Distributed ledger technologies for securities settlement – the case for running T2S on DLT

Alfred Taudes, Jakob Hackel, Wolfgang Haunold, Hannes Hermanky[1,2]
Refereed by: Fabian Schär, University of Basel

With a view to developing the Eurosystem's TARGET2-Securities (T2S) system further, we propose a system based on distributed ledger technology (DLT) that covers all major T2S settlement functionalities and investigate it with regard to regulatory compliance, performance, cost efficiency and risk. The system we propose is a federated system comprising European central banks and central securities depositories (CSDs) as node operators. The role of the central banks is to maintain the cash accounts; provide regulatory-approved "smart contract factories" defining workflows for securities issuance, lifecycle management and matching, settlement, auto-collateralization and corporate actions; and perform the oversight function. The CSDs maintain securities accounts, offer notary services for issuers, perform corporate actions, and carry out settlement. CSD nodes collect settlement requests from external trading and clearing systems, forward them to other CSDs for cross-border settlement, bundle them into transaction blocks and prepare the blocks for settlement. The ensuing ledger updates occur via a fully automated consensus process between the central banks. In T2S on DLT, specialized smart contracts provide the flexibility to settle a range of digitally represented assets, define novel workflows – and allow for variable settlement times. Rather than having to conform to a uniform settlement time of T+2, participants can choose among smart contracts that settle within seconds or longer periods of time. This feature is expected to reduce capital costs and, given the DLT-based enforcement of settlement discipline, settlement failures. Apart from conforming to the current regulatory requirements, the DLT framework also enables the central banks and authorized actors to conduct status checks at a granular level and in real time. Furthermore, comparisons with similar use cases and benchmarks show that the use of current DLT solutions would allow to meet the current daily performance goals of T2S. Preliminary cost estimates based on available public information indicate that the proposed system could be built and operated efficiently. The federated structure would also support the resilience of operations given the high number of backup nodes.

JEL classification: E44, G21, G23, K22
Keywords: distributed ledger technology, securities settlement, smart contracts, TARGET2-Securities

1 Introduction

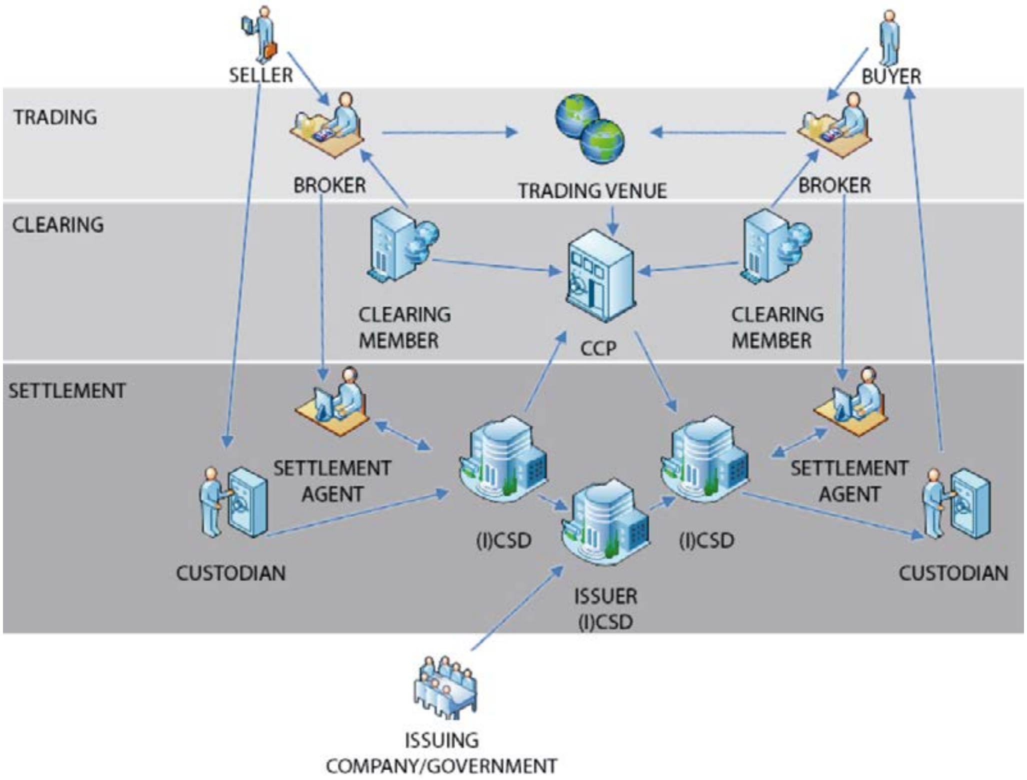
In securities transactions, ownership transfer is typically a three-stage process: first, a deal is established via brokers using a trading engine. Second, transactions are cleared through a central counterparty (CCP) to limit counterparty risk and provide netting benefits. Third, the deal is settled by central securities depositories

