before posting the identity of the subject on chain, which is stored as a new mapping by the Identifier Registry smart contract. The Adapter and the Identifier Registry could be in principle co-located on the same smart contract, but separating them in different smart contracts matches better with the functional decomposition of the solution (they truly serve different goals) and allow to extend the solutions with more or different adapters without the need of modifying the Identifier Registry smart contract.

Identity provided by the Blockchain and Social Media Account Pair pattern Figure 5 depicts the workflow for the registration of a new identity into the Identifier Registry using the Blockchain and Social Media Account Pair pattern. A subject that wishes to be registered using this method first generates an asymmetric cryptographic pair on its own. Once this pair is generated, the subject posts the public key together with the signed identity in the profile of some social media that the subject controls, obtaining the url of this post. Later on, the subject forwards the signed url to an Adapter smart contract. The Adapter, in turn, forwards this url to the Oracle by emitting an event on-chain to query the Oracle to validate the url and the identity contained in the social media post. The Oracle can now retrieve the post at the url, check the signatures, and thus validate that the Tezos wallet address used to invoke the Adapter smart contract is in fact controlled by the same subject that controls the social media profile. This validation lifts the trustworthiness of the social media on the identity that controls the profile, without the need for any express involvement from the social media in this authenticating operation. Finally, the oracle posts the identity of the subject on chain, which

[6] This mechanism, which is referred to as "emitting an event" in Solidity parlance can be implemented as well over Tezos with the inclusion of some transaction tagged by the Adapter that the Oracle will read.

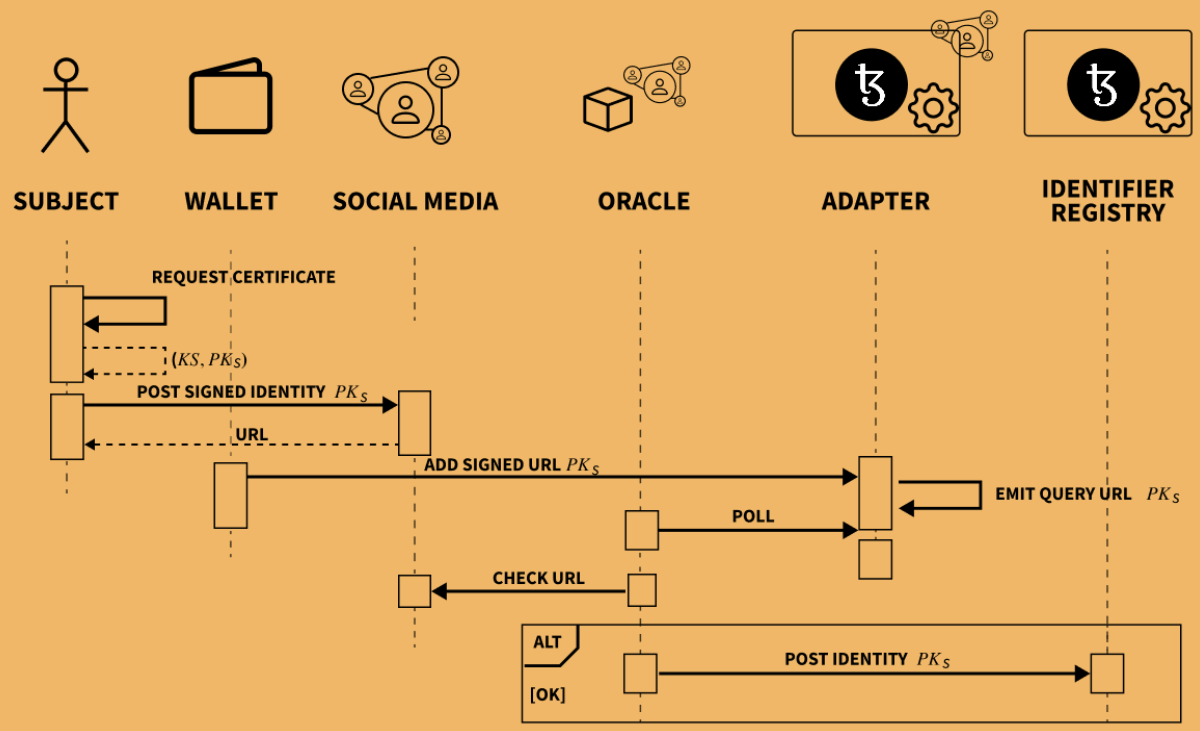

Figure 5: Blockchain and Social Media Account Pair

is stored as a new mapping by the Identifier Registry smart contract.

Other methods that consider third-party identity providers are possible. In particular, it is worth exploring the methods that involve open standards for authentication delegation, like implementations of the OAuth standard, and/or management of Decentralized Identity Documents (DID), like the Tezos Decentralized Identifier Management TZIP-19[7]. All of them could be adapted to our setting by using some variation of the workflows above.

Figure 6 depicts an abstract workflow for third-party identity providers which contains the key elements to bind an identity validated by some trustful entity with a Tezos wallet address. For this purpose, the Subject and the Identity Provider interact with each other to the end of issuing some credentials, whose type may depend on the Identity Provider and the method used. The Subject then posts these credentials into the blockchain (which binds them to the subject's wallet address) through the Adapter smart contract. The Adapter notifies the Oracle, which will interact with the Identity Provider (ans possibly with the Subject) in order to establish the validity of the identity and will finally post the identity to the Identifier Registry. Although not exploited in our examples above, the ability of the Oracle, Identity Provider, and Subject to share off-chain secrets may be crucial for establishing the validity of the identity while complying at the same time with any specific confidentiality requirements that any of the three parties may require. Only the credentials that prove the validity of the identity must be stored on chain. Since the system may require more than one identity provider, one can consider several in- stances of the solutions above that would coexist with each other. Figure 6 below depicts a scenario in which several alternative identity providers and their associated oracles will feed the Identifier Register. However, the solution in this figure cannot be readily applicable: the replication of the oracles comes at some cost, since it poses the very same

[7] https://gitlab.com/tezos/tzip/- /blob/master/proposals/tzip- 19/tzip-19.md

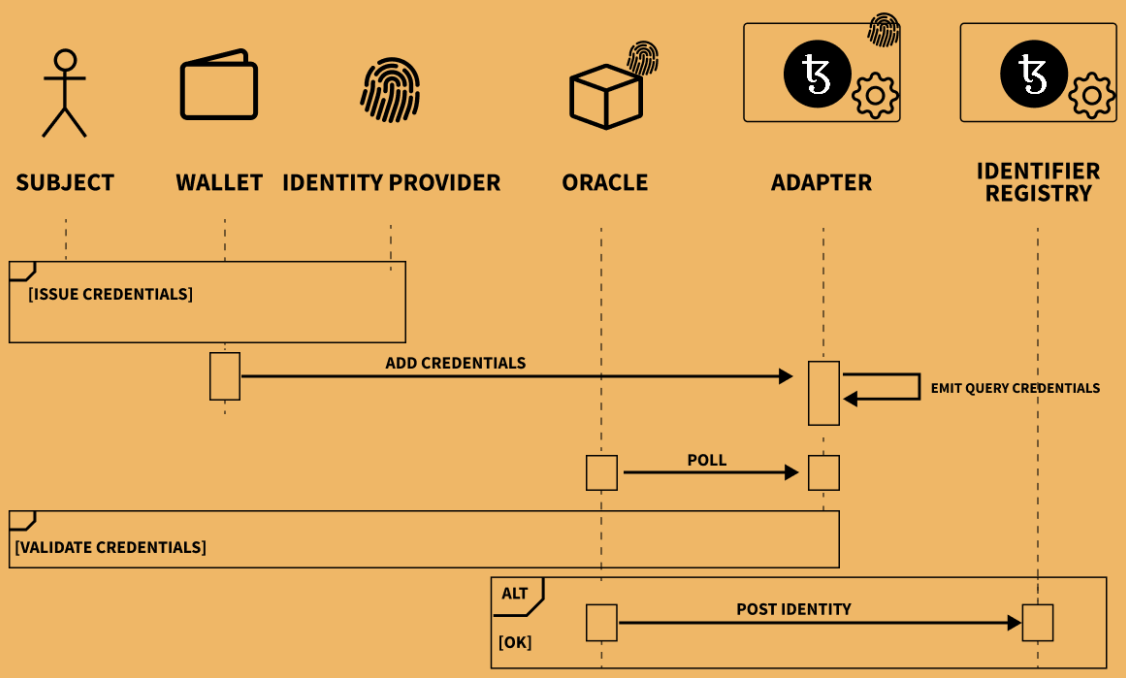

Figure 6: Abstract workflow for third-party identity providers.

safety problems that the ones addressed by the blockchain's consensus protocol. Two of the oracles could disagree on the off-chain information published on the blockchain, and post contradictory identities to the Identifier Registry (e.g., two mappings for the same identifier that carry different attributes) thus incurring in a violation of safety. This violation of safety could be the result of the failure of some oracle, or even worse, the result of a deliberate misbehaviour of some malicious oracle in an attempt to attack to the system (a Byzantine behaviour). The next section below explores a generalization of the Oracle pattern that provides a solution to the replication of oracles by adopting some ad hoc Byzantine-fault tolerance (BFT) technology that adds to that of the blockchain, and whose purpose is to support a particular blockchain-based application.

