Digital Finance
https://doi.org/10.1007/s42521-023-00094-w

ORIGINAL ARTICLE

Tokenizing assets with dividend payouts—a legally compliant and flexible design

Efim Zhitomirskiy[1] · **Stefan Schmid**[2] · **Martin Walther**[3]

Received: 9 June 2023 / Accepted: 23 August 2023

Abstract

The tokenization of financial assets using blockchain technology is a transformative process that allows for the fractionalization of ownership, thereby creating more accessible investment opportunities compared to traditional financial assets. Recent research has shown that token offerings are subject to moral hazard and fraud. In response to these challenges, we propose a novel token design that is compliant with the legal framework of Switzerland. Our design is characterized by its flexibility and can represent any yield or dividend-bearing asset, such as stocks, bonds, or rental income from real estate. Further enhancing its compatibility, the token conforms to the Ethereum ERC-20 standard, enabling seamless integration with existing decentralized finance solutions. Another contribution of our token design is its innovative approach to dividend distribution. Unlike traditional models that distribute dividends based on ownership at the time of payment, our token design distributes dividends based on holding times. This distinctive approach promotes smoother asset prices between dividend payouts by eliminating the need for compensation payments. Our token prototype represents a potential starting point for future research on leveraging the opportunities of decentralized finance.

Keywords Blockchain · Crowdsourcing · Dividend distribution · Decentralized finance · Security token · Tokenization

JEL Classification G18 · G23 · G32 · K22 · M13 · O33

✉ Martin Walther
martin.walther@tu-berlin.de

Efim Zhitomirskiy
efim.zhtm@gmail.com

[1] Technische Universität Berlin, Berlin, Germany

[2] Chair of Intelligent Networks, Technische Universität Berlin, Einsteinufer 17, Berlin, Germany

[3] Chair of Finance and Investment, Technische Universität Berlin, Sec. H 64, Straße des 17. Juni 135, 10623 Berlin, Germany

Published online: 31 August 2023

1 Introduction

Fundamentally, tokenization is the process of converting rights or a unit of asset ownership into a digital token on a blockchain, a cryptographically secured distributed ledger. These digital tokens can be bought and sold on a blockchain-based platform, similar to how traditional securities are traded on a stock exchange. The on-chain representation of income rights from ventures enables the use of smart contracts, which can reduce the cost of financial intermediation. Furthermore, the blockchain's immutable and transparent nature offers the potential for increased trust and security. However, anonymity also poses the risk of moral hazard and fraud (Gryglewicz et al., 2021; Hornuf et al., 2022; Momtaz, 2021a). Therefore, it is crucial to consider investor protection when implementing financing over the blockchain.

In our study, we establish the necessary requirements for the tokenization of financial assets guided by the latest regulation for digital assets on distributed ledger technology. We suggest a legally compliant and flexible digital asset architecture. Our token design can represent any yield or dividend-bearing token, such as stocks, bonds, or rental income from real estate, and features an innovative dividend distribution approach. Furthermore, it is compatible with the Ethereum ERC-20 standard, allowing the use of existing smart contracts for wallets and secondary markets.

A main challenge for constructing a compliant digital asset is identity management. This is due to the pseudo-anonymous nature of the blockchain and the fact that regulations forbid unidentified ownership of securities. Furthermore, on-chain application development requires specific algorithmic approaches due to the nature of blockchains in general and the Ethereum Virtual Machine (EVM) specifically. At the core of this study, we propose a dividend-bearing security token standard. Our prototype implementation shows that it is possible to represent yield bearing assets on-chain in accordance with international security trading laws. We optimize gas consumption and floating-point management to ensure the correctness and executability of the smart contract.

The price of a dividend-bearing asset typically depends on the time until the next dividend payout, as the entire dividend is paid to the owner of the asset at the due date. This is reflected in the secondary market price, which includes compensation for an early exit (Black, 1976). In our study, we propose a novel approach to dividend distribution calculation that smoothens the asset valuation in between payouts. Specifically, in our approach, a holder's reward is available for redemption after a dividend payout and depends on holding time instead of ownership at the time of dividend payout. This way, virtually no compensation, i.e., price adjustment, is needed when selling an asset before dividend payout. Furthermore, for bonds, a distinction between dirty and clean price is no longer necessary. Please note that our token also allows for dividend distribution based on ownership at the time of payout, which means that it can represent conventional and standard financial securities.

Overall, our study contributes to the literature on applications of the blockchain in finance by presenting a design and prototype realization that includes

several implementations of financial and legal aspects. Most importantly, it complements the literature on token offerings by addressing the need for practical solutions to the problem of token offerings bypassing financial regulation that has been identified and highlighted by numerous studies (e.g., Momtaz, 2021a). Specifically, we extend the ERC-20 token to include KYC compliance checks, administrative controls, and dividend distribution. To ensure reproducibility and as an additional contribution to the research community, we will make our code available.

The remainder of this study is structured as follows. Section 2 explains the background on token offerings and the legal framework. In Sect. 3, we derive the technical requirements and describe our design. In Sect. 4, we explain the prototype. Section 5 contains a discussion of benefits and challenges. Section 6 concludes.

2 Background

In this section, we present the idea behind digital ownership and review the literature on token offerings and the legal framework of digital assets.

2.1 Digital ownership

The digital representation of assets on the blockchain offers numerous potential benefits. The blockchain can serve as an immutable and transparent source of truth, requiring less trust in the platform itself as ownership data are recorded on the distributed ledger and the platform acts as an intermediary (Gupta et al., 2020). Furthermore, the blockchain enables cross-platform compatibility and more vibrant secondary markets for crowdfunders (Smith et al., 2019), compared to conventional crowdfunding.

Crowdfunding via the blockchain can have several advantages over conventional crowdfunding systems: The audit process is improved as the blockchain acts as an immutable data source and smart contracts as immutable computation logic (Rozario & Thomas, 2019). What was correct from the beginning either cannot be changed or changes transparently. The process of distributing dividends and making payouts is, therefore, improved due to the nature of the blockchain. Every behavior is recorded and requires different access control protocols. This reduces the risk of management mistakes. Tokenization opens new ways of gaining liquidity via a broader spectrum of investors not limited by the contract of the specific platform but compliant with common industry standards of identity management (European Insurance & Occupational Pensions Authority, 2021).