[1] *Vienna University of Economics and Business, Research Institute for Cryptoeconomics, alfred.taudes@wu.ac.at and jakob.hackel@wu.ac.at; Oesterreichische Nationalbank, Payment Systems Strategy Office, wolfgang.haunold@oenb.at and hannes.hermanky@oenb.at (corresponding author).* *Opinions expressed by the authors of studies do not necessarily reflect the official viewpoint of the OeNB or the Eurosystem.* *The authors would like to thank Vinzenz Treytl, Jamsheed Shorish and Michael Zargham for their valuable comments on an earlier version of the work.*

[2] *The work was supported by the Austrian Blockchain Center. ABC – Austrian Blockchain Center is funded within the framework of COMET – Competence Centers for Excellent Technologies by BMK, BMDW and the provinces of Vienna, Lower Austria and Vorarlberg. The COMET program is run by FFG.*

Figure 1

Post-trade processes in the securities leg of current transactions



Source: Pinna and Ruttenberg, 2016.

(CSDs) through the coordinated updating of cash and securities accounts (see figure 1).

1.1 Overview of TARGET2-Securities

In Europe, securities settlement in central bank money was harmonized and centralized with TARGET2-Securities (T2S), the common platform launched by the Eurosystem in June 2015. Before T2S, cross-border securities settlement in Europe was costly and cumbersome due to different settlement practices among countries and complex cross-border settlement procedures. As outlined by the ECB on its website, "T2S lays the foundations for a single market for securities settlement and thus contributes to achieving greater integration of Europe's financial market. It does this by:

- making it easier for investors to buy securities in other EU Member States
- reducing the cost of cross-border securities settlement
- increasing competition among providers of post-trade services (i.e. clearing and settlement services) in Europe
- pooling collateral and liquidity, meaning that banks no longer need to keep these in various locations and can quickly move them to where they are needed
- reducing settlement risk and increasing financial stability by using central bank money for transactions on the platform."

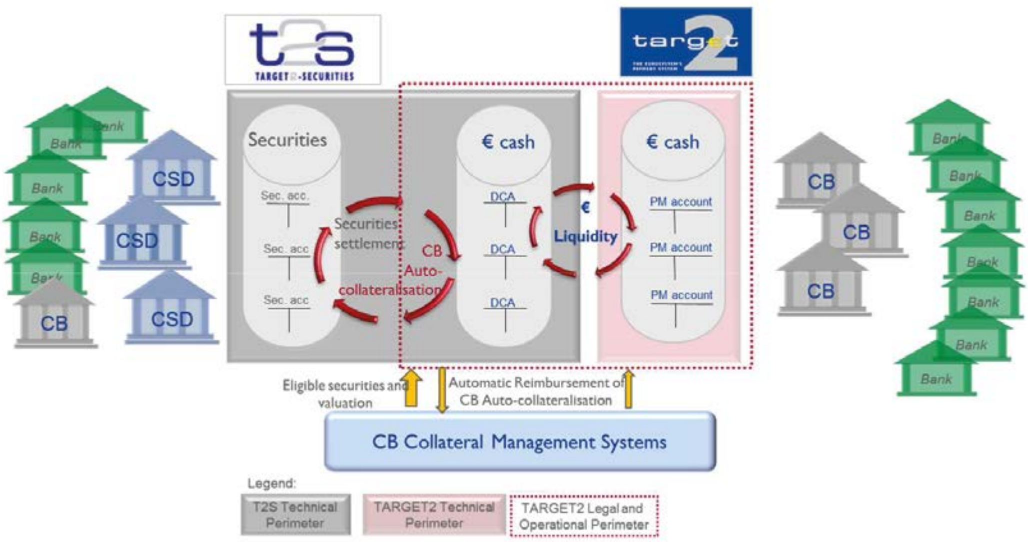
T2S matches settlement instructions submitted by central securities depositories and other directly connected T2S actors and coordinates the updates of the securities and cash legs of the transactions. T2S securities accounts are managed by the 21 participating CSDs while cash accounts are managed by the participating central banks. Of the six transaction categories handled by T2S, delivery-versus-payment (DvP, simultaneous transfer of central bank money and securities) accounted for 66.43% of the volume processed in 2019, followed by free-of-payment (FOP, delivery of securities without a simultaneous transfer of funds) with 30.60% of the volume (ECB, 2021a) (see figure 2). PFOD (payment free of delivery) transactions, SRSE (settlement restriction on securities) transactions, LQT (liquidity transfer) transactions and DWP (delivery-with-payment) transactions together accounted for 2.97% of the daily average volume. In addition to transactions to exchange securities, T2S handles corporate actions such as payments of dividends and administrative functions like the issuing of new securities.