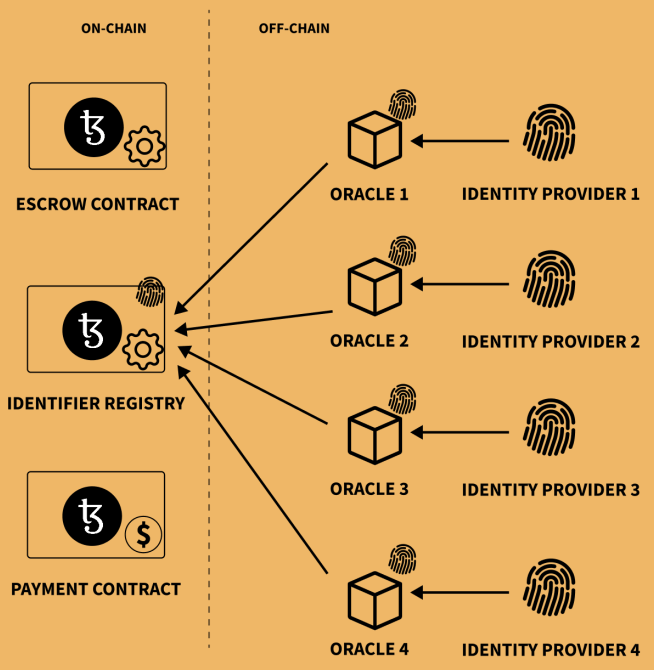

Figure 7: Identity management with several identity providers.

3.4.3 Decentralized oracle networks

Solutions for oracle replication have appeared in several sources in the literature. In the Decentralized Oracle pattern,[8] the trustworthiness of a single oracle is improved by using a set of oracles such that each of them would query data from independent sources, and the associated smart contract will only consider the information as valid if it comes from a majority of the oracles.

The decentralized oracle networks (hereinafter: DON) of [93] take this idea further and introduce a framework for hybrid smart contracts, a novel paradigm for blockchain-based applications that combines the following two kinds of computation environments:

(i) On-chain computation environments: guarantee availability and persistence through a blockchain, which is decentralized and open, and implements a safe, non-repudiable, append-only ledger. However, these environments are not performant due to the limited computational power of blockchains and break confidentiality since blockchains expose their entire state for verification purposes.

(ii) Off-chain computation environments: may provide confidentiality and performance, since they are centralized and closed, and may be supported by high-performance hardware. However, these environments may not be generally available since their host can terminate them at his or her discretion, and can neither ensure persistence since they may lack reliable network access.

The two kinds of computation (on-chain and off-chain) have complementary properties and it is very appealing to take advantage of both. This kind of composition is already present in existing layer-2 mechanisms. An example of off-chain computation environments with advanced guarantees are the trustworthy execution environments (hereinafter: TEE) of [94]. The TEEs are described as fully isolated computation environments that prevent different processes running on them to tamper with each other, or to even learn the state of each other. Such systems are implemented with hardware-supported security-related operations, like they Intel Software Guard eXtensions (SGX) instruction codes, which use private regions of memory that are decrypted by the CPU on-the-fly only for the code running from within such private regions. This prevents the private regions to be accessed even by processes that run at higher privilege levels, thus preventing the operating system, or even the host of the environment, to break confidentiality without compromising performance.

Without going so far as to rely on systems with guarantees as the ones provided by the TEEs of [94], which have strong hardware requirements, the use of general-purpose off-chain computation presents many opportunities to achieve performance and to keep certain information secret, which is impossible in the on-chain setting. The off-chain computation environments targeted by the DON in our proposal consists of those controlled by some authority it may be seen reasonable to trust, like for instance the computation hosted by the provider of the application (in our case the Smartlink API), or otherwise those computation environments for which some BFT technology is amenable that would render them trustworthy. Obviously, this BFT technology ought to be cheaper than the BFT implemented by the Tezos blockchain for the combination of the two computations (on-chain and off-chain) to be advantageous. Such BFT technology may be available in computation environments hosted by the provider of the application together with its business partners. This BFT technology needs not define a stand-alone system, since whose sole purpose is to support the blockchain-based application it is associated with.

[8] https://research.csiro.au/blockchainpatterns/general- patterns/interacting- with- the- external- world/ decentralized- oracles/

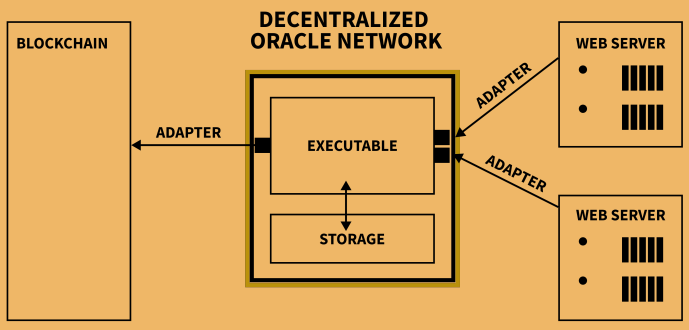

Figure 8: Conceptual structure of a DON [93]).

Figure 8 depicts the structure of a DON, highlighted in yellow. A DON consists of a set of oracles, each of which carries out some functionality (Executable) by gathering data from the off-chain services and relying it to the smart contracts on chain, which it does with the help of Adapters that target the specific off-chain and on-chain services used. An oracle can as well read and write information from some Storage, which in principle remains in control of the oracle and could therefore contain information private to the oracle.
The oracles within the DON communicate and cooperate with each other to fulfil the follow- ing design goals:

(i) Trust minimization, for enforcing protection against corrupted oracles by enabling a certain minority of oracles to inspect others and issue flags if they observe misbehaviour.

(ii) Incentive-based (crypto-economic) security, by incentivizing the oracles to behave correctly and avoid bribing by the means of staking (requiring the oracles to deposit funds in order to operate with the system) and slashing (confiscating the said deposits in case of misbehaviour).

(iii) Abstracting away complexity, as to blur the on-chain/off-chain distinction for the develop- ers and users of the decentralized services.

(iv) Scaling, by meeting the demands of high performance, while minimizing on-chain fees for both the providers of smart contracts and the final users.

(v) Confidentiality, by enabling oracles to retrieve in formation from off-chain systems in ways that protect user privacy.

(vi) Order-fairness, as to protect the system from censorship and front-running attacks, this is, attacks in which malicious oracles delay the posting on the blockchain of certain information they have received, while profiting from the malicious use of this information.

In a nutshell, a DON is a mechanism that enables to extend an on-chain computation environment by layering heterogeneous consensus technology on top of it, in order to bridge it with a set of high-performant off-chain computation environments, with the objectives of having crypto-economic security, abstracting away complexity, and enabling scalability.
The BFT technology that we propose for the DON in the setting of the Decentralized Escrow is based on the Federated Byzantine Agreement Systems of the Stellar blockchain [95]. The next section describes these systems in detail and presents an example of their application in our proposed solution.

3.4.4 Federated Byzantine agreement systems

The federated Byzantine agreement systems (hereinafter: FBAS) used by the Stellar blockchain [95] are a generalization of the already classical Byzantine quorum systems of [96], with the possibility of organic growth of such quorum systems driven by market forces. The trust topology in an FBAS emerges from the individual choices of each node in bottom-up fashion, bridging the traditional BFT technology based in quorum systems that is used in permis-

sioned blockchains with the openness of the public blockchains, for which the addition of a new node has a very reduced cost. These systems were proposed not so long ago, but they have reach a relative maturity after the extensive study of their properties [96, 97, 98, 99, 101, 102].
In an FBAS, a node independently chooses to trust the parties whom it considers important, where these choices are called slices. The individual choice of slices at each node induces a quorum system, in which a quorum is a set where all the nodes contained in it have some of their slices fulfilled within the set. This results in the organic growth of the quorum system lead by market forces, akin to the routing tables of IP routers. The FBASs come with associated BFT protocols that are based on the following two principles:

(i) Before externalizing a decision, a node must ensure that this decision does not contradict other decisions that have been previously externalized by the parties in its slices.

