Blockchain Vending Machine: A Smart Contract-Based Peer-to-Peer Marketplace for Physical Goods

Schär, Fabian and Schuler, Katrin and Wagner, Tobias

Center for Innovative Finance, Faculty of Business and Economics, University of Basel, Switzerland

2020

Blockchain Vending Machine: A Smart Contract-Based Peer-to-Peer Marketplace for Physical Goods

Fabian Schär, Katrin Schuler*, and Tobias Wagner

Center for Innovative Finance
Faculty of Business and Economics, University of Basel, Switzerland

July 10, 2020

Abstract – In this paper, we propose an autonomous vending machine that is governed by a public Blockchain and smart contracts platform. Set up as a decentralized autonomous organization, it serves as an open marketplace for physical goods, where anyone can buy and/or sell objects. We propose a basic architecture for the machine, analyze pricing and fee mechanisms and examine potential pitfalls. Moreover, we discuss open issues, possible extensions and further areas for improvement. We conclude that the deployment of such machines could significantly improve our understanding of decentralized autonomous organizations and build a bridge between virtual and physical markets. Insights gained from such an experiment may raise important questions for further research.

Keywords – Blockchain, Decentralized Autonomous Organization, Distributed Ledger, Internet of Things, Smart Contract, Tokenization.

JEL Classification – D47, L17, O39.

1 Introduction

Public Blockchain networks such as Bitcoin [1] and Ethereum [2] [3] allow anyone to store and transfer value in a secure and autonomous way. In particular, there is no need for a central bookkeeper and transactions cannot be censored or modified, [4]. Unfortunately, basic transfers are limited to the respective Blockchain's native protocol asset, i.e., BTC in the case of the Bitcoin Blockchain and ETH in the case of the Ethereum Blockchain. There are, however, ways to create on-chain representations of additional assets. Such representations are usually referred to as (Blockchain) tokens.

Despite a broad variety of ways to issue tokens, smart contract-based token creation is the predominant issuance form, with Ethereum as the primary platform of choice, [5]. Fungible tokens are usually created in compliance with the `ERC-20` token standard [6], while non-fungible tokens (collectibles) mostly use the `ERC-721` interface specifications, [7]. Using one of these standards, new tokens can be created.

One key issue of tokens is *counterparty risk*. If the issuer promises something in exchange for the token, the respective token's value will directly depend on the issuer's reputation. If the issuer is not willing or capable to deliver on its promise, then demand for and thus value of the token will collapse, [5]. For purely virtual assets this may be addressed by embedding the token's utility in a smart contract. For tokenized physical assets or services that cannot be natively fulfilled on-chain, *counterparty risk* remains a critical aspect.

The problem arises from the separation of legal ownership[1] (the token) and the control over the physical asset. If, for example, someone tokenizes a baseball card, the token may very well represent a legal claim on the underlying physical asset. However, if the token owner is unable to access the baseball card, a claim may be worthless or at least impaired by the enforcement cost. Consequently, Blockchain-based tokens can be used to accurately track the ownership of a physical asset, but do not inherently address counterparty risk. The protection of the holder's interest against fraudulent issuers has been one of the driving forces in many jurisdictions to classify tokenized promises as securities subject to respective

*Corresponding Author: katrin.schuler@unibas.ch

[1] in some cases it is not even clear if the token represents a legal claim.

regulation. Compliance with such regulation typically creates a significant cost burden for the issuer, and thus renders small scale tokenization of ownership effectively impossible. Furthermore, security regulations typically restrict trading activities to regulated exchanges.

One way to address counterparty risk for promises of physical goods is through escrow or custody services. Building on this approach, we propose a new type of vending machine, that links the delivery and the purchase of goods atomically, i.e., in an inseparable way. The exact conditions and procedures are transparently embedded in and deterministically executed by a smart contract system. Residing on a public Blockchain, these contracts form a decentralized autonomous organization (DAO) that controls the vending machine.

While the basic setup we are describing is not a perfect protection mechanism, it is a step towards a transparent, open and independent peer-to-peer marketplace for physical goods that can be regarded as a form of public infrastructure. There are many interesting applications involving physical objects, where the basic properties of such a vending machine could be leveraged. Last but not least, it is somewhat symbolic that the vending machine, which was among the first examples of a smart contract [8] [9], shall serve as a prototype for a physical incarnation of a decentralized autonomous organization (DAO).