T2S settles trades in four phases within two days. From 6:45 p.m. to 8:00 p.m., securities are validated, and liquidity is transferred from TARGET2, the real-time gross settlement system operated by the Eurosystem, to dedicated cash accounts in T2S. Then the nighttime settlement cycle is performed from 8:00 p.m. to 3:00 p.m. After a two-hour maintenance window, daytime settlement starts, at the end of which liquidity is transferred back to TARGET2 until 6:00 p.m. The time remaining to the next cycle is used for reporting.

If cash or securities necessary for settling a transaction are not available, settlement fails. To enhance settlement efficiency, T2S provides credit through auto-collateralization, either through "auto-collateralization on flow" (with transactions being secured by the securities that are being purchased) or "auto-collateralization on stock" (with transactions being secured by securities already held by the buyer). If settlement fails despite these measures, T2S retries settlement during a 60-day recycling period. In 2019, the percentage of transactions settled by T2S on the

Figure 2

Overview of T2S



Source: OeNB, 2017.

same day was 93.27% (ECB, 2021a). Since 2020, settlement failures have been discouraged by financial penalties and mandatory buy-ins under CSD Regulation (EU) No 909/2014 (EquityClear, 2020).

T2S is owned by the Eurosystem and run by the central banks of France, Germany, Italy and Spain. Following initial development costs of about EUR 584 million, the annual running costs amount to about EUR 102 million. In 2019, T2S processed on average 606,938 securities transactions per day, with a value of EUR 1,106.13 billion. On average, intra-CSD transactions, i.e. transactions within individual countries, represented 99.03% of all trades (ECB, 2021a). As T2S is a central platform, special efforts have been made to ensure robust operation, including rotation between primary and secondary sites. In 2019, the availability of T2S was equal to or above its target of 99.7%.

Notwithstanding major achievements of TS2, including higher security and lower cross-border transaction cost, the following shortcomings remain, as identified by BNP Paribas (2019):

- "The cost of settlement has not reduced. Indeed, it has increased. Even if this is explained by transaction volumes (lower than predicted at the launch of the project in 2010) and by the project's high amortization costs, it is disappointing
- Cross-border settlements (from one CSD to another) are easier and cheaper. However, they still account today for less than 1% of T2S transactions and hence are comparatively insignificant
- We do not yet have a single European capital market – issuers have continued issuing in the markets that they and their investors know best
- Competition between CSDs remains limited. Its impact on pricing is unclear, as some CSDs have increased their asset servicing fees. Nor has competition led to consolidation of CSDs
- Settlement and asset servicing remain interdependent."

1.2 Previous assessments of DLT use for securities settlement

Distributed ledger technologies (DLTs) enable the distributed storage and sharing of data records. At the same time, DLTs ensure data integrity through applied cryptography and distributed consensus-based validation protocols. Furthermore, they enable the execution of complex transactions via smart contracts, i.e. programming code that executes agreements automatically on DLT computer infrastructure. Due to their many functional features, DLTs have a potentially transformative impact on financial services. Implementation of these technologies is currently being considered for many financial services functions, including payments, deposits and loans, market provisioning, investment management, and insurance.

The potential of DLT and blockchains, a specific type of distributed ledger technology, for securities settlement has been studied by several authors from various perspectives.

Pinna and Ruttenberg (2016) analyze the current securities post-trade landscape and point out that the necessity to reconcile silos of information controlled by different intermediaries results in complex and expensive processes. They find that embracing DLT to increase the internal/cluster efficiency of existing players would not lead to substantial gains as long as current business practices remain unchanged. In contrast, a radical transformation of trading, where issuing companies, fintechs and governments would set up a peer-to-peer system in the spirit of

Bitcoin, could radically reduce post-trade cost and trading time – but this approach is in conflict with the current regulatory environment. Therefore, Pinna and Ruttenberg (2016) propose the collective adoption of DLTs by CSDs and central banks as a third alternative, which would yield substantial benefits within the current regulatory environment.

Analyzing the potentials and risks of DLT for payment processing and securities settlement, Deutsche Bundesbank (2017) finds that DLT promises improvements in transparency and immutability, operational efficiency, security and resilience, independence from intermediaries, and automated contract processing. Yet, these improvements come at a cost: privacy may be at risk if current encryption technology becomes unsafe as technology improves, a network with different node types may be more prone to attacks, and links to real assets represented on a DLT have to be established by an intermediary.