(ii) A node will only externalize a decision when it corroborates that there is enough information in the system (i.e., has heard enough messages) as for all the other nodes in at least one of its slices to externalize the same decision.

The FBAS formalism is expressive enough as allow nodes to choose to trust alternative sets, in a way similar to non-deterministic choice, such that for a node to externalize decision, it suffices to agree with the nodes in only one of its slices. This confers great flexibility in the individual choices of trust, and gives rise to a topology of trust that are much more general than the ones entailed by centralized quorum systems.

In particular, the FBASs allow for a hierarchical topology of trust as the tiered quorum structure depicted in Figure 9, where the nodes at each tier choose as their only slice a reduced number

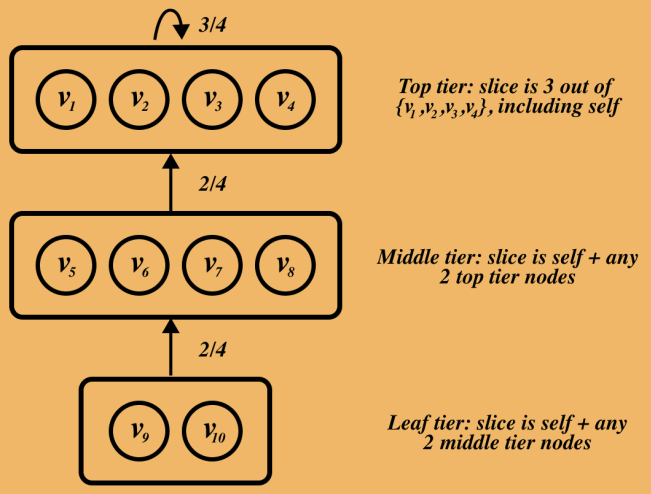

Figure 9: Tiered quorum structure example [95].

of nodes in the tier immediately above them. The nodes in the top tier need necessarily to choose as slice a bigger number of nodes in the top tier itself. At the top tier, the threshold for tolerance of Byzantine parties is similar to the threshold in centralized quorum systems (this is, a node needs to agree with strictly more than two thirds of correct nodes). However, the threshold of tolerance in the lower tiers decreases, since they only need to lift their trust to successively higher tiers such that the induced quorums ultimately have non empty intersection in the top tier (typically, this means that a node needs to agree to strictly more than one third of correct nodes form the upper tier). This decrease in the tolerance threshold enables an exponential reduction in the communication complexity of the protocols that run on an FBAS, since the tiered structure could adopt the form of a tree rather than that of a list (this is, more than one lower tier trust some upper tier, and the level of each tier is akin to the depth in the resulting tree, with a single top tier at the root).

The FBASs enjoy the following key properties:

(i) Flexible trust, since nodes have the freedom to choose who they see fit.

(ii) Decentralized control, since anybody can join by picking its choice of trust, and the quorum system will organically grow according to those choices.

(iii) Low latency, since agreement can be reached by each node exchanging information only with its vicinity.

The properties of the FBASs that we have analyzed render them an ideal candidate for the BFT technology in the DON of our solution: the possibility of alternatively trusting one slice or the other can be used to model the non-deterministic choice on the identity providers that feed the Identifier Registry in the Decentralized Escrow; some methods may be more trustworthy that others, and therefore the slices will include only one instance of them, or alternatively other less trustworthy methods could be used, which may require some degree of redundancy, and thus other slices would include more than one instance of them.

The thresholds needed for the slices to uphold the required properties in an FBAS may be in practice bigger than the available alternatives. For instance, in the setting of the identity providers it may be unrealistic to require to trust three out of four certification authorities (there might not be so many available to start with). In this case, the FBASs could be applied by letting each organisation to provide more than one node (i.e., intra-organisation replication), all of which will include the same certification authority in their slices. The final decision could then be made upon the agreement of several nodes from different organizations. In order to retain flexible trust and to avoid sibling attacks in this scenario, each of the slice needs to include at least a small number of nodes from sufficiently many different organisations. By all means, our proposal of using FBASs is conditional on an increase in the complexity of the trust topology of the network of oracles. It may not be needed at first, but it is a good candidate if we turn the DON into an open system with the participation of organizations other than Smartlink, in which case the the number of oracles involved and the complexity of their interactions is expected to increase.

An example of application of the FBASs and the DON in the setting of identity providers is depicted in Figure 10. We consider one oracle associated to each identity provider on the right (both numbered form 1 to 4) that perform the actions described in the abstract workflow of Figure 6. Each oracle has an adapter associated to it that consists of a smart contract that behaves as the Adapter in Figure 6. Rather than communicating directly to the Identifier Registry, these four oracles exchange the information they intend to post among themselves, and also with an additional oracle (Oracle ID) that constitutes the only node in the lower tier and which is in charge of aggregating the information received by the other four. An oracle in the top tier decides on some identity when it agrees with a set of three oracles from the top tier itself. The oracle in the bottom tier decides on an identity when it agrees with other two oracles in the top tier. The combination of these two conditions entails that a quorum that contains the oracle in the bottom tier needs to contain as well at least three oracles from the top tier, which ensures the safety guarantees and provides tolerance to at most one oracle in the top tier being Byzantine. Once Oracle ID has reached an agreement by the means of some FBAS consensus protocol (see [95, 99, 97, 101, 102] for the details of such protocols) it will post the decided identity to the Identifier registry smart contract, which acts as its Adapter. (The example in Figure 10 is for illustration purposes only: it uses a plain tiered quorum structure with simple thresholds for the tolerance to Byzantine parties. Other more realistic trust topology as the one discussed in the previous paragraphs would be applied in a production system.)

Our next section presents detailed specifications for the use case of the exchange of physical assets, which use our proposed solution for identity management based on the elements that we have presented so far (Blockchain patterns, DONs, FBASs).

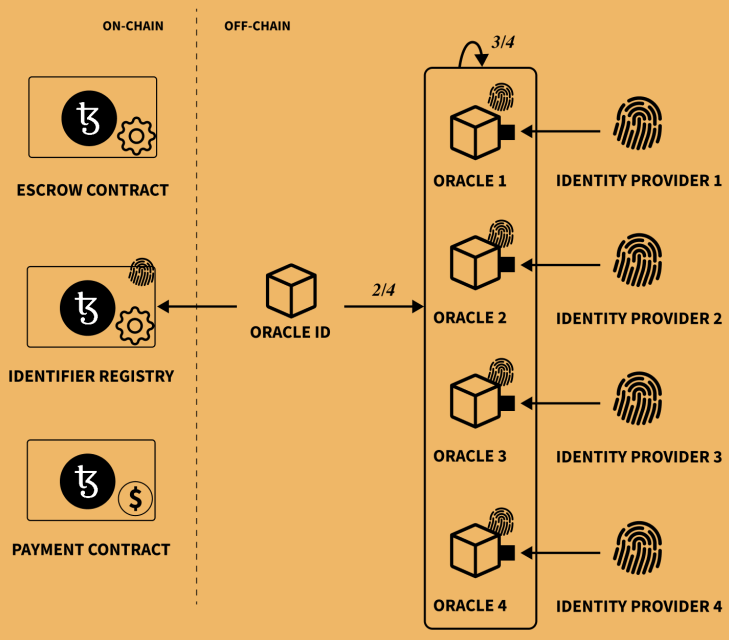

Figure 10: DON for identity providers with FBAS technology.

3.4.5 Detailed specifications for the exchange of physical assets

We put in place the identity management described in the previous sections, and present detailed specifications of two concomitant workflows in the use case of the exchange of physical assets: the workflow for the transfer of custody in the exchange of physical assets, and the auxiliary workflow for the connection to the Smarlink API. We first present the auxiliary workflow for the connection to the Smartlink API.