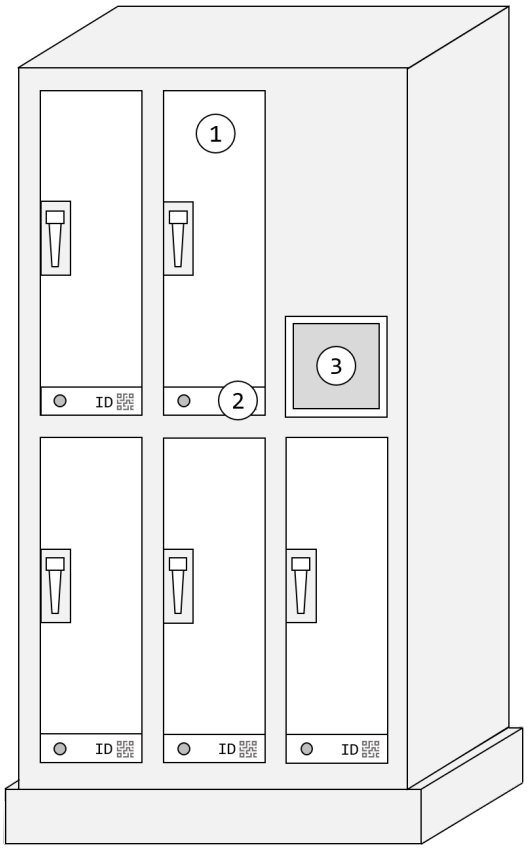

Figure 1: Illustration Basic Vending Machine

2 Basic Setup

The basic setup for the envisioned open peer-to-peer vending machine consists of two main elements. First, the machine, i.e., the actual physical vending machine including the required software to connect to the Blockchain and translate the signals received into corresponding actions. Secondly, the DAO in form of a dedicated smart contract structure on a public Blockchain. The former provides a physical incarnation, while the latter governs the behavior of the machine and controls the logic and conditions of the interactions. It is fully transparent, protected from unforeseen intervention, and open to anyone.

2.1 The Machine

Let us assume that the machine consists of $N > 0$ slots (1). Each slot shows a unique identifier (2) and has a goods compartment with a transparent door that can be locked individually. It also has a display (3), to assist users in their interactions. The vending machine is located in a public space. It is easily accessible, meaning that anyone can interact with the vending machine by assuming the role of a buyer or seller.

Buying works in the traditional way. When someone sees a good in the vending machine for which they have a buy interest at the given price, they can buy it instantly. The main difference to a regular vending machine is that instead of buying from a central counterparty, i.e., the vending machine operator, the buyer engages in a peer-to-peer transaction with someone who placed the object in the machine.

Analogously, selling via the vending machine is open to anyone, provided there is a currently unused slot. A seller simply places the goods in the compartment and provides the sales parameters, such as pricing. The machine will then initiate the sale and take over custody by locking the door. Thereafter, no further action is required of the seller, the proceeds are automatically distributed after a successful sale.

2.2 The DAO

Both the buying and the selling process are governed by the DAO's smart contracts. To release goods or lock a compartment, the machine relies on events emitted by the DAO. Also, it is the source for the currently valid parameters on pricing and fees, which are detailed later on.

To increase the autonomy of the DAO, i.e., reducing the dependency on humans [10], the smart con-

tract structure may be designed to cover a multitude of aspects. For the basic setup, however, we propose a lean structure that focuses on the autonomous handling of the core processes of buying and selling goods through the machine, plus a governance mechanism to propose and vote on fee parameter changes or extraordinary events.

While it is possible to interact with the machine directly via smart contract function calls, a simple user interface is proposed to lower the barriers to entry for potential users with limited Blockchain and smart contract knowledge. To provide a basic user experience, the machine has a display to guide through the buying and selling process as well as a button next to each slot to unambiguously indicate which slot the interaction is targeting.

3 Core Processes

3.1 Buy

Anyone who sees interesting goods in one of the slots can press the button next to it. The machine then queries the sales parameters on the Blockchain and displays the current price plus a prepared buy transaction in form of a QR code. To accept the offer, the buyer can scan the QR code, sign the entailed transaction proposal and relay it to the Blockchain network using a mobile web3 wallet. Once the buy transaction is successfully confirmed, the vending machine releases the goods from custody by unlocking the corresponding slot's door.[2] The buyer is now free to pick up the goods.

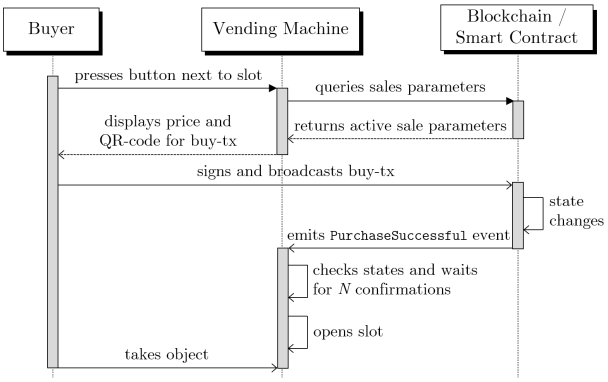

Figure 2: UML diagram buyer

3.2 Sell

Whenever a slot is vacant, anyone can use the vending machine to offer goods for sale. The seller deposits the goods in the compartment, closes the door and enters the desired parameters for the offer with regards to pricing and duration. The machine queries the current fee schedule (to be detailed later on) on the Blockchain and displays a transaction proposal in the form of a QR code. To confirm the conditions and initiate the sale, the seller can scan, sign and relay the proposed transaction to the Blockchain network with a mobile web3 wallet. When the transaction is confirmed, the door of the slot locks and the goods are ready to be sold. In case of a successful sale, the seller receives the proceeds automatically from the vending machine with no need for further interactions.