The Committee on Capital Markets Regulation (2019) argues that public blockchains like Bitcoin are not suited for real-time settlement of securities transactions. They recommend collaborative efforts of existing stakeholders to improve current systems based on permissioned blockchains, pointing out the integration of the cash leg and reversibility of transactions as important issues. Similarly, Chiu and Koeppl (2019) state that, "For policymakers and regulators, three key themes emerge from our analysis. First, to ensure DvP, it is important to link digital ledgers for asset ownership and payments together to support atomic trades. Second, the feasibility of using a blockchain for settlement depends on a sufficient volume of transactions, high enough costs for tampering with the blockchain (possibly in the form of fines) and a limited default exposure. Here, regulation and supervision could play a role to ensure such conditions. Finally, in the case of a permissionless blockchain, coordination to adjust its design might prove difficult. Here, the regulator can help to coordinate the different participants to reach agreement."

Mainelli and Milne (2016) report the outcome of a series of interviews and focus group meetings with professionals working in post-trade processing and the provision of mutual distributed ledger services. Respondents argued that DLTs for securities transaction processing would need to be permissioned, and that substantial reengineering of business processes is needed to reap the benefits of a transition to DLT.

Another factor to be taken into account is settlement time, as it determines the collateral and regulatory capital necessary to cope with counterparty risk. This would imply that the settlement time should be as short as possible. Yet, a too short settlement cycle may require dealers to pre-fund their trades or to borrow the securities they need to settle. In 2013, for instance, the Moscow Stock Exchange transitioned from real-time settlement to T+2, citing security borrowing costs as the key rationale for this move (see Pavliva, 2013). It therefore makes sense to implement flexible settlement times, letting market participants choose this parameter. However, Khapko and Zoican (2020) argue that flexible settlement speed coupled with mandatory borrowing can lead to an inefficient race to shorter-than-optimal settlement cycles, excessive security borrowing activity, and economic rents for security lenders. They find that this tension is reduced by flexible failure-to-deliver penalties that depend on the cost of borrowing securities, disciplining security lender competition and allowing for real-time settlement. In a DLT based settlement system, such features can be implemented in the smart contracts that handle settlement in a straightforward way (see Szabo, 1994 and 1997, for smart contracts).

The BIS Committee on Payments and Market Infrastructures (2017) provides an analytical framework for analyzing the use of blockchains in payment, clearing and settlement. The framework consists of a method for describing the architecture of a DLT network and a set of questions regarding the efficiency, safety, and market implications of a proposed system.

Parallel to the ongoing theoretical analysis of DLT, several prototypes of DLT systems for securities settlement have been built and studied, the most notable ones being Jasper, Stella, Ubin, Blockbaster and Helvetia (see Bech et al., 2020).

Project Jasper is a collaboration between Payments Canada, the Bank of Canada, TMX, Accenture and R3 (see Bank of Canada et al., 2018). In the project, DvP of equity tokens representing a claim on equity held in Canada's depository system against cash tokens representing a claim on the Bank of Canada was tested using atomic settlement on the same ledger. It was found that the new process was more efficient and less risky when compared to the existing settlement system.

Project Stella is a collaboration between the ECB and the Bank of Japan (see ECB and Bank of Japan, 2018). The project tested single-ledger and cross-ledger DvP using security and cash tokens with a focus on settlement failures. In the single-ledger case, trades were found to fail when trading details had not been agreed between parties or when validation of the transaction failed. In such cases, the tokens remain with their owners, exposing traders to replacement cost risk only. In cross-ledger DvP, trades were found to fail if one leg of the transfer could not be delivered, exposing participants to principal risk, too. Hence, the ECB and the Bank of Japan (2018) conclude that an arbitration function on the ledger is needed to deal with such cases.

Based on these findings, Project Ubin (Monetary Authority of Singapore, et al., 2018) served to build a framework for governing settlement processes, including arbitration processes to deal with settlement fails and a recognized market operator for monitoring and facilitating market functionalities. These new processes were found to compress the settlement cycle and to reduce principal risk.

Project Blockbaster by Deutsche Börse and Deutsche Bundesbank (see Deutsche Bank and Deutsche Börse, 2018) served to investigate the performance of DLT for securities settlement using the Hyperledger Fabric system. In these experiments, DLT was shown to fulfill the performance requirements necessary for building real-life settlement systems. Moreover, Deutsche Börse, Deutsche Bundesbank and Germany's Finance Agency have recently demonstrated that it is possible to establish a technological bridge between blockchain technology and conventional payment systems to settle securities in central bank money with a transaction coordinator in TARGET2 (see Deutsche Bank, 2021).

In Project Helvetia, the BIS, in cooperation with SIX Group AG and the Swiss National Bank, showed that it is possible to provide central bank money to settle securities transactions in a realistic near-live setting using new technologies (see BIS et al., 2020). This exercise confirmed the feasibility of linking up the existing systems and of issuing digital central bank money.