Using distributed ledger technology (DLT) can simplify the process of financing a venture and distributing dividends to investors, as well as ensure a fair and transparent process for all parties. In particular, small investors who do not have the resources for expensive legal actions can benefit from the equal distribution of cash flows enforced by smart contracts. Smart contracts offer the possibility to make payments from financial assets more comprehensible and avoid

compensation payments due to later dividend or interest payments. Our prototype offers an implementation of such an innovative dividend distribution.

Regarding the legal framework, (Swiss) regulators already consider digital ownership as equivalent to physical ownership (State Secretariat for International Finance SIF, 2020). Therefore, digital ownership implies a liability of entrepreneurs and legally enforceable investor rights. However, due to the anonymity of cryptocurrencies, the enforcement of these rights can be difficult. Our token prototype offers solutions that mitigate this problem.

One potential application of digital tokenization is the real estate sector that Baum (2021) investigates. According to him, tokenization is at a very early stage and should focus on assets with an existing and proven demand for fractionalization. With respect to real estate, these include funds, which have an established structure and an expressed demand for fractionalization, and debt contracts that are standardized and have already been fractionalized in the form of mortgage-backed securities. Furthermore, digital tokenization can only be successful when market participants are comfortable with blockchain technology. The token design we propose in this study is flexible and can be used to model existing financial instruments, such as funds or debt contracts. It is, therefore, likely to be suitable for the tokenization of real estate asset ownership. Furthermore, it improves investor protection and can, thus, contribute to strengthen market participants' confidence in the blockchain.

Markheim and Berentsen (2021) discuss theoretical benefits of tokenizing real estate assets. Using a practical example, they show that some of these theoretical advantages are not yet realized. They identify uncertainties regarding the regulation of tokens as cause, underlining the importance of considering the legal framework of tokenization.

Swinkels (2023) considers a sample of 58 real estate tokens in the USA. He finds that a token has on average 254 owners, which shows that tokenization can improve risk sharing across households. Furthermore, investors with investments exceeding USD 5000 hold well-diversified portfolios, which indicates that they are sophisticated.

Kreppmeier et al. (2023) provide first empirical evidence on real estate tokenization by analyzing a data set on 173 real estate tokens in the USA with more than 200,000 blockchain transactions. They find that the ownership of properties is not concentrated on a small number of small investors, which confirms that tokenization can provide broad access to real estate for many small investors. However, on average, investors only hold ten different tokens and more than a quarter of all considered investors have invested in only one token. This shows that investors are not yet well diversified. Furthermore, the secondary market that enables liquidity only plays a minor role. This emphasizes the need for technical innovation, to which our study contributes. In addition, Kreppmeier et al. (2023) find that the specifics of the crypto market play a central role in the success of STOs and capital flows. This indicates that investors tend to follow trends instead of fundamentals and highlights the relevance of consumer protection, which our token design addresses.

2.2 Token offerings

Token offerings, in the literature often referred to as Initial Coin Offerings (ICOs), are an innovative fundraising mechanism (Fisch, 2019). While the approach is similar to crowdfunding, a key difference is the use of smart contracts on distributed ledger technology (DLT), i.e., the blockchain, to create and sell tokens (Block et al., 2021). Tokens can either provide utility (utility tokens), such as the right to use a product or service of a venture or resemble a security (security tokens). Block et al. (2021) refer to ICOs that use the latter as security token offerings (STOs). However, Lambert et al. (2022) argue that STOs are not a subset of ICOs. They require STOs to fall under the regulation of securities laws and define a security token as "a digital representation of an investment product, recorded on a distributed ledger, subject to regulation under securities laws".

Due to substantial growth and capital raised, token offerings are discussed intensively in the literature. Theoretical studies investigate token offerings in comparison to traditional forms of financing, such as equity or venture capital. Potential benefits of token offerings include cost reduction as a result of the elimination of financial intermediaries, and network effects (Li & Mann, 2018; Shakhnov & Zaccaria, 2020), while moral hazard is a potential disadvantage (Chod & Lyandres, 2021; Gryglewicz et al., 2021; Malinova & Park, 2018).

Empirical studies focus on the determinants of ICO success (e.g., Fisch, 2019; Masiak et al., 2020), subsequent short-term and long-term performance (Benedetti & Kostovetsky, 2021; Fisch & Momtaz, 2020; Lyandres et al., 2019, 2022; Momtaz, 2020, 2021b), characteristics and motives of investors (Fahlenbrach & Frattaroli, 2021; Fisch et al., 2021), determinants of token liquidity (Howell et al., 2020), or regulatory and geographical aspects (Cohney et al., 2019; Huang et al., 2020).

Despite the different focuses, most studies identify a lack of legal protection of investors due to ICOs bypassing financial regulation (Adhami et al., 2018) as a limitation of token offerings. The possibilities and extent of scam and fraud are discussed, among others, in Chohan (2019), Liebau and Scheuffel (2019), and Hornuf et al. (2022). Importantly, Momtaz (2021a) shows that the absence of functioning institutions that verify signals ex ante or punish false signals ex post leads to a systematic exaggeration of information in ICO-disclosure. Investors notice this bias only when trading with other investors, which leads to disappointment, a depreciation of the cryptocurrency and an increase in the probability of platform failure. Therefore, there is a pressing need for practical studies like ours that investigate research questions such as "what regulatory standards, platform governance, and token exchange policies could promote healthy token market development" (Momtaz, 2021a). A main contribution of our study is that our design addresses the problem of pseudo-anonymity by making asset ownership traceable and corporate management liable. In this way, as called for by Momtaz (2021a), we introduce a way to punish the management or insider investors for sending false signals. This mitigates false incentives to exaggerate the company's prospects for success or fraud schemes such as exit scams, in which startups pretend to be an attractive and sustainable investment, only to use the acquired funds for private benefits and abandon the startup.