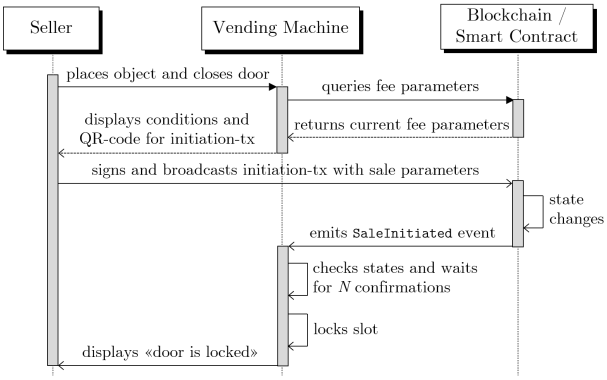

Figure 3: UML diagram seller

3.3 Price Determination

The price to be paid to purchase a good is determined through an open descending-bid auction format (Dutch auction). In this format, the bid price for the goods of a slot decreases linearly over time from a starting value set by the seller, until the first interested buyer accepts and thus closes the sale. The sale is final and since the buy transaction has to contain sufficient funds, there is no buyer default risk.

Formally, the current price $P(t)$ can be expressed as shown in equation (1), where time is measured in blocks[3] with t denoting the current period, t_s the starting period of the auction, and T the period the the price reaches 0.

$$P(t) = \max\left[0, P(t_s) - \left(\frac{(t - t_s) \cdot P(t_s)}{T - t_s}\right)\right] \quad (1)$$

The price decreases linearly (subject to variations in block time) hereby the price at any t can be described using $P(t_s)$, t_s and T.

[2] In practice, this will require a certain number of confirmations to defend against double spending attacks and reorgs.

[3] Mining is a probabilistic process. The average block time differs for each proof-of-work Blockchain network. For Ethereum, the expected block time is between 10 and 20 seconds, for Bitcoin it is around 10 minutes.

The Dutch auction format is relatively simple to implement in a smart contract and the instant purchase nature of a bid is a good fit for the basic vending machine scenario. Furthermore, limitations regarding the choice of sales parameter T at the beginning prohibit extension of the sale. Also, T serves as an important parameter for the fee schedule discussed in Section 4. This outweighs the drawback of Dutch auctions that strategic interactions of buyers may not lead to an optimal outcome in terms of overall welfare, [11], [12].

If a sale is unsuccessful, i.e., the time limit T is reached and the price has decreased to zero without a valid bid, the machine unlocks the slot and releases the goods for anyone to pick up for free. Unless the seller is present at the machine, the loss of the goods without any reimbursement is likely. An alternative approach to handle this case would be to include a grace period, during which the seller can repossess the goods. Arguments against this are twofold. First, the slot would be blocked throughout this period with no sale going on, thus decreasing the utility as public infrastructure. Secondly, the risk for the seller to part with the goods for an amount only marginally greater than zero would still be present.

4 Fee Schedule

While anyone can use an empty slot and offer goods for sale, the number of slots is limited and the vending machine incurs operating costs. To set the right incentives for efficient use of the infrastructure and provide an income source for the vending machine, a fee schedule must be defined.

In this section, we analyze different models for fee schedules, covering price-based, time-based and mixed fee implementations. In addition to the fees, which are driven by the sales parameters, the vending machine may charge a fixed fee ϵ per auction.

To keep the price presentation to buyers straightforward, fees are always owed by the seller. Any outstanding fees will be deducted from the amount paid by the buyer before the remaining proceeds are disbursed to the seller.