Shabsigh et al. (2020) summarize the findings from DLT prototype projects in settlement as follows: "In general, the DLT prototypes showed that DLT could be viable for post-trade securities processing and all projects concluded that securities settlement is a highly suitable and feasible environment for DLT-based solutions. The experiments showed that different DvP models can be implemented in DLT-based systems. DLT solutions can vary considerably in features and tools, with which a more efficient processing and account method can be designed and customized for improved efficiency and security in specific markets according to market needs."

Regarding the architectures tested, Shabsigh et al. (2020) state: "In all prototypes, the central bank was given the role of cash instrument provider and could thereby also be the one ensuring DvP requirements. A project assumption appeared to be that securities clearing and settlement systems operate within a market structure close to the current structure—that is, exchanges, dealers, CCPs, CSDs, custodians, and central banks operate in similar or near-similar roles as they do today and in a multilayered registration structure. None of the projects analyzed flatter market structures and DvP processing at the end-investor level or other radical structural changes in the market and associated risks." With regard to open issues, Shabsigh et al. (2020) mention the study of the impact of real-time 24/7/365 processing on the design of the system, the analysis of liquidity and credit risk in a realistic setting and the possible changes in market structures.

In addition to the experimental project discussed above, two DLT-based systems for securities settlement are at the pre-production stage, one in Australia and one in Switzerland. The Australian Stock Exchange has developed a DLT-based system for clearing, settlement, and securities registration to replace its current system, called CHESS (Australian Stock Exchange, 2020). The new system, which builds on a prototype developed in 2016, only covers the securities leg. Development costs were reported to amount to USD 50 million.

The Swiss DLT settlement prototype, developed by SDX, covers the full securities value chain including order entry, order crossing in the matching[3] engine, DvP settlement on Corda DLT and distributed holdings of intermediated securities/tokenized cash. The reported costs are USD 100 million so far. According to SDX (2019) "Test-cases will showcase the potential of SDX's riskless trading model, as well as settlement on DLT. Early-stage functionality will cover digital security token issuance as well as live trading and instant settlement. This will include the cash-leg of the transaction embracing the concept of a payment token as well as access to a distributed portal where it would be possible to monitor transactions across specific DLT member nodes." When moving to the new system, SDX expects costs to decrease due to reduced collateral requirements, lower operational costs, and lower data management costs enabling potentially lower fees per transaction. Further benefits anticipated are an increased asset universe, new primary and secondary markets, a private marketplace for interbank/inter-client trades, real-time information at the client holding level enabled by the link between asset and owner and a significant simplification of corporate event handling.

1.3 Outline

Based on these findings, we present a DLT-based architecture for T2S and describe how T2S would work in this new environment. In the description, we concentrate on delivery-versus-payment (DvP) transactions and corporate actions. The principles discussed here also apply to the other transaction types. Subsequently, we analyze the feasibility and advantages of our design from a technical and economic

[3] *Matching is the process of comparing the settlement details provided by the buyer and the seller of securities in order to ensure that they agree on the settlement terms of the transaction.*

perspective and with regard to compliance with the regulatory environment/framework based on the framework presented by the BIS Committee on Payments and Market Infrastructures (2017). In the conclusion section, we summarize our findings and outline some topics for future research.

2 Specification of T2s on DLT

2.1 Architecture – understanding the arrangement

Type of DLT: Following the findings in literature, the system we propose is not publicly accessible but private and permissioned. It employs a heavily centralized consensus protocol, based on a predefined (closed) set of consensus-relevant nodes, and restricts read access. Unlike with public DLT solutions like Bitcoin or Ethereum, this provides advantages from a regulatory perspective, as public DLT solutions are incompatible with existing case law (Pinna and Ruttenberg, 2016). Moreover, permissioned DLTs have a higher capacity and fewer restraints than current permissionless blockchains. Public blockchains currently have trade-offs in lower throughput to preserve as much decentralization as possible (see Schäffer et al., 2019). Since permissonless networks are incompatible with current regulation regarding EU-wide securities settlement, our system makes a tradeoff in decentralization to achieve higher throughput than decentralized public solutions. Such a tradeoff necessarily comes with the caveat of loosened immutability, since permissioned networks are by design controlled by the parties that are authorized to establish consensus on the state of the network. Additionally, the permissioned model does not allow regular users to verify transactions or the current state themselves, which is a core premise of the permissionless model as used in some public blockchains.