Connection to the Smartlink API In the workflow depicted in Figure 11, the Identifier Registry is the source of the identities for the users of the system, while Smartlink API's log-in service acts as a proxy to these identities, and controls a Data Base which, for efficiency concerns, caches the identities registered in the Identifier Registry. A User who wants to connect to the system issues a connect query to the Smartlink API signed by the User's public key PK_U . The Smartlink API, in turn fetches the Data Base (the cache) for the identity that corresponds to PK_U . If there is cache hit, the identity is retrieved and the Smartlink API answers the User with a successful connection. If there is a cache fail (the key is not stored in the Data Base) then the Smartlink API will query the Identifier Registry to authenticate the identifier PK_U . If the Identifier Registry does not contain a mapping for this identifier (the User has not been authenticated) then it returns an authentication failure that is forwarded to the User by the Smartlink API. Otherwise (the User has been authenticated successfully) the Identifier Registry returns the User's identity, which is cached in the Data Base by the Smartlink API before answering the User with a successful connection.

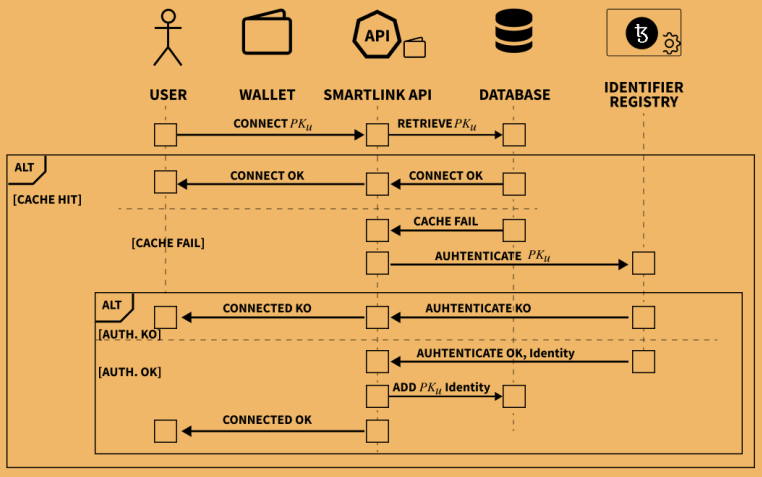

Figure 11: Workflow for the connection to Smartlink API.

Transfer of custody in the exchange of physical assets The workflow in Figure 12 combines ideas from both the Seller Credential pattern,[9] and the Off-Chain Secret Enabled Dynamic Authorization pattern.[10] In our case the credentials are those of the Recipient (identity authenticated

[9] https://research.csiro.au/blockchainpatterns/general- patterns/blockchain- payment- patterns/ seller- credential/

[10] https://research.csiro.au/blockchainpatterns/general- patterns/security- patterns/ off- chain- secret- enabled- dynamic- authorization/

by the Identifier Registry, which is implicit in the Recipient's connection to the Smartlink API, as described in the paragraph above). The recipient is authorized to receive the custody from the Dealer by the exchange of an off-chain secret. When a Dealer wants to transfer the custody of some physical asset, it connects to the Smartlink API and queries the transfer of custody to the Recipient identified by the public key PKR. If the Recipient is successfully authenticated by the

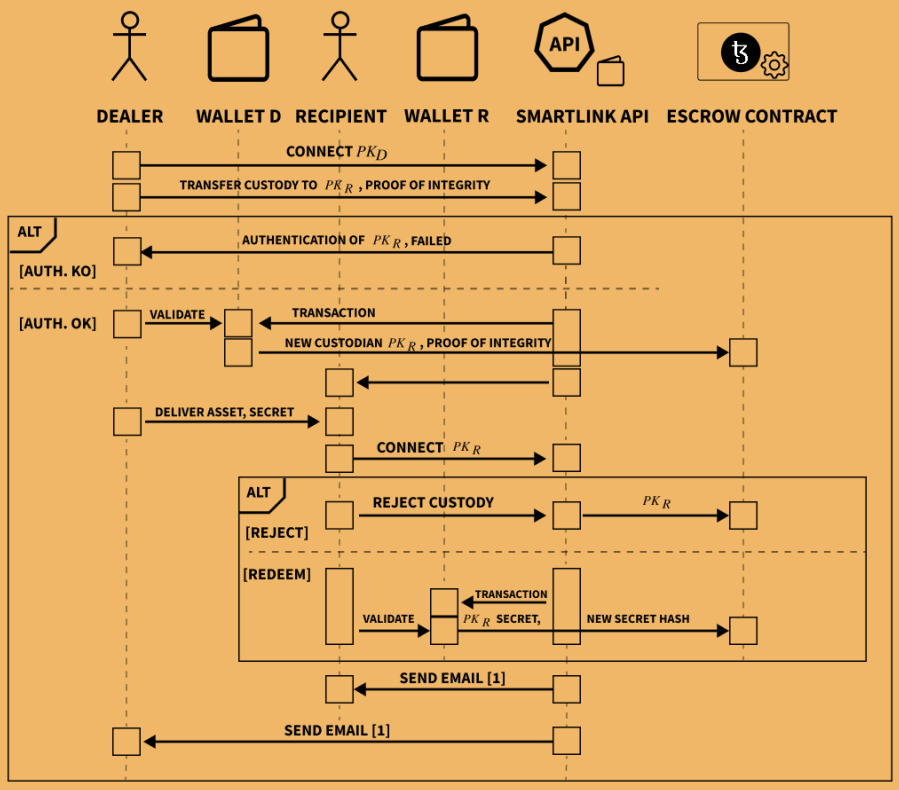

Figure 12: Workflow for the transfer of custody of a physical asset.

[1] The emails respectively notify the Dealer and the Recipient of the success or the failure of the transfer of custody. After a failure, the Dealer may retrieve the asset being delivered and any of them may chose to open a dispute.

Smartlink API (this triggers the workflow in the paragraph above) then the Smartlink API generates a transaction to invoke the Escrow contract to query for the new custodian, which is validated by the Dealer's Wallet and issued to the blockchain together with the public key of the Recipient and with a proof of integrity of the asset (i.e., graphical evidence like pictures, or other required information to check the integrity of the asset that may be specified by a manifest that accompanies the asset). Once this transaction is finalized on the blockchain, the Smartlink API will notify the Recipient through an email that includes the proof of integrity of the asset. Now the Recipient will wait for physically receiving the asset from the Dealer, together with the off-chain secret associated to the custody of the asset. If the Recipient does not accept the proof of integrity, or if the delivery of the asset never takes place in the expected time frame, then the Recipient will reject the custody of the asset by querying it to the Smartlink API. After the rejection of the custody, the Smartlink API will notify both the Dealer and the Recipient of this fact by email,

after which the Dealer may retrieve the asset and any of them may open a dispute.
Otherwise, if the Recipient accepts the proof of integrity, it would redeem the custody of the asset by querying it to the Smartlink API, by sending the off-chain secret received from the the Dealer. The Smartlink API will generate a transaction to invoke the Escrow contract to accept the transfer of custody, which will be validated by the Recipient by signing it with the Recipient's Wallet, and by providing the hash of a new off-line secret that is to be associated from now on to the custody of the asset. Once this transaction is finalized on the blockchain, the Smartlink API will notify both the Dealer and the Recipient by mail of the success of the transfer of custody, after which both parties conclude their interaction.

3.5 Handling Disputes

The expected global e-commerce market will be valued at approximately 5.5 trillion USD in 2022 [50]. The industry is one of the backbones of the global trade industry; due to the continuous global digitalization, the growth is expected to advance. The consumer-to-consumer e-commerce market, in general, has a significantly higher perceived risk than any other e-commerce market (e.g. Business-to-Consumer) [51]. Forsythe and Shi explained that the perceived risk in online shopping as the expected loss of a consumer correlated with specific online shopping behaviour [52]. The degree of asymmetric information is relatively high, which impacts the amount of moral hazard within the market [53].