2.3 Legal framework

The legal aspect of creating digital assets represents a major challenge to realizing a legally compliant on-chain security. In this section, we analyze the findings from related studies to define the regulatory requirements and technical possibilities for tokenization. Smith et al. (2019) conclude that the tokenization of tangible and intangible assets is regulated by the securities law, as the transactions of such tokens satisfy the characteristics of the Howey test: "(1) The Investment of Money, (2) Common Enterprise, (3) Reasonable Expectation of Profits, (4) Derived from Efforts of Others". It follows that the exchange of tokens must adhere to essential compliance regulations such as Know-Your-Customer (KYC) and Anti-Money Laundering (AML), to stop financial crimes. One potential solution for the KYC restrictions on the trading of such tokens is an on-chain identity management implementation (Parra Moyano & Ross, 2017). In this model, KYC entities would issue certificates of truth authorization as non-fungible tokens (NFT) and bind them immutably to a wallet (Weyl et al., 2022). This allows the wallet owner to authorize themselves as KYC individual without going through the KYC process for each account creation on the new platform. The certifiers can also revoke the certificate to control compliance with internal and external standards. Smart contract implementation of KYC verification would enable the possibility of an architecturally compliant market. One of the approaches that were proposed by tokeny.com[1] includes a complex architecture of implementing an on-chain registry such that every transfer calls a validator function that allows or declines the action. A market kept compliant by code would allow for more flexibility and accessibility in the trading of these assets.

To ensure the token holder's rights are protected by the regulator in case of violation, there should be a solid legal basis for such financial contracts. The holding company, usually a special purpose vehicle (SPV), acts as a legal shell for the packaged asset and issues shares that represent the financial claim with the asset as collateral. Switzerland recognizes the possession of tokens as equivalent to the possession of shares of the company, thus establishing a legal framework for storing specific financial rights on the blockchain (State Secretariat for International Finance SIF, 2020). These rights include the dividend distribution and liquidation penalty payout in case of bankruptcy.

Figure 1 illustrates the structure of financing via tokenization. First, the operating company transfers the asset to the holding company, an SPV. Then the SPV issues and sells shares to investors that are represented by a token. This form of digital ownership is considered equivalent to physical ownership by Switzerland, thus allowing for a regulatory protection of investors. Our prototype offers such a compliant architecture. When the asset yields a dividend, all investors that hold the token are eligible for a proportional reward that is distributed via the smart contract.

Our study considers Switzerland, a country in which a considerable number of ICOs and STOs have been conducted. Specifically, according to Bellavitis et al. (2021), Switzerland is one of seven countries that account for more than half of the

[1] See https://github.com/TokenySolutions/T-REX (accessed June 2, 2023).

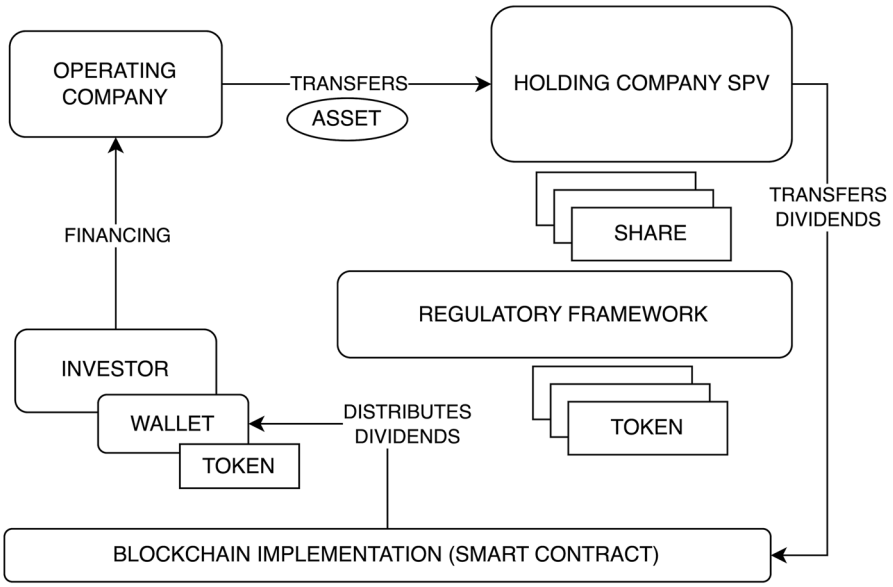

Fig. 1 Structure of financing via tokenization. First, the asset is transferred to a holding company, an SPV. The latter issues shares, which are represented by a token. When the asset yields a dividend, investors who own the token receive a proportionate payment that is distributed via a smart contract

ICO activity between 2015 and the first half of 2020. Furthermore, Lambert et al. (2022) note that Switzerland attracts a large number of STOs. The fact that Switzerland was one of the earliest countries to regulate cryptocurrencies and that the Federal Council announced that it "wishes to exploit the opportunities offered by digitalisation for Switzerland" and "create the best possible framework conditions so that Switzerland can establish itself and evolve as a leading, innovative and sustainable location for fintech and blockchain companies" (Federal Council, 2018) make Switzerland an interesting target for our study.

The State Secretariat for International Finance SIF (SIF) sets the following special requirements:

1. Joint management: According to the "Bundesgesetz" Art. 973d 2 2, the tokenized shares of the holding company have to be controlled by several independent participants via a joint management. A possible solution could be an admin multisignature wallet or some form of decentralized autonomous organization (DAO) with distributed intervention capabilities in the smart contract logic.
2. Metadata: Another requirement of SIF is the metadata availability and viewability without a third party according to Art. 973d 2 3 and 973d 2 4:
   - "The content of the rights, the functioning of the ledger, and the registration agreement are recorded in the ledger or in linked accompanying data.
   - Creditors can view relevant information and ledger entries and check the integrity of the ledger contents relating to themselves without intervention by

a third party." This requires the issuer of the smart contract to provide the necessary linked company data either in an external link or in special variables to be stored directly on-chain. The specific implementation depends on the particular regulator and does not entail technological difficulties. Our implementation is compatible with the ERC-20[2] standard. This means that investors can use open-source wallets to have full control over assets without intervention by a third party.