Some of these conditions might change in the future. Regulation might adapt and become more welcoming to decentralized consensus on a European settlement layer, accepting some level of power over the infrastructure by unknown participants while preserving regulatory oversight and final say over settlement on a settlement layer connected to a permissionless blockchain implementation. Moreover, public and decentralized DLTs are steadily improving their base layers, as well as introducing various solutions of off-chain scaling possibilities, such as Layer 2 implementations. Such Layer 2 implementations allow for a fully secure, slower settlement layer while more scalable implementations handle most of the network load. Notably the Lightning Network is an ongoing attempt to outsource load from the Bitcoin network onto a Layer 2 solution, which handles transactions through a network of bidirectional payment channels (Poon and Dryja, 2016). Most implementations attempt to solve scalability issues by conducting off-chain transactions and only committing limited data as proof to the settlement layer. Some of these implementations use rollups, mainly ZK rollups (which commit bundled transactions through more complex "zero-knowledge proof" technology) and optimistic rollups (which leverage users actively monitoring and reporting on invalidly committed proofs) (see Whitehat, 2018, for ZK rollups and Optimism for an implementation of optimistic rollups). Additionally, "decentralized finance" (DeFi) tools might bring forward newer technological innovations, which might allow for a preservation of decentralization with high throughput. DeFi acts under different constraints and is described in detail by Schär (2021).

Nodes: The DLT design proposed comprises two types of nodes:

- Central bank nodes: These nodes are authority nodes and designed to manage the infrastructure and develop it further. They have supervisory duties and are responsible for maintaining cash accounts, regulating access to the cash leg and the trading engine, and updating the ledger of transactions.
- Central securities depository nodes: These nodes are settlement nodes and responsible for maintaining securities accounts, issuing new securities, performing settlement, and handling corporate actions. CSD nodes have selected read access to the ledger.

Users: Users send settlement instructions to be relayed by CSDs and receive reports about their holdings and transactions. They do not have access to the ledger but interact with the system via a dashboard which enables them to access messages, send message requests, and select transaction possibilities and currently available methods for settlement. Users, such as commercial banks, can sign their transactions with a key pair. However, direct access to the ledger, which would allow for independent verification by users, would necessitate either a much higher transparency of other users' actions or highly complex cryptographic methods, which would introduce drawbacks and complexities of their own. In our system, the group of users is still restricted to holders of central bank accounts.

Accounts: We distinguish between user-controlled accounts and smart contract accounts, much like permissionless blockchains such as Ethereum (see Buterin, 2014). Members of central banks, CSDs and user organizations interact with the system via user-controlled accounts, with the control tools being keys for the authorization of transactions with one or multiple signatures, depending on local governance rules. Smart contract accounts contain computer code that sends transactions which constitute ledger updates if included in a block, based on function invocations (see Szabo, 1994 and 1997). For T2S on DLT, we propose smart contracts to ensure that buying and selling instructions are executed (settlement smart contracts), to represent securities holdings and execute corporate actions (securities smart contracts), and to enable auto-collateralization.

Smart contract factories: Smart contract factories enable central banks to offer a dynamic collection of regulatory-compliant building blocks for settlement processes rather than default smart contracts limited to a single type of settlement and security. Smart contract factories serve to generate a range of smart contracts based on predefined standards, a feature already used on public blockchains such as Ethereum by projects such as Uniswap and Authereum. Thus, CSDs can create specific smart contracts to enable transactions with certain assets (e.g. stocks) to be settled in a certain way (e.g. DvP) with certain workflow specifications (e.g. T+1) subject to the prevailing technical and regulatory requirements. In other words, while being responsible for the execution of transactions, CSDs are constrained by the types of assets and workflows available from the smart contract factories managed by the central banks. Allowing for contracts to be made fully flexible without mandatory smart contract factory control might imply too drastic a departure from the way T2S operates today.

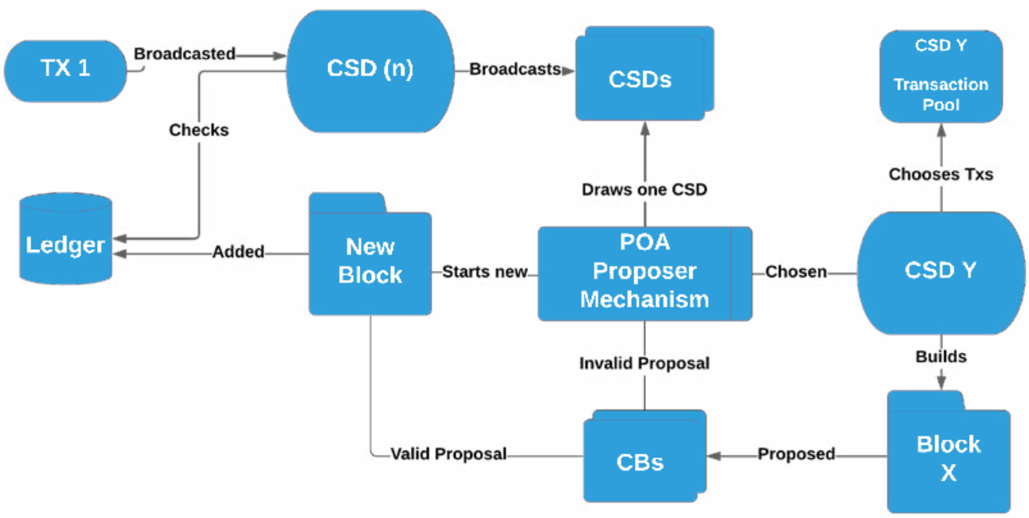
Basic settlement process: Figure 3 provides an overview of the proposed system's consensus and describes the path for a transaction to be included in an update of the ledger's state, by inclusion in a block.