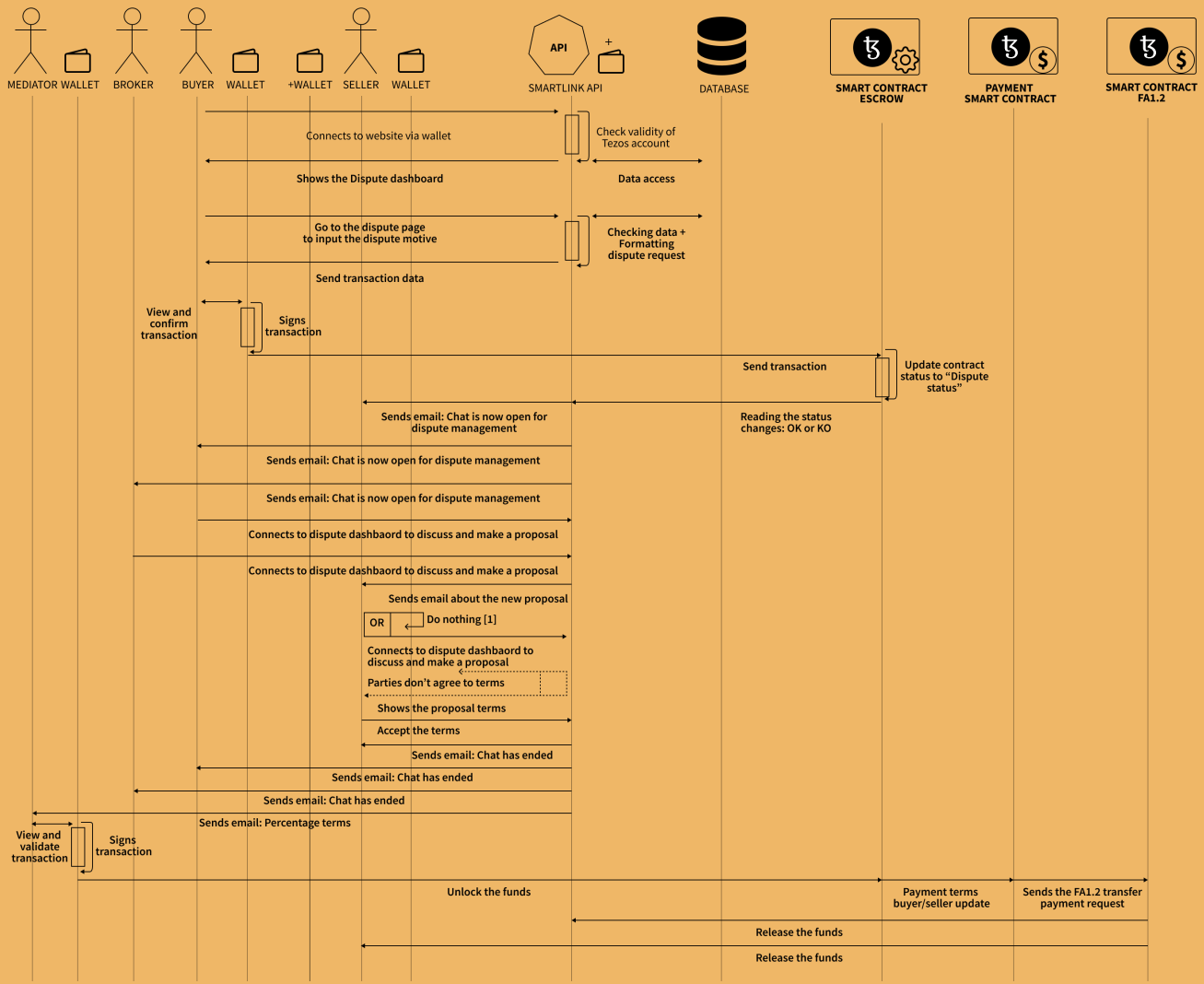

Figure 13: Workflow for a dispute resolution

Kuan, Bock, and Vathanophas highlighted that the quality perception of the dispute settlement system, data input, and service facilities have a significant impact on the initial buying and retention rate [54].

Smartlink acknowledges the significance of convenient and reliable dispute settlement systems. Figure 13 above illustrates the workflow of the Smartlink platform to handle dispute resolutions off-chain while the funds are safely kept in the smart contract. The system relies on a built-in chat feature dedicated to solving disputes on the platform and the potential intervention of a mediator if the parties can't agree to the new terms. Resolve Disputes Online (hereinafter: RDO) or a similar solution might be used as a dispute settlement mechanism. The provider is one of the leading Alternative Dispute Resolution (hereinafter: A.D.R.) software developers for several international and private institutions [55]. The RDO network consists of a network of judges, registered arbitrators, and a built-in A.D.R. process for a streamlined litigation experience. Furthermore, RDO features an AI-enabled mediation module for high volume dispute management and an expedited litigation process (21-day resolution) for high-ticket transactions. The smart contract infrastructure of RDO can be implemented with Smartlink. This solution would integrate mediation clauses and dispute settlement mechanisms through a voting system comprising professional arbitrators.

3.6 Other lines of work Smartlink will be exploring other existing Blockchain Patterns from CSIRO Data61 [96] that could help to make the functionality of Decentralized Escrow even more decentralized. We are aware that patterns such as Embedded Permission, Token Registry, Key Shards, Multiple Registration, Dual Resolution, Time Constrained Access, and Blockchain Anchor could benefit various aspects in the use case of the exchange of physical assets.

A long term endeavour which is particularly appealing is to explore the possibility of externalizing the functionality of the Smartlink API, whether into business partners of Smartlink, or into other third parties, by designing and exploiting cost models and incentive models that would make it interesting to other parties to develop and maintain proxies to the smart contracts in the Decentralized Escrow ecosystem.

4. Economy

The native utility token of the Smartlink ecosystem is SMAK. The token has a finite total supply of 896,083,333 tokens. The SMAK token will be used for payments and utility and is exchangeable for multiple Smartlink' services. The token functions of SMAK are versatile and can be divided into the following: medium of exchange and utility [59], ensuring appropriation of the platform's benefits [60].

4.1 Token Features

Utility and token features have become more and more important to the cryptocurrency industry over the last few years [61]. The cryptocurrency community is getting increasingly capital-efficient due to the number of deployed cryptocurrency projects that are rising while capital constraints remain. Among the top 20 crypto projects by market capitalization, roughly half are utility tokens projects at the time of reporting [62]. The SMAK token has multiple facets, and these can be broken down to Governance, Medium of Exchange, Fee Exemption, and Micro Rewards.

4.1.1 Governance

Smartlink intends to develop an on-chain governance system for its platform. On-chain governance refers to the set of rules and decision-making processes that have been coded into the underlying infrastructure of a blockchain-based system [63]. This type of governance defines the rules of interaction between involved participants

through the infrastructure; these interactions are conducted by rules embedded within the underlying blockchain code, often referred to as rule of code [64]. The rules may be layered; therefore, one set of rules is subject to another set [65]. For example, a particular rule may allow for platform infrastructure changes by defining the procedures to change other lower-level or potentially higher-level rules by themselves [66].

Smartlink community members will need SMAK tokens to participate in critical platform decisions, such as development proposals, partnerships, and integrations. A governance staking pool alongside a ranking system will help users identify the legitimacy of voters and proponents on the governance board.

Smartlink uses a whitelist to validate users' participation in the upcoming governance. The whitelist allows users to identify themselves as a natural entity through a decentralized registry that uses an off-chain authentication service. The service utilizes Tezos profiles SDK to retrieve user credentials, this is a web application where users can associate their public online identity (i.e. social media accounts) to their Tezos addresses. The whitelist allows users to be part of the Smartlink ecosystem and, therefore, have voting power on the upcoming Smartlink DAO. It also prevents voting spamming, whereby users manipulate proposals by possessing multiple accounts.

4.1.2 Internal Medium of Exchange

In addition to the SMAK token that will be used as a medium of exchange on the Smartlink platform, a few other FA 1.2 compatible tokens are supported. Moreover, using the SMAK tokens in transactions will reduce the transaction fee, which will be further highlighted in the upcoming paragraph "4.1.3 Fee exemption". Additionally, consumers will be eligible to receive Micro-Rewards if transactions use SMAK as a medium of exchange; this will be further highlighted in paragraph "4.1.5 Micro Rewards". The accessibility of the platform is considered essential for the lasting of the platform. By allowing various FA 1.2 tokens, the user has a broad selection of supported tokens which lowers complexity and financial thresholds. As highlighted earlier in this whitepaper, accessibility is crucial for user adoption.

4.1.3 Fee Exemption

The native Smartlink token, SMAK, will nullify the transaction fee if the token is used as a medium of exchange. Therefore, users have a financial incentive to use the SMAK token in any Smartlink product. However, by not limiting the consumer to one asset but giving a financial incentive, the user is not limited in its potential choices while still being attracted to the platform. The transaction fee on any other supported FA 1.2 compatible token is 1%.

4.1.4 Micro Rewards

The Smartlink Micro Rewards are an innovative concept to increase the retention rate of consumers. The ecosystem grants Micro Rewards to the consumer for each transaction they have processed in SMAK. The Micro Rewards are stored on a reward wallet that the user may claim at any time.