3. Forced transfer: One of the most important problems that investors face in tokenized assets is self-custody. Therefore, in Art. 973 h, the regulator requires the possibility to cancel the security for investors in case of losing access to the wallet and issue replacement. This requirement is implemented and does not correspond to any technological difficulty.

   Besides the discussed requirements, any stock trading requires centralized management. This includes specific admin privileges that also need to be addressed and implemented in the design and prototype.
4. Freezing of transfers and withdrawals: In the stock market, it is common for the trading of a particular stock to be halted or frozen before the release of important announcements. This is done to prevent any kind of insider trading or manipulation of the stock's price that could occur as a result of the announcement. The freeze is typically put in place by the exchange where the stock is traded, or by the regulatory body overseeing the market. In the context of the tokenized assets, it is possible to freeze the asset on the contract level.
5. Blocklisting: In the stock market, a trader can be blocklisted by a stock exchange or regulatory body if they engage in illegal or unethical trading practices.

   An additional potential advantage of financing via tokenization is the possibility to implement voting rights. In traditional crowdfunding, these are usually limited (Rossi et al., 2019). On the blockchain, by interacting with the external smart contract, investors could vote on specific management decisions and influence the SPV behavior by allocating funds for specific purposes declared in the voting proposals (Mosley et al., 2022). However, for the sake of simplicity, and as voting rights are not a requirement for compliance, we do not include voting rights into our design and prototype.

3 Technical requirements and design

In this section, we derive the necessary requirements from the current regulation and propose a digital asset design. The requirements include on-chain KYC management and operator privileged protocols. Furthermore, the implementation of a dividend distribution logic is necessary.

The first key requirement is that the issuer of the tokens must store the data in the smart contract in such a way that it can be viewed by the holders without a

[2] See Smith et al. (2023).

third party. To achieve this, all relevant information has to be stored in the contract variables.

The second key requirement is a KYC compliant identity management. KYC can be achieved with the help of external certificate providers. In our approach, the admin of the smart contract is responsible for defining the set of KYC certificate providers that will be used for the verification process. Initially, this set may only include the admin. However, any trusted KYC certificate provider can be added. This increases the number of potential investors to all investors that are verified by the added KYC certificate provider with a single transaction. To ensure compliance with the regulatory requirements, any transfer of tokens can only be successful if both the sender's and recipient's wallets have been certified by a KYC provider from the set defined by the admin and have not been included in any of the blocklist contracts. The integration of the verification logic in the code of our token makes it auto-compliant. Our prototype's design is inspired by the operating Binance Account Bound (BAB) token, which is a special contract on the Binance Smart Chain that certifies that a given wallet was verified by Binance.[3] Binance, a prominent exchange, adheres to stringent AML and KYC regulations in verifying the identity of its clients. This verification process extends to the issuance of a certificate of verification for a user's chosen wallet, linking it to a certification contract on the Ethereum Virtual Machine (EVM) network. The KYC contract, residing on the blockchain, encapsulates a set of rules governed by a specialized operator, in this case, Binance, who manages these certificates. Traditional KYC operators, upon verifying a user, furnish a "proof" to the requesting financial entity, enabling the linkage of the user's digital identity with their physical persona. Binance has innovated upon this approach by materializing the "proof" as a blockchain-resident token, known as the BAB token. This token, a special contract on the Binance Smart Chain, certifies that a given wallet has been verified by Binance. It represents a non-transferable digital verification tool, minted after a series of steps including identity verification, wallet connection, wallet ownership verification, and payment of associated gas fees. This method not only enhances the robustness of identity verification but also integrates seamlessly with the blockchain's decentralized architecture, reflecting a novel convergence of regulatory compliance and technological innovation.

The third key requirement is an adequate cost of operating the system. Each transaction on the Ethereum Virtual Machine induces a cost that is paid in the cryptocurrency Ether. The cost depends on the total amount of computations in that particular transaction. The total amount of computations of a single transaction is limited by the so-called block gas limit,[4] which has to be considered when designing the functions. Gupta et al. (2020) propose a naive approach to distributing dividend rewards to token holders by iterating over all holders in a single transaction initiated by the admin/operator. This approach is not viable due to the limitations of the system since the gas consumption of the transaction depends on the number of holders. If

[3] See https://bscscan.com/address/0x2b09d47d550061f995a3b5c6f0fd58005215d7c8#code (accessed June 2, 2023).

[4] See https://Ethereum.org/en/developers/docs/gas/ (accessed June 2, 2023).

the token represents a small portion of the underlying asset, the potential maximum number of holders could become very large, causing the transaction to run out of gas and not be executed.

We propose a pull-based approach that reduces the use of loops. By enforcing the calculation of the reward at the time of the user-initiated payout, we only have to iterate over a small number of KYC certificate providers and not a large number of individuals. In our design, we propose that the holder pays the transaction fees associated with the redemption. Our approach allows holders to retrieve their rewards at their convenience, while also incentivizing them to avoid unnecessary computations. This may reduce total gas consumption. The main benefit of our approach is that outsourcing the calculations to holders avoids a large number of computations by the operator of the contract, which could exceed the block gas limit, and ultimately lead to the dividend distribution not being executable.

Our proposed approach makes some essential extensions to the ERC-20 token contract. These include integrating KYC compliance checks for token holders, administrative controls, and a system for dividend distribution. Administrators will have the ability to halt the activity of token holders, add or remove holders from blocklists and allowlists, and modify the signing address of the account. This last feature allows for a change of ownership if required by regulatory authorities. Every interaction a holder has with the contract will be verified according to the rules set by the administrator.