Transactions are broadcasted from one CSD to the next, with each CSD storing transactions to be processed in a pool until they are settled with finality through inclusion in a block, i.e. a permanent record of transactions, by him or another CSD. Whenever a CSD is chosen by the proof-of-authority (POA) selection mechanism to be next in line for block proposition, he selects transactions outstanding from the pool and then proposes his block to the central banks by broadcasting it. The central banks check the block formally for requirements and sign off if the block was formed validly, or refuse their signature if it was formed invalidly. If a block is not accepted, the proposal mechanism chooses another CSD and starts the process again. Blocks that are signed off as valid are stored as an update to the ledger by all parties, who also delete the now-included transactions from their pool, and the process starts again.

In this setting, national banks cannot suggest that a particular transaction be settled. Nor can they reject a transaction for arbitrary reasons, which would be obvious to everyone else. All of this happens within seconds. Unlike in permissionless systems, which currently establish consensus mostly based on proof-of-work (POW, see Nakamoto 2008), in a POA consensus mechanism all participants are known and identifiable. This restricts the participation in settlement to CSDs and central banks, as current regulation demands. As a necessary drawback, the system is highly centralized when compared to open and permissionless blockchains. Most notably, the framework enables CSDs to censor transactions by not relaying them further or by not including them into the blocks they form. This issue is somewhat mitigated by users being able to send their transactions to a different CSD as well as central bank oversight. Additionally, as central banks have final authority over the infrastructure they can roll back transactions to restore a previous state, either if reconciliation is impossible otherwise or if enough central banks were to collude ("malicious nodes"). For a more formal description of POA and its benefits and limitations see De Angelis et al. (2018).

Figure 3

Consensus mechanism



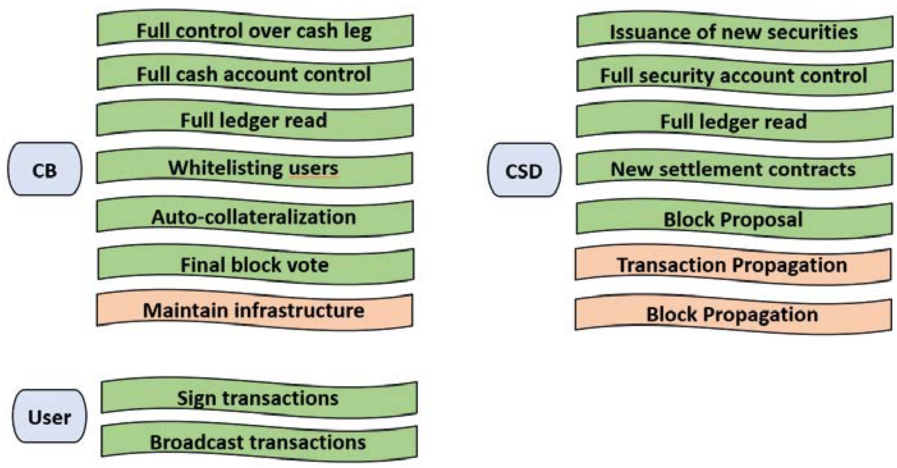
Source: OeNB/Vienna University of Economics and Business.

Cash leg: Each central bank has the right to initiate new cash generation against collateral to provide liquidity to the system. When the DLT system is launched, each participating central bank defines their initial cash balance. This balance is prefunded and serves initial funding requirements. To top up this balance, each central bank can initiate self-funding transactions to be included in the next block; much like Bitcoin blocks include "Coinbase" transactions, which allow for the creation of new Bitcoins. Together, all central banks also operate a multi-signatory account, requiring signatures from all parties, to collect cash that is to be removed from the system. Once sent to said address, the respective funds are locked for anyone and can only be unlocked through a unanimous decision of all central banks. These two mechanisms allow for the creation and destruction of cash in the system. Together, they allow for a flexible cash regime where clients in TARGET2 can deposit cash with their central bank, which in turn creates that amount of cash via a self-funding transaction on the DLT ledger and then sends this cash to the client's cash account on the DLT ledger. Until TARGET2 has been consolidated with TARGET2-Securities, which removes the requirement to net out end-of-day balances, this DLT process can also be used to create and remove daily balances. When the multi-signatory address has a large enough balance, central banks can use this already existing but locked cash to fund cash accounts again or use it for auto-collateralization by unanimous decision and signature.