4.2 Token Distribution

The token distribution model of Smartlink is focused on the sustainable growth of the project through a gradual token vesting unlock. The importance of a balanced token distribution is vital for the future ahead of the project because the token supply shocks can significantly impact the ecosystem. The Treasury wallet is the operational wallet of Smartlink and will be used for development and legal, marketing, and operational costs. The wallet will be replenished through transaction fees.

4.2.1 Revenue Model

The revenue model provides financial stability for business development, and companies are conducted to implement a revenue model that ensures healthy and sustainable long-term growth [67]. The Smartlink ecosystem will have a revenue model correlated with product usage. The consumers of the Smartlink products are paying a relative transactional fee. The transactional fee on any non-SMAK transaction is pledged to a 1% transaction fee. As highlighted earlier, utilizing SMAK on the Smartlink platform will grant a fee exemption. The revenue model of Smartlink is sustainable due to the imminent demand for a blockchain escrow service. Additionally, the transaction fee can be increased through a governance proposal if the transaction fee is insufficient to maintain the stability of the ecosystem.

4.3 Applications

The applications of Smartlink are versatile because of the combination of the flexibility of the ecosystem and the imminent need of consumers and businesses to decrease the perceived risk in the e-commerce industry. The accessibility of the ecosystem is one of the key points to attract potential consumers, so the ecosystem has a focus on a broad audience. The upcoming highlight applications are fictional and viewed by Smartlink as potential use-cases of the developed products.

4.3.1 High-value goods

The perceived risk of a consumer transaction increases if the involved financial risk is considered high. The financial risk is the potential monetary outcome associated with the initial purchase price and the maintenance cost of the product [68]. This particular risk is mostly perceived while transacting [69-79]. The financial risk increases if the product's value is higher, which expands the overall perceived risk of the consumer. The consumer wants to decrease this perceived risk by lowering the overall financial risk through a digital escrow service [80]. Smartlink escrow services allow consumers to reduce their perceived risk while being cost-efficient. Additionally, the ecosystem prioritizes the accessibility of the platform by allowing multiple FA1.2 compatible assets.

4.3.2Milestone Payments

Smartlink milestone management targets enterprises and individuals alike. The involved parties can set up various agreed-upon milestones using smart contracts. The completion of the first milestone automatically triggers the second milestone, progressing in a similar manner until the end of the transaction.

When a business hires a freelancer for a project, both parties can create a timeline, list of deliverables, set up an inspection schedule for individual stages, and respective payment timeframes. In the case of five separate stages in a project, the initial milestone smart contract comprises five sequential smart contracts. As the freelancer delivers the product, the business must inspect the delivery within the programmed inspection timeframe. Once the business accepts delivery, the smart contract releases payment for the milestone and automatically triggers the next milestone smart contract.

Smartlink milestone management features

Multi-stage smart contracts: The parties involved in a transaction can create multi-stage milestone smart contracts. It allows users to execute complex projects within agreed budget and timelines.

Auto-execution: Smart contracts execute upon the fulfillment of underlying conditions, providing swift execution with limited manual intervention.

4.3.3 Non-Fungible Tokens (NFTs)

The NFT market is relatively illiquid with extreme volatility [81]. Financial market inefficien-

cies cause the illiquidity of the market. The market has few participants due to the high financial barriers for entrants, scarcity, and indivisibility. NFT projects use a ceiling for the number of generated NFTs to create asset scarcity [82]. The NFT collectors are willing to pay a higher price premium for scarce assets; as a result, the floor price of these NFTs increases.
Furthermore, NFTs are indivisible, leading to a further increase in market suppression. The finite number of owners, due to the limited nature of NFTs, pushes NFT collectors to the financial boundaries that inflate the NFT prices. GameFi projects occasionally require players to have certain NFTs to interact with their game to put this in perspective. A typical example is Axie Infinity, one of the most popular blockchain games based on player counts [83]. The player has to acquire three Axies, in-game battle creatures, to be eligible to play the game. The current price of a single Axie is 0,02 ETH, which will result in a total expense of 0,06 ETH [84]. Due to artificial in-game asset scarcity, the price to engage with the Axie Infinity ecosystem is significantly higher to engage with any video game of a triple-A studio.

The Smartlink escrow service proposes a solution for this issue. Players can lend out their NFTs through the Smartlink escrow service and be compensated through a fixed payment or royalties for the perceived risk. Allowing players to lend out their digital assets increases the liquidity of GameFi NFTs and therefore lowers the liquidity risk for the asset class.

4.3.4 OTC trades

Institutional organizations are gradually accessing the cryptocurrency industry. The legitimacy of the digital asset industry is progressively increasing in the traditional financial market, and consequently, the trading volumes and asset values are increasing. The impact of the involvement of institutional institutions is observable with the rapid increase in Over-the-counter (hereinafter: OTC) trading [85]. OTC trading is conducted between two parties without going through an exchange.

The Smartlink Escrow Service can play a crucial role by improving the transparency of OTC trading through the underlying blockchain layer. Using Escrow smart contracts to trade Over the counter makes it more secure and transparent for trading fungible or non-fungible assets between two parties. Smartlink's escrow services eliminate trusted third parties and avoid distrust of involved parties.

4.3.5 Token Vesting

Vesting tokens is a useful feature for projects that want to bring transparency to their community and investors. Smartlink's vesting contract is scalable and can be used for an unlimited number of beneficiaries with each having different amounts of FA tokens. Cliffs can also be set with predetermined time periods. A complete dashboard for both admins and recipients will allow users to keep track of their vesting schedules and easily claim their rewards. There will be a fee for the token vesting module which will be charged in SMAK token.

5 Future

The Smartlink ecosystem has a wide array of usecases and will revolutionize the traditional and blockchain escrow services industry by significantly improving accessibility and transparency. The ecosystem is rapidly evolving and onboarding new ecosystem partners that will use the robust SSCL to create secure escrow contracts. The primary focus of giving the consumer a user-friendly experience remains; therefore, Smartlink will continue to integrate convenient features.
Smartlink will release more complementary products on top of its escrow service. The primary intention of Smartlink is to create a decentralized ecosystem whereby consumers and businesses are protected from malicious intent while

having access to a wide array of blockchain-based products.

Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of Smartlink, CEA List, Smartchain, House of Chimera or their affiliates and does not necessarily reflect the opinions of Smartlink, CEA List, Smartchain, House of Chimera, their affiliates or individuals associated with them. The opinions reflected herein are subject to change without being updated.

References

[1]Arrow, Kenneth J., 1974. The Limits of Organization. Norton, New York.

Axie Infinity. (n.d.). *Marketplace Axie Infinity*. Retrieved January 20, 2021, from https://marketplace.axieinfinity.com/axie/?auctionTypes=Sale.

[2] Putnam, R. D. (1993). What makes democracy work? National Civic Review, 82(2), 101–107. https://doi.org/10.1002/ncr.4100820204

[3] Knack, S., & Keefer, P. (1997). Does Social Capital Have an Economic Payoff? A Cross-Country Investigation. The Quarterly Journal of Economics, 112(4), 1251–1288. http://www.jstor.org/stable/2951271

[4] McEvily, B., Perrone, V., & Zaheer, A. (2003). Trust as an Organizing Principle. Organization Science, 14(1), 91–103. https://doi.org/10.1287/orsc.14.1.91.12814

[5] Guiso, L., Sapienza, P., & Zingales, L. (2000). The Role Of Social Capital In Financial Development. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.209610

[6] K.J. Stewart, Trust transfer on the World Wide Web, Organization Science 14 (2003) 5–17.

[7] Glaeser, Edward L., Laibson, David I., Scheinkman, Jose A., Soutter, Christine L., 2000. Measuring trust. Quart. J. Econ. 115 (3), 811–846.

[8] Berg, Joyce E.; Dickhaut, John W. and McCabe, Kevin A. "Trust, Reciprocity, and Social History." Games and Economic Behavior, 1995, 10(1), pp. 122– 42.

[9] Karlan, Dean S. "Social Connections and Group Banking." Yale University, Economic Growth Center Discussion Paper: No. 913, 2005.

[10] Schechter, Laura. 2007. "Theft, Gift-Giving, and Trustworthiness: Honesty Is Its Own Reward in Rural Paraguay." American Economic Review, 97 (5): 1560-1582. DOI: 10.1257/aer.97.5.1560

[11] Glover, S., & Benbasat, I. (2010). A Comprehensive Model of Perceived Risk of E-Commerce Transactions. *International Journal of Electronic Commerce*, *15*(2), 47–78 https://doi.org/10.2753/jec1086-4415150202.