Our solution features dividend distribution based on holding times. Traditional bonds and stocks exhibit increasing prices until the dividend is paid, and a price drop right after the payout (Black, 1976). This is due to the fact that the entire dividend is paid to the investors who hold the assets at the time of the payout. Dividend distribution based on holding times has the potential to change how financial assets are valued between dividend payouts. In our design and prototype, distributing dividends proportionately according to holding times eliminates the need for compensation payments (except for small payments to account for compound interest), which in the case of uncertain dividends of stocks would include risk premiums. Furthermore, it is not necessary for bonds to have two prices, a dirty price that includes the prorated yield and a clean price that excludes accrued interest between coupon payments. This increases transparency and prevents misunderstandings, especially for smaller and unsophisticated investors.

Our dividend distribution system takes into account the unique characteristics of the blockchain. It minimizes the computational load for each transaction by integrating a loop-free implementation for both dividend distribution (on the admin side) and dividend calculation (on the holder side).

4 Prototype

In this section, we present a prototype using Solidity and Ganache. It is a proof-of-concept for our proposed design that demonstrates the feasibility of our concept. The prototype enables us to estimate the associated gas costs and performance of our token in a realistic setup and facilitates further research.

Solidity[5] is a statically typed programming language designed for developing smart contracts that run on the Ethereum Virtual Machine. The Solidity code is compiled to byte-code, deployed on-chain and gets a unique address that everyone on the network can interact with. Ganache[6] is a personal blockchain emulation for the Ethereum Virtual Machine. It allows us to get real indicators of the resource intensity of the algorithm and estimate the cost of transactions.

Recall that a key feature of our design is the dividend distribution based on holding times. As suggested by Estevam et al. (2021), we measure time in block numbers, as nodes tolerate tens of seconds of deviation. The reward depends on the weighted amount of the holder's share for each block, which is calculated as the ratio of the holder's balance to the total supply. Therefore, we define the reward of user w for period p as:

$$R_p^w = \frac{\text{total Payout}_p}{bln_p - bln_{p-1}} \cdot \sum_{b=bln_{p-1}}^{bln_p} \frac{\text{balance}_b^w}{\text{total Supply}_b}, \tag{1}$$

where total Payout_p is the total dividend payout for a particular period p, bln_p is the block number of the end of period p, total Supply_b is the total circulated amount of tokens at the block$b$, and balance_b^w is the balance of the particular holder w at block$b$. A naive approach is an implementation similar to the MiniMi-token[7] that stores the transaction history of all users in the form of a Snapshot array by recording the balance of the user for a particular block number any time the balance changes. This array is used to calculate the reward for each holder after a dividend payout takes place and to reconstruct holders' weighted share of the dividend payout in an iterative, and therefore inefficient, manner. As the Ethereum block gas limit is set to a fixed value and the computational requirements grow linearly with the increase in iterations, frequent traders could reach the cap and consequently lose the ability to withdraw. Performance measurements derived from our prototype implementation demonstrate that dozens of trades per day could block the withdrawal functionality already within a couple of months, while hundreds of transactions per day might block the contract even within a month. This observation demonstrates that a significant level of activity exerted by the holder can lead to the functional disruption of the smart contract. Furthermore, the immutable nature of the system does not allow for a manual recovery. Therefore, this simple design architecture is not viable.

In our approach, we spread the calculations over all balance change interactions, store running state variables, and avoid the use of loops as described by Batog et al. (2020). Our algorithm is pull-based and postpones the calculations of running reward variables to the point of user interaction. Our reward distribution approach features constant gas consumption for the user, and therefore avoids exceeding the block gas limit.

[5] See https://soliditylang.org/ (accessed June 2, 2023).

[6] See https://trufflesuite.com/docs/ganache/ (accessed June 2, 2023).

[7] The code is available at https://github.com/Giveth/minime (accessed June 2, 2023).

Every balance change interaction with the contract forces an update function that changes the running variables. The dividend reward is recalculated and saved in the dividend balance of the account. The dividend distribution mechanism depends on the total supply for a given period and restricts the change of total supply within a period. Thus, total supply can be moved out of the sum. The reward R for the particular holder w in the period p is defined as:

$$R_p^w = \frac{\text{total Payout}_p}{(bln_p - bln_{p-1}) \cdot \text{total Supply}_p} \cdot \sum_{b=bln_{p-1}}^{bln_p} \text{balances}_b^w. \tag{2}$$

Since the division results in a remainder that must be stored as an undistributed dividend, we should perform this operation when the dividend is paid and only multiply or summarize when the respective user calculates the reward. The sum of a user's balances over all block numbers for the current period is stored in the running cumulative balance (CB):

$$\text{CB}_p^w = \sum_{b=bln_{p-1}}^{bln_p} \text{balances}_b^w. \tag{3}$$

The algorithm stores the cumulative dividend per token for each period to resolve the weighted portion of the reward for the holder by multiplying the respective dividend per token per block with holder's cumulative balance. Since the EVM only allows integer operations, this has an effect on division calculations. We manually integrate floating-point control into the algorithm to track the remainder of the division by storing the value of non-distributed funds, *restDiv*. It is summed up until the next dividend payout period as follows:

$$\text{dividend Per Token Per Block}_P = DpTpB_p = \left\lfloor \frac{\text{total Payout}_p + restDiv_{p-1}}{\text{total Supply}_p \cdot \Delta_p} \right\rfloor, \tag{4}$$

where $\Delta_p = bln_p - bln_{p-1}$ stands for the length of the period p and the remainder is $restDiv_p = (\text{total Payout}_p + restDiv_{p-1}) \mod (\text{total Supply}_p \cdot \Delta_p))$.