4.1 Time-based Fee

The basic idea of the time-based fee is to charge the seller depending on the duration that the slot is occupied. For this purpose, the vending machine maintains a fee parameter φ per block. This value depends on the targeted yearly revenue $\widetilde{y}$, the expected utilization percentage $E(z)$, and expected number of blocks per year $E(b)$.

$$\varphi = \frac{\widetilde{y}}{E(b) \cdot E(z)} \tag{2}$$

To protect the vending machine in case of an unsuccessful auction, the seller has to deposit a collateral C that corresponds to the fee for the maximum sale duration defined at the initiation of the auction with T. The difference between the maximum fee and the actual fee will be returned to the seller's wallet when the sale closes – alongside the payment for the good.

$$C = (T - t_s) \cdot \varphi + \epsilon \tag{3}$$

The actual fee earned by the machine π_v is a function of t at the sale's closure.

$$\pi_v(t) = (t - t_s) \cdot \varphi + \epsilon \tag{4}$$

With C due at initiation, a time-based fee schedule incentivizes the seller to carefully choose T, thus promoting frequent turnover and efficient allocation of the slots. However, since time-based fees exclusively depend on the duration of the auction, there is no differentiation with regards to the value of the goods sold. This may be problematic, as high value goods will likely increase the probability of physical attacks and the cost for insurance policies. As such, a purely time-based fee is hardly ideal.

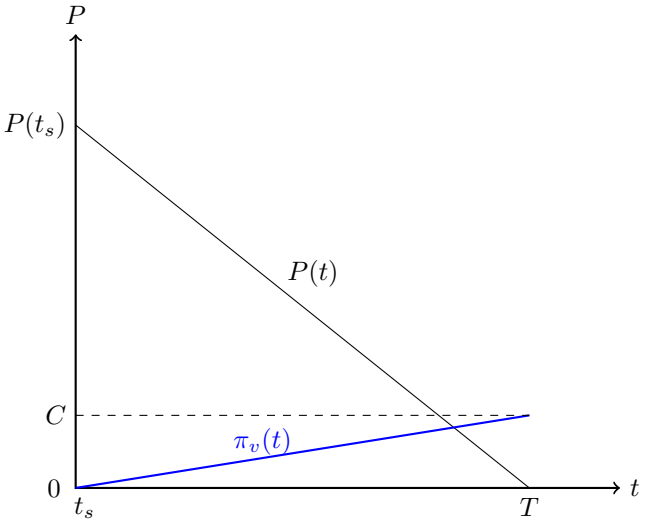

Figure 4: Time-based fee schedule with $\epsilon = 0$.

4.2 Price-based Fee

The price-based fee defines the income of the vending machine as a fraction ρ of the sales price $P(t)$. This fee parameter is set by the DAO.

$$\pi_v(t) = P(t) \cdot \rho + \epsilon \tag{5}$$

The price-based fee does not require any collateral, so beyond any base fee ϵ, no payment from the seller is required to initiate the sale. The vending machine may simply retain the outstanding fee from $P(t)$ paid by the buyer when disbursing $D(t)$ to the seller.

$$D(t) = P(t) \cdot (1 - \rho) \tag{6}$$

Since $P(t)$ is linearly decreasing in t and π_v equals any fixed base fee ϵ plus a fraction of $P(t)$, it can be easily shown that $\frac{\partial \pi_v}{\partial t} < 0$. This relationship is illustrated in Figure 5.

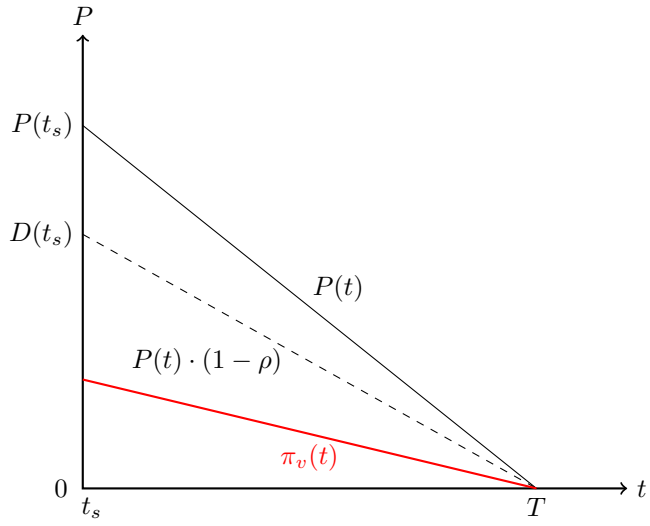

Figure 5: Price-based fee schedule with $\epsilon = 0$

This model has several drawbacks. First, the vending machine's potential income decreases over the duration of the auction and may reach zero. If no fixed fee ϵ is charged, the machine's income is fully dependent on the demand for the goods offered for sale. This is problematic, since the vending machine has no influence on the objects that are being offered for sale. Secondly, sellers have no incentive to use the slots efficiently. Consequently, this opens the possibility for malicious actors to block slots by placing worthless goods in the machine and setting the maximum values for $P(t_s)$ and T as sales parameter. Apart from the network fees for the initiating transaction, this would render the slot useless at no cost for the attacker.