[12] McEvily, B., Radzevick, J. R., & Weber, R. A. (2012). Whom do you distrust and how much does it cost? An experiment on the measurement of trust. *Games and Economic Behavior*, *74*(1), 285–298 https://doi.org/10.1016/j.geb.2011.06.011.

[13] Choi, S.-Y., Stahl, D. O., and Whinston, A. B. "The Economics of Electronic Commerce," Indiana: Macmillan Technical Publishing, 1997.

[14] Akerlof, G. "The Market for Lemons: Quality Uncertainty and the Market Mechanism," Quarterly Journal of Economics (84), 1970.

[15] Dimoka, Angelika & Hong, Kevin & Pavlou, Paul. (2011). On Product Uncertainty in Online Markets: Theory and Evidence. MIS Quarterly: Management Information Systems. 36. 10.2307/41703461.

[16] Mitnick, B. M. (1975). The Theory of Agency: A Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1021642

[17] PWC. (2020, December). *Fighting fraud: A never-ending battle - PwC's Global Economic Crime and Fraud Survey*. https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

[18] Nick Szabo. The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 1997.

[19] Ibid.

[20] Buterin, V. (2013, April). *Ethereum Whitepaper 1.0*. Ethereum. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[21] Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019.

[22] Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. *Financial Cryptography and Data Security*, 79–94. https://doi.org/10.1007/978-3-662-53357-4_6.

[23] Schane, S. (2002). Ambiguity and misunderstanding in the law. *Thomas Jefferson Law Review*, *25*(1), 167–193. https://www.proquest.com/docview/198186565.

[24] Raffles v. Wichelhaus (1864) Court of the Exchequer 2 Hurl. & C. 906.

[25] Alarie, B. (2009). Mutual Misunderstanding in Contract. Am. Bus. LJ, 46, p. 532.

[26] Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019.

[27] Solé, R. V., & Seoane, L. F. (2015). Ambiguity in language networks. *The Linguistic Review*, *32*(1). https://doi.org/10.1515/tlr-2014-0014.

[28] Merton, R. C. (1992). FINANCIAL INNOVATION AND ECONOMIC PERFORMANCE. *Journal of Applied Corporate Finance*, *4*(4), 12–22. https://doi.org/10.1111/j.1745-6622.1992.tb00214.x.

[29] Berger, A. N. (2003). The Economic Effects of Technological Progress: Evidence from the Banking Industry. Journal of Money, Credit, and Banking, 35(2), 141–176. https://doi.org/10.1353/mcb.2003.0009

[30] Allen, F., & Gale, D. (1991). Arbitrage, Short Sales, and Financial Innovation. *Econometrica*, *59*(4), 1041. https://doi.org/10.2307/2938173.

[31] Ross, S. A. (1976). Options and Efficiency. *The Quarterly Journal of Economics*, *90*(1), 75. Https://doi.org/10.2307/1886087.

[32] Houston, J. F., Lin, C., Lin, P., & Ma, Y. (2010). Creditor rights, information sharing, and bank risk taking. *Journal of Financial Economics*, *96*(3), 485–512 https://doi.org/10.1016/j.jfineco.2010.02.008.

[33]Beck, T., Chen, T., Lin, C., & Song, F. M. (2016). Financial innovation: The bright and the dark sides. *Journal of Banking & Finance*, *72*, 28–51 https://doi.org/10.1016/j.jbankfin.2016.06.012

[34]Shao, M. H., & Wen, S. H. (2010). A study on secure and fair escrow services for digital commerce. *International Conference on Networked Computing and Advanced Information Management*, *6*. https://ieeexplore.ieee.org/abstract/document/5572062/authors#authors

[35] Spence, A. M. (1975). Monopoly, Quality, and Regulation. The Bell Journal of Economics, 6(2), 417. doi:10.2307/3003237

[36] Escrow.com. (2020, January 1). *How long does it take for Sellers to be paid? - Escrow FAQ - Escrow.com*. Retrieved January 12, 2022, from https://www.escrow.com/support/faqs/how-long-does-it-take-for-sellers-to-be-paid

[37] Burri, X., Casey, E., Bollé, T., & Jaquet-Chiffelle, D. O. (2020). Chronological independentlyverifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation*, *33*, 300976. https://doi.org/10.1016/j.fsidi.2020.300976

[38] Raskin, M. (2016). The Law of Smart Contracts. *SSRN Electronic Journal* https://doi.org/10.2139/ssrn.2842258.

[39] Ibid.

[40] Goodman, L. M. (2014, September). *Tezos — a self-amending crypto-ledger White paper*. Tezos. https://tezos.com/whitepaper.pdf

[41] *Getting started with FA1.2 · Digital Assets on Tezos*. (n.d.). Https://Assets.Tqtezos.Com/. Retrieved January 15, 2022, from https://assets.tqtezos.com/docs/token-contracts/fa12/1-fa12-intro/

[42] Tezos. (n.d.). *FA2*. Tezos Developer Portal. Retrieved January 15, 2022, from https://tezos.b9lab.com/fa2/*Top Blockchain Games*. (n.d.).

[43] Ibid.

[44] Square. (2021, December). *Square Q3 2021 Shareholder Letter*. https://s29.q4cdn.com/628966176/files/doc_financials/2021/q3/SQ-3Q-2021-Shareholder-Letter.pdf

[45] Bloomberg, K. O. (2022, January 16). Bitcoin's Dominance of Crypto Payments Is Starting to Erode. Time. Retrieved January 15, 2022, from https://time.com/6139727/bitcoin-crypto-payments/

[46] Kharif, O. (2022, January 17). *Bitcoin's Dominance of Crypto Payments Is Starting to Erode*. BloombergQuint. Retrieved January 18, 2022, from https://www.bloombergquint.com/crypto/bitcoin-s-dominance-of-crypto-payments-is-starting-to-erode

[47] Froehlich, M., Wagenhaus, M. R., Schmidt, A., & Alt, F. (2021). Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency

Users. Designing Interactive Systems Conference 2021. doi:10.1145/3461778.3462071

[48] Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. IEEE EUROCON 2017 -17th International Conference on Smart Technologies. doi:10.1109/eurocon.2017.8011213

[49] Bloomberg. (2020, May). *The sham of the MSC label*. https://www.bloomassociation.org/wp-content/uploads/2020/05/sham-msc-label.pdf

[50] Keenan, M. (2021, May 13). *Global Ecommerce: Stats and Trends to Watch (2021)*. Shopify Plus. Retrieved January 18, 2022, from https://www.shopify.com/enterprise/global-ecommerce-statistics

[51] Hsieh, M.-T., & Tsao, W.-C. (2013). Reducing perceived online shopping risk to enhance loyalty: a website quality perspective. Journal of Risk Research, 17(2), 241–261. doi:10.1080/13669877.2013.794152.

[52]Forsythe, S. M., and B. Shi. 2003. "Consumer Patronage and Risk Perceptions in Internet Shopping." Journal of Business Research 56 (11): 867–875.

[53] Institute for Information Industry, Market Intelligence & Consulting Institute. 2011. Taiwan E-Commerce Yearbook. Taipei: Ministry of Economic Affairs, R.O.C. Press.

[54] Kuan, H. H., Bock, G. W., & Vathanophas, V. (2008). Comparing the Effects of Website Quality on Customer Initial Purchase and Continued Purchase at E-Commerce Websites. Behaviour and Information Technology, 27, 3-16. https://doi.org/10.1080/01449290600801959

[55] *Resolve Disputes Online*. (n.d.). Https://Resolvedisputes.Online/. Retrieved January 17, 2022, from https://resolvedisputes.online/

[56] Lo, Y. C., & Medda, F. (2020). Assets on the blockchain: an empirical study of Tokenomics. Information Economics and Policy, 100881. doi:10.1016/j.infoecopol.2020.100881

[57] FINMA, 2018. Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs). Regulatory guidance. Swiss Financial Market Supervisory Authority

[58] Catalini, C., Gans, J.S., 2018. Initial Coin Offerings and the Value of Crypto Tokens. Working paper 24418. National Bureau of Economic Research doi:10.3386/w24418.

[59] Lo, Y. C., & Medda, F. (2020). Assets on the blockchain: an empirical study of Tokenomics. Information Economics and Policy, 100881. doi:10.1016/j.infoecopol.2020.100881

[60] Catalini, C., Gans, J.S., 2018. Initial Coin Offerings and the Value of Crypto Tokens. Working paper 24418. National Bureau of Economic Research doi:10.3386/w24418.