Subsequently, we can reconstruct the dividend per token as follows:

$$\text{cumulative Dividen Per Token}_P = DpT_P = \sum_{p=1}^{P} DpTpB_p \cdot \Delta_p. \tag{5}$$

Finally, the reward for the holder for a particular period is calculated without division as follows:

$$R_p^w = CB_p^w \cdot DpTpB_p. \tag{6}$$

If a holder accrues dividends from multiple periods before withdrawing, the reward is calculated without iteration as follows:

$$R^{w}_{\{p_n;p_m\}} = \text{balance}^{w}_{p_n} \cdot \left(DpT_{p_m} - DpT_{p_n}\right). \tag{7}$$

Overall, our design and prototype offer a possibility to represent yield bearing assets as a token that is compliant to the regulatory requirements of Switzerland's legal framework. In particular, we cover centralized control over investors' activity, the dividend distribution process, on-chain verification, and KYC compliance based on the industry standard of ERC-20-Tokens. Our prototype, hence, realizes the innovative reward distribution concept from our design and eliminates the need for compensation payments, and thus contributes to smoother prices. Furthermore, our implementation of distributing dividends ensures that the block gas limit cannot be exceeded and reduces gas consumption per transfer by 25% compared to the naive strategy. The additional functionalities and compliance checks in our prototype are associated with a reasonable additional cost: Transfers are no more than three times the cost of the standard ERC-20 implementation.

5 Discussion

In this section, we discuss the benefits of our approach as well as the remaining challenges and opportunities.

5.1 Benefits

First, our design and prototype are compliant with the regulatory framework of Switzerland, which means that investor security is improved, and the probability of fraud is reduced. This is particularly relevant, as recent research has shown that bypassing regulation is one of the major weaknesses of ICOs. Most importantly, our design introduces possibilities to punish corporate management or insiders for unethical behavior by making them legally liable. This reduces incentives for moral hazard and can contribute to investors' confidence in blockchain technology.

Our study focuses on the specific requirements of Switzerland's jurisdiction. However, the foundational principles are grounded in international law on financial assets, particularly in the stipulation that financial assets cannot be held by anonymous parties. Our design covers the pseudo-anonymity problem that is crucial for security trading in most jurisdictions and due to its flexibility can be adjusted to meet the specific requirements of other legal frameworks.

Second, our approach enables trading on a secondary market that is not limited to a single platform, such as a crowdfunding platform, but is accessible by any member of the blockchain community that is certified by any trusted certificate provider. This increases the amount of potential trading partners, and therefore liquidity.

Third, our implementation of distributing dividends is pull-based and solves the problem that the block gas limit can be exceeded. Furthermore, our innovative dividend distribution leverages the opportunities that tokenization offers by distributing dividends based on holding times, rather than ownership at the end of the period. This eliminates the need for compensation payments and leads to smoother prices.

Overall, increased investor protection, i.e., reduced risk, increased liquidity, and a distribution of dividends that does not require additional compensation payments may increase investors' willingness to participate in token offerings. This can facilitate financing via tokenization. Therefore, our design and prototype can benefit investors as well as entrepreneurs and ventures. Furthermore, our prototype shows that legal requirements can be met at a reasonable cost, as the gas cost of interacting with the contract is at most three times higher than in the standard ERC-20 implementation.

5.2 Challenges for future adoptions

In our design and implementation, dividends that are not redeemed stay in the pool of the smart contract. This guarantees that the dividend can be paid out to the asset holder at any time. However, when holders do not redeem their dividend claims, these are not invested, and therefore do not yield a return. In future adoptions, lending protocols, such as "Aave",[8] could be integrated into our token to realize a return on the funds in the smart contract's pool.

One limitation of our implementation of financing via tokenization is that the returns of small investors are more affected by the fixed transaction costs. In our approach, investors have to pay the gas cost of redeeming a reward, i.e., claiming their dividend payment. This transaction cost does not depend on the withdrawal amount, but only on the amount and current price of computations. It implies that the (net) realized return of investors will always be less than the nominal return. For example, assuming a 5% dividend yield and once-a-year withdrawal, investors who do not want to lose more than 10% of the dividend on fees would require a minimum asset value of 200 times the fee value. With the current gas cost of 48 gwei,[9] about 100,000 gas needed for one withdrawal, and a current Ether price of 1,858 USD, claiming a dividend would cost about 9 USD. Therefore, the minimum investment amount would be about 1800 USD. These requirements regarding minimum investment amounts may limit the opportunities of small investors to benefit from token offerings, and thus hinder the democratization of finance. Theoretically, the transaction costs could be reduced by an order of magnitude[10] if the contract was deployed on layer2 (Arbitrum one[11]) or the side chain (Binance Smart Chain[12]). However, it is not trivial to exchange information between blockchain networks. Therefore, outsourcing complicated computations is not a viable option (Kalodner et al., 2018).

Our prototype implementation only covers the representation of digital ownership as a token and does not include the token offering or the secondary market.

[8] See https://app.aave.com/markets/ (accessed June 8, 2023).

[9] See https://etherscan.io/tx/0x2c2e3019d3aaf6284a6a2af4bd30eae917b3a5374b05497725b65d86e780640e (accessed May 31, 2023).

[10] See https://dune.com/queries/1168730/1998286 (accessed June 2, 2023).

[11] See Kalodner et al. (2018).

[12] See https://www.bnbchain.org/en/smartChain (accessed June 2, 2023).

However, our token is ERC-20 compatible. This means that existing smart contracts can be used to conduct STOs and enable secondary markets.

The recent crypto disaster has shown that custodial markets, such as FTX, can collapse (Wilson, 2022). Therefore, the creation of non-custodial secondary markets is particularly relevant. Due to its limitations of transaction speed and high costs of the DLT, the blockchain technology does not feature an efficient centralized limit order book (CLOB) implementation. However, two interesting market maker solutions are available.

Automated market maker: Existing smart contracts that are called liquidity pools (LP) are a possibility to implement a decentralized secondary market (Loesch et al., 2021). An LP contains tokens and an amount of a currency, e.g., Ether. The price of a token is determined by the ratio of tokens to Ether in the pool. Investors can buy or sell a token by swapping a token against the current price in the liquidity pool, which changes the balance of tokens and Ether, and leads to a new price. As our token is yield bearing, using LPs would require an additional non-trivial logic for distributing dividend rewards among liquidity providers. Therefore, the standard architecture would have to be adjusted, to reward the liquidity providers not only with the fees from exchanging on the particular LP but also with the rewards coming from the dividend-bearing asset.