4.3 Mixed Fee

In a mixed fee schedule, the fee is determined by duration and sales price.

$$\pi_v(t) = \underbrace{P(t) \cdot \rho}_{\text{price element}} + \underbrace{(t - t_s) \cdot \varphi}_{\text{time element}} + \underbrace{\epsilon}_{\text{fixed element}} \tag{7}$$

Recall that time-based fees increase over the duration of the auction towards the maximum amount of C at T, whereas price-based fees are a fraction of $P(t)$ and therefore decrease linearly over time. As a result, the first derivative of π_v with respect to t depends on the parametrization of the machine regarding φ and ρ in combination with the sales parameters $P(t_s)$ and T set by the seller. This is summarized in table 1.

Table 1: The three cases of mixed fee structures

	$P(t_s) \cdot \rho$	$\frac{\partial \pi_v}{\partial t}$
Negative time return	$> C$	< 0
Constant time return	$= C$	$= 0$
Positive time return	$< C$	> 0

As soon as the machine acquires a certain transaction history, the average actual sale durations and sales prices may be used to recalibrate the fee parameters φ and ρ. This, in combination with the incentivization for efficient utilization and participation in proceeds from successful sales, leads us to conclude that a mixed fee schedule may be the best option to realize the goals and protect the interests of the vending machine.

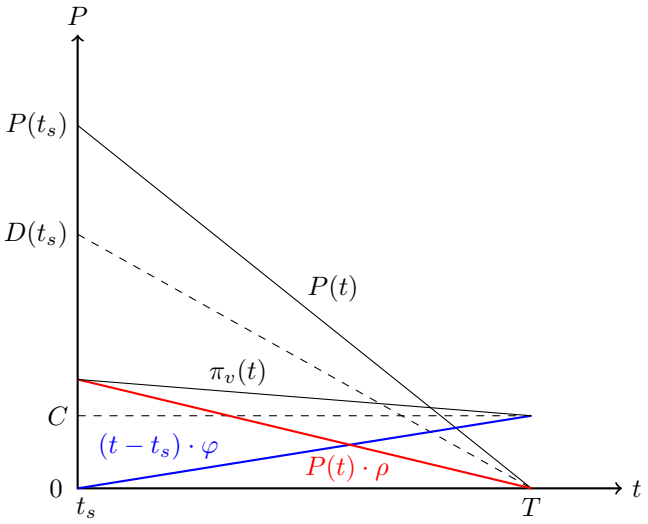

Figure 6: Mixed fee schedule with negative time return and $\epsilon = 0$

5 Security

With the machine as an IoT device in a public space and the DAO as a set of open source smart contracts deployed on a public Blockchain, there are many potential security issues whose discussion would exhaust

the scope of this paper. Assuming the integrity of the Blockchain, the smart contracts and the physical machine itself, we propose basic measures for securing the connection between the machine and its governing DAO as well as for protecting the sale process against front running.

5.1 Secured Connection

The connection between the machine and the public Blockchain the DAO contracts are deployed on can be seen as the lifeline of the vending machine. Due to its size and connection to the power grid, the vending machine is not subject to the same limitations many IoT devices face [13] and can easily run its own full Blockchain node. However, by simply hijacking the ethernet connection of the machine with a network of fake nodes, or by infiltrating the peer connections of the machine node on the actual Blockchain network through an eclipse attack [14], the physical machine may be isolated from the rest of the network. Monopolizing all peer communication of an unwitting vending machine node, the attacker is in full control of the machine's information set and may feed it an imposter Blockchain to effectively trick it into wrongfully releasing goods.

The extent of the vulnerability to such imposter attacks depends on the protocol specifications of the Blockchain network, as well as the client configuration. Both on network [15] and on client level [16], mitigation ideas are emerging relying on observed behavior of nodes, i.e., their reputation. Picking up this principle, we propose a whitelisting approach with N known and trusted peers. The vending machine client is modified such that (1) it prefers to connect to trusted nodes and (2) unless M thereof can be connected to successfully and continuously, the network connection is not deemed secure. Moreover, all data exchanged between the nodes is cryptographically signed to prevent man-in-the-middle attacks. If no secure connection can be established or maintained, the machine enters an emergency protocol that entails a shut-down as the ultimate step.

5.2 Front Running

The fully transparent nature of a public Blockchain is a key aspect for the machine's value proposition. However, coupled with the Dutch auction format, this transparency opens up the possibility of front running. Consider a situation in which two agents are interested in buying the same good. As per Dutch auction rules, the first agent to broadcast a valid buy transaction to the Blockchain should close the deal successfully. Due to the Blockchain-inherent delay between broadcasting and confirmation, however, the buy transaction may be observed in the mempool. A second agent can now interfere with a competing buy transaction. If the attacker includes a higher transaction fee, consensus relevant nodes have an incentive to prioritize the second transaction. Apart from the frustration of front-run agents, the possibility to outbid competitors by monitoring the broadcast transactions may create reluctance to buy as soon as an agent's willingness to pay for the good is reached. This lowers realized prices, directly hurting the seller's interest.