[61] Häfner, S. (2021). Utility Token Design. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3954773

[62] CoinGecko. (n.d.). *Cryptocurrency Prices, Charts, and Crypto Market Cap*. Retrieved January 19, 2022, from https://www.coingecko.com/en

[63] Reijers, W., Wuisman, I., Mannan, M., & de Filippi, P. (2018). Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3340056

[64] De Filippi P, Wright A (2018) Blockchain and the Law: the Rule of Code. Harvard University Press.

[65] Reijers, W., Wuisman, I., Mannan, M., & de Filippi, P. (2018). Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3340056

[66] Ibid.

[67] Remeňová, K., Kintler, J., & Jankelová, N. (2020). The General Concept of the Revenue Model for Sustainability Growth. *Sustainability*, *12*(16), 6635. https://doi.org/10.3390/su12166635

[68] Sharma, J. K., & Kurien, D. (2017). Perceived Risk in E-Commerce: A Demographic Perspective.
NMIMS Management Review, XXXIV(1), 1–27.https://management-review.nmims.edu/wp-content/uploads/2017/april/perceived-risk-in-e-commerce-a-demographic-perspective-jitendra-k-sharma-daisy-kurien.pdf

[69] Cunningham, S. M. (1967). Perceived risk and brand loyalty. Risk taking and information handling in consumer behavior, 507-523.

[70] Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. European Journal of marketing, 27(3), 39-50.

[71] Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience, and Internet shopping behavior. Communications of the ACM, 43(11), 98-105.

[72] Crespo, A. H., del Bosque, I. R., & de los Salmones Sanchez, M. G. (2009). The influence of perceived risk on Internet shopping behavior: a multidimensional perspective. Journal of Risk Research, 12(2), 259-277

[73] Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. In SV-Proceedings of the third annual conference of the association for consumer research

[74] Peter, J. P., & Ryan, M. J. (1976). An investigation of perceived risk at the brand level. Journal of marketing research, 184-188.

[75] Ingene, C. A., & Hughes, M. A. (1985). Risk management by consumers. Research in consumer behavior, 1, 103-158.

[76] Almousa, M. (2011). Perceived Risk in Apparel Online Shopping: A Multi-Dimensional Perspective/LE RISQUE PERÇU DANS DES ACHATS EN LIGNE D'HABILLEMENT: UNE PERSPECTIVE DE DIMENSIONNELLE MULTIPLE. Canadian Social Science, 7(2), 23.

[77] Zhang, L., Tan, W., Xu, Y., & Tan, G. (2012). Dimensions of consumers' perceived risk and their influences on online consumers' purchasing behavior. Communications in Information Science and Management Engineering, 2(7).

[78] Candra, R. M., & Iahad, N. A. (2013). Analysis of Consumer Risk Perception on Online Auction Features. International Journal of Informatics and Communication Technology (IJ-ICT), 2(2), 64-70

[79] Almousa, M. (2014). The influence of risk perception in online purchasing behavior: examination of an early stage online market. International Review of Management and Business Research, 3(2), 779

[80] Hu, X., Lin, Z., Whinston, A. B., & Zhang, H. (2004). Hope or Hype: On the Viability of Escrow Services as Trusted Third Parties in Online Auction Environments. Information Systems Research, 15(3), 236–249. doi:10.1287/isre.1040.0027

[81] Kong, D. R., & Lin, T. C. (2021). Alternative investments in the Fintech era: The risk and return of Non-Fungible Token (NFT). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3914085

[82] Ibid.

[83] *Top Blockchain Games*. (n.d.). DappRadar. Retrieved January 20, 2022, from https://dappradar.com/rankings/category/games

[84] Axie Infinity. (n.d.). *Marketplace Axie Infinity*. Retrieved January 20, 2021, from https://marketplace.axieinfinity.com/axie/?auctionTypes=Sale

[85] Kochkodin, B. (2021, June 16). *Bloomberg - Are you a robot?* Bloomberg. Retrieved January 20, 2022, from https://www.bloomberg.com/tosv2.html?vid=&uuid=78f74c30-7f95-11ec-bb83-495151574d6c&url=L25ld3MvYXJ0aWNsZXMvMjAyMS0wNi0xOC92ZW50dXJlLWNhcGl0YWwtbWFrZXMtYS1yZWNvcmQtMTctYmlsbGlvbi1iZXQtb24tY3J5cHRvLXdvcmxkLXNyZWY9M1JFSEVhVkk=

[86] TABB Group. (2018, April). Crypto Trading: Platforms Target Institutional Market. https://research.tabbgroup.com/report/v16-013-crypto-trading-platforms-target-institutional-market

[87] Gandal, N., Hamrick, J., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, *95*, 86–96. https://doi.org/10.1016/j.jmoneco.2017.12.004

[88] White, J. T. (2016). Outcomes of Investing in OTC Stocks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2889360

[89] Fetisov, G. (2009). Measures to Overcome the Global Crisis and Establish a Stable Financial and Economic System. Problems of Economic Transition, 52(5), 20–33. doi:10.2753/pet1061-1991520502

[90] Irtyshcheva, I., Kramarenko, I., Shults, S., Boiko, Y., Blishchuk, K., Hryshyna, N., Popadynets, N., Dubynska, R., Ishchenko, O., & Krapyvina, D. (2020). Building favorable investment climate for economic development. *Accounting*, 773–780. https://doi.org/10.5267/j.ac.2020.6.006

[91] Jeremy Martin, Adrien Hubert, Lucas Levy, Anastasia Duchesne, and Danny Ba. Cahier de charges fonctionnelles — Escrow partie digitale (version 2.4). Technical report, Smartlink and SmartChain, 2021.

[92] Jeremy Martin, Lucas Levy, Danny Ba, and Charles Beyer. Technical specifications — blockchain digital Escrow (version 1.0). Technical report, Smartlink and SmartChain, 2021.

[93] Lorenz Breidenbach, Christian Cachin, Alex Coventry, Steve Ellis, Ari Juels, Andrew Miller, Brendan Magauran, Sergey Nazarov, Alexandru Topliceanu, Fan Zhang, Benedict Chan, Farinaz Koushanfar, Daniel Moroz, and Florian Trame`r. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks, 2021. https://research.chain. link/whitepaper-v2.pdf.

[94] F. Zhang, W. He, R. Cheng, J. Kos, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song. The Ekiden platform for confidentiality-preserving, trustworthy, and performant smart con- tracts. IEEE Security & Privacy, 18(3):17–27, 2020.

[95] David Mazières. The Stellar consensus protocol: a federated model for internet-level consensus, 2015. https://www.stellar.org/papers/ stellar-consensus-protocol.pdf (accessed february 2022).

[96] Dahlia Malkhi and Michael K. Reiter. Byzantine quorum systems. Distributed Computing, 11(4):203–213, 1998.

[97] Álvaro García-Pérez and Alexey Gotsman. Federated Byzantine quorum systems. In 22nd International Conference on Principles of Distributed Systems (OPODIS 2018), volume 125 of LIPIcs, pages 17:1–17:16. Schloss Dagstuhl, 2018. http://www.dagstuhl. de/dagpub/ 978-3-95977-098-9.

[98] Nicolas Barry, Giuliano Losa, David Mazières, Jed McCaleb, and Stanislas Polu. The Stellar consensus protocol (SCP). Internet-Draft draft-mazieres-dinrg-scp-05, 2018. https: //datatracker.ietf.org/doc/html/draft-mazieres-dinrg-scp-05.

[99] Álvaro García-Pérez and Alexey Gotsman. Federated Byzantine quorum systems (extended version). CoRR, abs/1811.03642, 2018. http:// arxiv.org/abs/1811.03642.

[100] David Mazières, Giuliano Losa, and Eli Gafni. Simplifed SCP, 2019. http://www. scs.stanford.edu/˜dm/blog/simplified-scp.html.

[101] Álvaro García-Pérez and Maria Anna Schett. Deconstructing Stellar consensus. In 23rd International Conference on Principles of Distributed Systems (OPODIS 2019), volume 153 of LIPIcs, pages 5:1–5:16. Schloss Dagstuhl, 2019. http://www.dagstuhl.de/ dagpub/ 978-3-95977-133-7.

[102] Álvaro García-Pérez and Maria Anna Schett. Deconstructing Stellar consensus.(extended version). CoRR, abs/1911.05145, 2019. http://arxiv.org/abs/1911.05145.

[96] The Architecture and Analytics Platforms team at CSIRO Data61. Blockchain patterns, 2020. https://research.csiro.au/blockchainpatterns/ (accessed febru- ary 2022).