Non-custodial centralized limit order book: The non-custodial CLOB features a centralized off-chain matching and an on-chain execution protocol that is implemented by platforms such as 1 inch.io.[13] It is non-custodial because the token stays in the users' wallets while the market maker platform matches the orders. Therefore, this approach could be used with our token without the need for additional adjustments to the non-custodial CLOB architecture.

Overall, our study suggests three interesting avenues for future research. First, creating the possibility of a (safe) interest on funds in the smart contract could reduce the costs for holders and increase the flexibility in the design of tokens. Second, the fixed transaction costs that are particularly relevant for smaller investors should be investigated to facilitate the democratization of finance. Third, token offerings and secondary markets could be optimized to maximize liquidity, security, and transparency to leverage the opportunities of decentralized finance that DLT offers.

6 Conclusion

Recent research on token offerings has identified moral hazard and fraud as a major challenge of financing via the blockchain. In this study, we contribute to solutions for this challenge by developing a legally compliant token design. Our prototype is flexible as it can represent any yield or dividend-bearing asset. It is ERC-20 compatible and can, therefore, be integrated in existing decentralized finance solutions. The approach to distributing dividends is innovative as it is based on holding times rather than ownership at the time of dividend payment. This leads to smoother asset

[13] See https://docs.1inch.io/docs/limit-order-protocol/introduction (accessed June 2, 2023).

prices between dividend payouts. These enhancements may increase investors' willingness to participate in token offerings, benefiting both investors and companies.

Author contributions EZ was a major contributor to the conceptualization of the study, the literature review and technical research, the design and implementation of the prototype, and wrote a first draft of the manuscript. SS majorly contributed to the token design and implementation of the prototype, the organization of the manuscript, and supervised the project, especially regarding the technical aspects. MW made significant contributions to the conceptualization, the literature review, and the final draft of the manuscript. Furthermore, he supervised the project, especially regarding the financial aspects. All authors reviewed the final manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL.

Declarations

Conflict of interest The authors report there are no competing interests to declare.

References

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business, 100*, 64–75. https://doi.org/10.1016/j.jeconbus.2018.04.001

Batog, B., Boca, L., & Johnson, N. (2020). Scalable reward distribution on the ethereum blockchain. Working paper. http://batog.info/papers/scalable-reward-distribution.pdf. Accessed 12 August 2023.

Baum, A. (2021). Tokenization—The future of real estate investment? *The Journal of Portfolio Management, 47*(10), 41–61. https://doi.org/10.3905/jpm.2021.1.260

Bellavitis, C., Fisch, C., & Wiklund, J. (2021). A comprehensive review of the global development of initial coin offerings (ICOs) and their regulation. *Journal of Business Venturing Insights, 15*, e00213. https://doi.org/10.1016/j.jbvi.2020.e00213

Benedetti, H., & Kostovetsky, L. (2021). Digital tulips? Returns to investors in initial coin offerings. *Journal of Corporate Finance, 66*, 101786. https://doi.org/10.1016/j.jcorpfin.2020.101786

Black, F. (1976). The dividend puzzle. *The Journal of Portfolio Management, 2*(2), 5–8. https://doi.org/10.3905/jpm.1976.408558

Block, J. H., Groh, A., Hornuf, L., Vanacker, T., & Vismara, S. (2021). The entrepreneurial finance markets of the future: A comparison of crowdfunding and initial coin offerings. *Small Business Economics, 57*(2), 865–882. https://doi.org/10.1007/s11187-020-00330-2

Chod, J., & Lyandres, E. (2021). A theory of ICOs: Diversification, agency, and information asymmetry. *Management Science, 67*(10), 5969–5989. https://doi.org/10.1287/mnsc.2020.3754

Chohan, U. W. (2019). Initial coin offerings (ICOs): Risks, regulation, and accountability. *Cryptofinance and mechanisms of exchange* (pp. 165–177). Springer.

Cohney, S., Hoffman, D., Sklaroff, J., & Wishnick, D. (2019). Coin-operated capitalism. *Columbia Law Review, 119*(3), 591–676.

Estevam, G., Palma, L. M., Silva, L. R., Martina, J. E., & Vigil, M. (2021). Accurate and decentralized timestamping using smart contracts on the Ethereum blockchain. *Information Processing & Management, 58*(3), 102471. https://doi.org/10.1016/j.ipm.2020.102471

European Insurance and Occupational Pensions Authority. (2021). Discussion paper on blockchain and smart contracts in insurance. *Publications Office of the European Union*. https://doi.org/10.2854/136043

Fahlenbrach, R., & Frattaroli, M. (2021). ICO investors. *Financial Markets and Portfolio Management, 35*(1), 1–59. https://doi.org/10.1007/s11408-020-00366-0

Federal Council. (2018). Federal Council wants to further improve framework conditions for blockchain/DLT. https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73398.html. Accessed 5 June 2023.

Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of Business Venturing, 34*(1), 1–22. https://doi.org/10.1016/j.jbusvent.2018.09.007

Fisch, C., Masiak, C., Vismara, S., & Block, J. (2021). Motives and profiles of ICO investors. *Journal of Business Research, 125*, 564–576. https://doi.org/10.1016/j.jbusres.2019.07.036

Fisch, C., & Momtaz, P. P. (2020). Institutional investors and post-ICO performance: an empirical analysis of investor returns in initial coin offerings (ICOs). *Journal of Corporate Finance, 64*, 101679. https://doi.org/10.1016/j.jcorpfin.2020.101679

Gryglewicz, S., Mayer, S., & Morellec, E. (2021). Optimal financing with tokens. *Journal of Financial Economics, 142*(3), 1038–1067. https://doi.org/10.1016/j.jfineco.2021.05.004

Gupta, A., Rathod, J., Patel, D., Bothra, J., Shanbhag, S., & Bhalerao, T., et al. (2020). Tokenization of real estate using blockchain technology. In J. Zhou, M. Conti, & C. M. Ahmed (Eds.), *Applied cryptography and network security workshops* (pp. 77–90). Springer.