Among potential remedies are *commit and reveal* schemes. This has been proposed previously to address front running in the Dutch auction context [17]. The scheme splits the information into two transactions with the second (*reveal*) only relayed when the first (*commit*) has reached a certain number of confirmations. The *commit*-transaction locks the intent to purchase but includes only the hash value of the information identifying the targeted auction. Still visible to any observer when broadcast, the cryptographic hash is impossible to associate with any current offer. Only the subsequent *reveal*-transaction, containing the clear-text information, closes the sale.

A second, less nuanced but effective mitigation approach would be to simply set a limit to the gas fees for buy transactions that are accepted by the vending machine's smart contract. Transactions with gas fees exceeding said limit are not accepted as valid.

While the phenomenon of front running must not be classified as an attack on the integrity of the machine per se, it is nevertheless an exploit that should be addressed in order to avoid outcomes that impair the perceived fairness of the public marketplace.

6 Extensions

6.1 Participation Token

In the basic setup, the vending machine does not require an owner. It could be created as its own independent entity. However, this independence could lead to certain challenges. Alternatively, the vending machine may issue tradable tokens that entail the right to vote on governance proposals and participate in future cash flows. This approach may be preferable for a number of reasons.

First, the initial setup of the vending machine will require significant investments. Analogous to crowdfunding, a token sale may be a suitable way to raise the required funds. In addition, the machine could foster user adoption by granting buyers and sellers micro-participation rights through fractions of tokens.

Secondly, tokenized participation rights would allow the vending machine to react to a dynamic environment and unforeseeable events. Token holders

could create proposals and cast votes in proportion to their token holdings. Combining cash flow and voting rights in the same token may help to align interests and incentivize token holders to act in the machine's best interest.

Thirdly, a purely self-contained machine may raise a variety of complex legal questions. In most jurisdictions, it is not possible for a machine to be its own legal entity. This is certainly an interesting concept with increasing importance, but can lead to considerable legal uncertainty.

6.2 Long-Term Custody

The utility of the vending machine can be extended to the tokenization of physical goods. In this case, goods are placed in the slots for the purpose of long-term custody. The right to open a slot is tokenized in the form of a non-fungible token (NFT). The vending machine assumes the role of a custodian and guarantees that the NFT can be redeemed for the asset in custody. This approach has a variety of potential use cases.

First, the NFT could be traded without the need to move the physical object. It could be part of an atomic exchange against other NFTs or fungible cryptoassets, thereby effectively eliminating counterparty risk.

Secondly, the NFT would allow various conditions, such as timelocks, multisig and combinations thereof. A collector could choose to store a collectible in the machine and manage the NFT in a smart contract that, under certain conditions, grants access to relatives, business partners or friends. In this case, the vending machine essentially becomes a programmable safe deposit box with a large variety of use cases, including collateralized loans, smart contract-based implementations of a last will and the issuance of sub-tokens which represent partial ownership of the NFT.

The primary modifications required are with regards to slot access, fee schedule and security measures.

Access

A token owner may access a slot by burning the NFT. The machine must wait for a sufficient number of confirmations to ensure that the token has been irreversibly burnt before releasing the physical good. As with any tokenized promise, reorgs and forks may lead to severe issues, [18].

Fees

In the custody case, there is no reliable price information. Consequently, the fee must be purely time-based. This requires a collateral, the option to top-up, and a protocol for what happens in case the collateral is used up.

Security

The goods in custody can reasonably be expected to be of high value. As a result, the vending machine must be more robust against physical attacks. Moreover, it should be insured.

6.3 Reputation

Mere visual inspection of a good for sale may be insufficient for a buyer to assess important aspects of its value. This may increase the buyer's perceived risk [19], and lead to a market for lemons, [20]. To assess important factors of goods, such as authenticity, provenance, raw materials or production methods, buyers often rely on brand names and labels (signalling theory), [21]. Similarly, we propose an extension for the vending machine that includes attributes of the seller's reputation.

Already in the basic setup, a seller may repeatedly use the same Blockchain identity and build a brand. In extension thereof, the machine can give the seller the possibility to vouch for his honest behaviour by putting a collateral at stake. One option could be that at sale initiation, the seller may deliberately defer the payout of the proceeds by the machine. This would grant the buyer a grace period for fraud claims. As a second option, the vending machine can offer a staking contract, where a seller can lock up a variable amount. Both options require a decision body to handle claims. Analogous to resolution procedures in Blockchain-based prediction markets, the seller can be given the flexibility to assign a third party as an ombudsman. Alternatively, the machine can foresee the handling through a participation token holder vote.

Another approach would be the option to reference Blockchain-based certifications tied to the identity (address) used by the seller, [22] [23]. To create trust, certificates (claims) are cryptographically signed by trusted third parties and then timestamped using Blockchain transactions. While there is considerable flexibility with regards to format and way of storing or referencing the data on-chain, the actual utility of this approach fully depends the buyers ability to access and interpret the certificate, [24].

A third approach is the restriction of the ability to initiate sales to whitelisted addresses. However, this scenario comes at considerable cost. First, the management of whitelist entries requires human intervention, either by a service provider or participation token holders. Secondly, maintenance of an on-chain whitelist contract may prove expensive over time.

6.4 Decentralized Finance Interface

Integrating the vending machine with selected Decentralized Finance (DeFi) protocols has the potential to enrich the services offered to users and increase overall benefit [25].

First, excess liquidity could be added to lending protocols and constant function market maker (CFMM) liquidity pools. Integrating with these protocols, the vending machine could turn any idle liquidity into interest-bearing deposits. Depending on the fee schedule, the predictability of cash outflows may vary. While purely time-based fees limit the vending machine to liquid protocols, for which the assets can be withdrawn at any time, mixed fee schedules are more forgiving in this regard. In any case, the interest income supplements the vending machine's fee income.

Secondly, an integration with exchange protocols would allow the vending machine to accept a large variety of cryptoassets as means of payment. This may significantly increase convenience for buyers at no risk for the vending machine. Any payment would be routed through a liquidity pool (internal transaction) and thereby exchanged to the vending machine's preferred cryptoasset.

Thirdly, there are DeFi insurance protocols that allow the vending machine to purchase cover against financial losses from unintended (smart contract) code use. This may increase trust and complement traditional insurance against physical attack vectors. Additionally, the mere existence of a smart contract insurance policy implies that an expert third party has analyzed the smart contracts and deemed them safe enough to offer coverage at terms that are economically reasonable for the machine.

6.5 Autonomous Contracting

The long-term vision for the vending machine is to operate as autonomously as possible. While the general ability to upgrade as well as unforeseeable events require third party (participation token holder) intervention, foreseeable activities could be autonomously handled by the machine.

First, operational activities may be changed. If, for example, the machine detects a malfunction, it could start a reverse Dutch auction for the repair job. Similarly, the machine could offer rewards for regular cleaning of currently unused slots and autonomously buy insurance policies.

Secondly, expansion may be an interesting idea. Once the vending machine's funds reach a certain threshold, it could order the production of a new physical machine as well as its subsequent transport and installation. With the original vending machine able to reproduce, it has the potential to create an extended network of interconnected branches and thereby diversify risk. All of these machines would belong to one factory (smart) contract, which itself is owned by the participation token holders.

The correct fulfilment of contracts would be validated by independent third parties. Payments to contractors can only be triggered by positive signals from such oracles. Setting the right incentives for contractors is key, as every oracle validation comes at an additional cost and introduces a risk of collusion. One option may be for the machine to rely on its active sellers to check if the state of the machine is up to par. They have a vested interest in the best presentation of their goods. Moreover, contractors could be paid in vested participation tokens, aligning the interest of the agent with the long-term economic success of the machine.

Autonomous contracting is the most ambitious extension and would have to be implemented with great care, as it may introduce a variety of new attack vectors. If implemented successfully though, it would be an important step towards a truly autonomous vending machine.

7 Discussion

A DAO-based vending machine offers interesting properties as a publicly accessible, peer-to-peer marketplace for physical goods. It mitigates counterparty risk and thereby fosters trade in the absence of trusted relationships. Although transactional atomicity cannot be reached in a strict sense, since probabilistic finality of unrestricted consensus models may always lead to a situation, in which the on-chain transaction is excluded after the physical good has been released (reorg or fork), the setup can be parametrized in such a way that emulates atomicity for all practical use cases.

Funds and goods are exchanged transparently and deterministically under the governance of smart contracts, with the machine acting as physical custodian and process enforcer. The conditions of the sale are transparently defined on the Blockchain, thus minimizing required trust. The parties involved can stay anonymous apart from their physical presence at the machine. The potential for process automation and disintermediation might reduce transaction costs significantly. Lastly, the proposal positively affects censorship resistance and allows anyone to participate in the machine's success.

The proposed setup and outlined extensions should be seen as an initial analysis. In particular, there are several open points and we highly encourage further research across disciplines.

Legal scholars may analyze the (corporate) status of the vending machine and how it could fit into judi-

cial systems. Responsibilities of the machine in case of the sale of illicit or counterfeit goods as well as warranty and liability claims may offer potential for discussion. Moreover, participation tokens are likely to qualify as securities and fall under respective regulations.