Hornuf, L., Kück, T., & Schwienbacher, A. (2022). Initial coin offerings, information disclosure, and fraud. *Small Business Economics, 58*(4), 1741–1759. https://doi.org/10.1007/s11187-021-00471-y

Howell, S. T., Niessner, M., & Yermack, D. (2020). Initial Coin offerings: Financing growth with cryptocurrency token sales. *The Review of Financial Studies, 33*(9), 3925–3974. https://doi.org/10.1093/rfs/hhz131

Huang, W., Meoli, M., & Vismara, S. (2020). The geography of initial coin offerings. *Small Business Economics, 55*(1), 77–102.

Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S.M., & Felten, E.W. (2018). *Arbitrum: Scalable, private smart contracts. Proceedings of the 27th USENIX Security Symposium* (pp. 1353–1370). https://collaborate.princeton.edu/en/publications/arbitrum-scalable-private-smart-contracts. Accessed 12 August 2023.

Kreppmeier, J., Laschinger, R., Steininger, B. I., & Dorfleitner, G. (2023). Real estate security token offerings and the secondary market: Driven by crypto hype or fundamentals? *Journal of Banking & Finance, 154*, 106940. https://doi.org/10.1016/j.jbankfin.2023.106940

Lambert, T., Liebau, D., & Roosenboom, P. (2022). Security token offerings. *Small Business Economics, 59*(1), 299–325. https://doi.org/10.1007/s11187-021-00539-9

Li, J., & Mann, W. (2018). Initial coin offering and platform building. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3088726

Liebau, D., & Scheuffel, P. (2019). Cryptocurrencies & Initial Coin Offerings: Are they Scams?—An Empirical Study. *The Journal of the British Blockchain Association, 2*(1), 1–7. https://doi.org/10.31585/jbba-2-1-(5)2019

Loesch, S., Hindman, N., Richardson, M.B., Welch, N. (2021). Impermanent loss in Uniswap v3. Working Paper.

Lyandres, E., Palazzo, B., Rabetti, D., 2019. Do tokens behave like securities? An anatomy of initial coin offerings. https://www.runi.ac.il/media/1otedfav/do-tokens-behave-like-securities-lyandres.pdf. Accessed 12 August 2023.

Lyandres, E., Palazzo, B., & Rabetti, D. (2022). Initial coin offering (ICO) success and post-ICO performance. *Management Science, 68*(12), 8658–8679. https://doi.org/10.1287/mnsc.2022.4312

Malinova, K., & Park, A. (2018). Tokenomics: When tokens beat equity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3286825

Markheim, M., & Berentsen, A. (2021). Real estate meets blockchain: Opportunities and challenges of tokenization of illiquid assets. *Zeitschrift Für Immobilienökonomie, 7*(1), 59–80. https://doi.org/10.1365/s41056-020-00051-3

Masiak, C., Block, J. H., Masiak, T., Neuenkirch, M., & Pielen, K. N. (2020). Initial coin offerings (ICOs): Market cycles and relationship with bitcoin and ether. *Small Business Economics, 55*(4), 1113–1130. https://doi.org/10.1007/s11187-019-00176-3

Momtaz, P. P. (2020). Initial coin offerings. *PLoS ONE, 15*(5), e0233018. https://doi.org/10.1371/journal.pone.0233018

Momtaz, P. P. (2021a). Entrepreneurial finance and moral hazard: Evidence from token offerings. *Journal of Business Venturing, 36*(5), 106001. https://doi.org/10.1016/j.jbusvent.2020.106001

Momtaz, P. P. (2021b). The pricing and performance of cryptocurrency. *The European Journal of Finance, 27*(4–5), 367–380. https://doi.org/10.1080/1351847X.2019.1647259

Mosley, L., Pham, H., Guo, X., Bansal, Y., Hare, E., & Antony, N. (2022). Towards a systematic understanding of blockchain governance in proposal voting: A dash case study. *Blockchain: Research and Applications, 3*(3), 100085. https://doi.org/10.1016/j.bcra.2022.100085

Parra Moyano, J., & Ross, O. (2017). KYC Optimization using distributed ledger technology. *Business & Information Systems Engineering, 59*(6), 411–423. https://doi.org/10.1007/s12599-017-0504-2

Rossi, A., Vismara, S., & Meoli, M. (2019). Voting rights delivery in investment-based crowdfunding: A cross-platform analysis. *Journal of Industrial and Business Economics, 46*(2), 251–281. https://doi.org/10.1007/s40812-018-0109-x

Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *Journal of Emerging Technologies in Accounting, 16*(1), 21–35. https://doi.org/10.2308/jeta-52432

Shakhnov, K., & Zaccaria, L. (2020). (R)Evolution in entrepreneurial finance? The relationship between cryptocurrency and venture capital markets. Working Paper. https://doi.org/10.2139/ssrn.3613261.

Smith, J., Vora, M., Benedetti, H.E., Yoshida, K., & Vogel, Z. (2019). Tokenized securities and commercial real estate. Working paper. https://doi.org/10.2139/ssrn.3438286.

Smith, C. et al. (2023). ERC-20 token standard. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/. Accessed 2 June 2023.

State Secretariat for International Finance SIF. (2020). Federal act on the adaptation of federal law to developments in distributed ledger technology. https://www.sif.admin.ch/dam/sif/en/dokumente/Blockchain/blockchain_dlt_gesetz.pdf.download.pdf/DLT%20Federal%20Act.pdf. Accessed 2 June 2023.

Swinkels, L. (2023). Empirical evidence on the ownership and liquidity of real estate tokens. *Financial Innovation, 9*(1), 45. https://doi.org/10.1186/s40854-022-00427-5

Weyl, E. G., Ohlhaver, P., & Buterin, V. (2022). Decentralized society: Finding Web3's soul. Working paper. https://doi.org/10.2139/ssrn.4105763.

Wilson, G. (2022). The fall of FTX will lead to a rise in crypto self-custody solutions. https://www.palmbeachgroup.com/palm-beach-daily/the-fall-of-ftx-will-lead-to-a-rise-in-crypto-self-custody-solutions-2/. Accessed 2 June 2023.