Computer scientists and cryptographers may be interested in studying potential attack vectors, such as display manipulations, eclipse- or man-in-the-middle attacks. In addition, there is a need to formalize the system architecture and communication protocols.

Economists may be interested in analyzing the overall efficiency, the incentive models and the auction format. Moreover, it would be helpful to study the complex governance systems of some of the proposed extensions in a formal game theoretical model.

More applied research could focus on specific use cases. For example, taking up the trend of farm-to-table eating, an experimental variation of the proposed vending machine could be built. The decreasing pricing format poses a good match for perishable goods. The same applies for the aspects of instantaneous buying decisions, public infrastructure and goals for high slot turnover. Located in a highly frequented area, such as a train station, producers could use the machine to offer their goods for sale directly, without any intermediary. The best-before date serves as the end-point for the auction, thus preventing food waste.

To sum up, the concept offers a way to address counterparty risk in the trade of physical goods and emulates atomic transactions. Moreover, it allows us to gain experience and experiment with semi-autonomous machines. Both of these aspects are highly relevant and a good foundation for further research.

Acknowledgements

The authors would like to thank the think tank Dezentrum for their inputs as well as Sonja Burger and Emma Littlejohn for proof-reading.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[3] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[4] A. Berentsen and F. Schär, "a short introduction to the world of cryptocurrencies," *Review of the Federal Reserve Bank of St Louis*, vol. 100, no. 1, pp. 1–16, 2018.

[5] J. Roth, F. Schär, and A. Schöpfer, "The tokenization of assets: Using blockchains for equity crowdfunding," *SSRN Electronic Journal*, 2019.

[6] F. Vogelsteller and V. Buterin, "Erc-20 token standard," 2015. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

[7] W. Entriken, D. Shirley, J. Evans, and N. Sachs, "Erc-721 non-fungible token standard," 2018. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md

[8] N. Szabo, "Smart contracts," 1994. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[9] ——, "The idea of smart contracts," 1997. [Online]. Available: https://nakamotoinstitute.org/the-idea-of-smart-contracts/

[10] V. Buterin, "Daos, dacs, das and more: An incomplete terminology guide," 2014. [Online]. Available: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

[11] V. Smith, V. Coppinger, and J. Titus, "Incentives and behavior in english, dutch and sealed-bid auctions," *Economic Inquiry*, vol. 18, pp. 1–22, 02 1980.

[12] J. C. Cox, B. Roberson, and V. L. Smith, "Theory and behavior of single object auctions," *Research in experimental economics*, vol. 2, no. 1, pp. 1–43, 1982. [Online]. Available: http://www.excen.gsu.edu/jccox/research/SingleObjectAuctions.pdf

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173 – 190, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17329205

[14] Y. Marcus, E. Heilman, and S. Goldberg, "Low-resource eclipse attacks on ethereum's peer-to-peer network." *IACR Cryptology ePrint Archive*, vol. 2018, no. 236, 2018.

[15] G. Xu, B. Guo, C. Su, X. Zheng, K. Liang, D. S. Wong, and H. Wang, "Am i eclipsed? a smart detector of eclipse attacks for ethereum," *Computers & Security*, vol. 88, p. 101604, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818313798

[16] D. Letz, "Blockquick: Super-light client protocol for blockchain validation on constrained devices," *IACR Cryptology ePrint Archive*, vol. 2019, p. 579, 2019.

[17] H. S. Galal and A. M. Youssef, "Verifiable sealed-bid auction on the ethereum blockchain," in *International Conference on Financial Cryptography and Data Security*. Springer, 2018, pp. 265–278. [Online]. Available: https://eprint.iacr.org/2018/704.pdf

[18] F. Schär, "Blockchain forks: A formal classification framework and persistency analysis," 2020.

[19] M. Montecchi, K. Plangger, and M. Etter, "It's real, trust me! establishing supply chain provenance using blockchain," *Business Horizons*, vol. 62, no. 3, pp. 283–293, 2019.

[20] A. George, "The market for lemons: Quality uncertainty and the market mechanism." *The Quarterly Journal of Economics*, 1970.

[21] T. Erden and J. Swait, "Brand equity as a signalling phenomenon," *Journal of Consumer Psychology*, vol. 7, no. 2, pp. 131–157, 1998.

[22] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[23] D. Reed, M. Sprony, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (dids) v1.0 core architecture, data model, and representations," 2020. [Online]. Available: https://www.w3.org/TR/2020/WD-did-core-20200421/

[24] R. Knechtli and F. Schär, "Immutability and transparency: On blockchain-based information management and data integrity," 2020.

[25] F. Schär, "Decentralized finance: On blockchain- and smart contract-based financial markets," 2020. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3571335