Overview of roles and obligations: Figure 4 summarizes the roles and obligations in the system. Central banks act as validators and are obliged to propagate blocks. They also mint/burn cash and are able to lock funds. The central banks cooperatively create smart contract factories, keep the infrastructure up to date by building and updating the protocols, handle permissions of CSDs and approve blocks. The CSDs can create new contracts using the smart contract factories provided by the central banks, and handle transactions and corporate actions. Moreover, it is their job to validate the existence of securities and to propagate transactions. Users initiate and sign transactions.

Figure 4

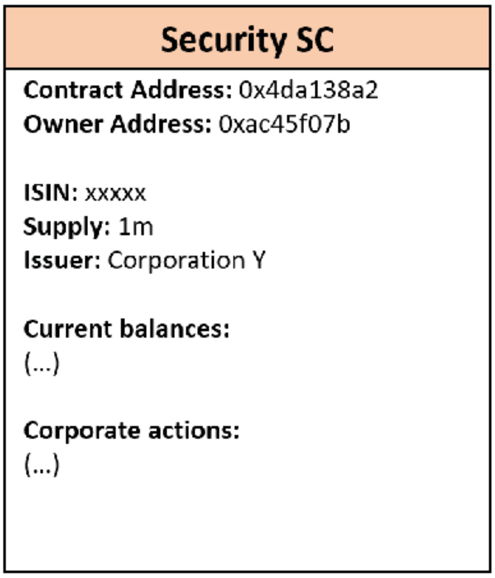
Overview of roles



Source: OeNB/Vienna University of Economics and Business.

Figure 5

Security smart contract



Source: OeNB/Vienna University of Economics and Business.

2.2 Security smart contracts

Creation: Similar to regular token contracts on permissionless DLTs, such as ERC20 (Vogelsteller and Buterin, 2015), which contain standardized functions that, for instance, allow anyone in the system to check the balance of any user, a T2S DLT security smart contract is created by a CSD and contains standardized functions. It consists of building blocks provided by the smart contract factories, which define the possible data structure and entries available to the CSD. This mechanism ensures that newly created securities comply with the relevant regulatory requirements. Factories are used to provide largely harmonized constructs for corporate actions and settlement processes, too. The ability of smart contracts to interact with each other allows for transparent automated processes. Similar security contracts have been proposed for standardization in permissionless blockchains such as Ethereum via EIP/ERC-1400 (Dossa, 2018).

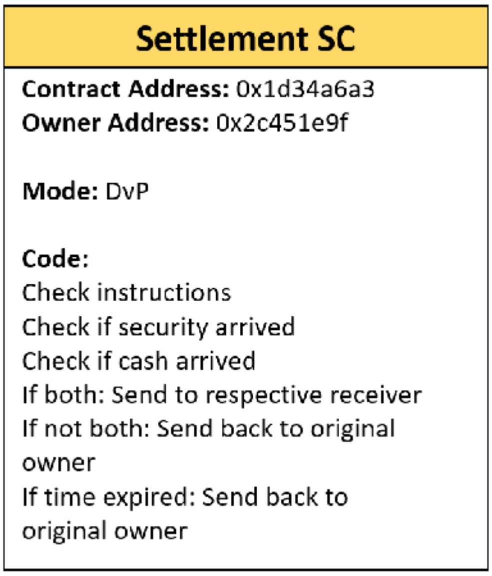
Structure: As can be seen from figure 5, a security smart contract has an address through which it can be called, and through which it can receive/send euro amounts and the contract's security token. Moreover, it stores the ISIN as a link to the CSD database. A security smart contract is owned by the CSD that records the security, and this CSD is the only party that can invalidate the contract by issuing a new one with a copied state (to allow for upgrades). Issuer information is provided either with in-system addresses or stored outside of the system. Ownership is tracked with a dictionary recording the current owners of the respective tokens. These variables are updated by settlement smart contracts (see below). Another variable indicates whether the security is available for auto-collateralization. This variable is set by the central bank controlling the auto-collateralization whitelist contract. Further, the contract can lock and unlock holdings when "called" by either central banks or through auto-collateralization contracts (see below). This prevents owners from sending their balance while the security is locked by auto-collateralization. Finally, contract functions are designed to execute corporate actions. For instance, a dividend function can be called with a certain timestamp/blockstamp set to dividend payout days with a view to distributing the current euro balance to the owners according to current holding structures.

2.3 Settlement smart contracts

Settlement smart contracts serve to trigger exchanges according to defined rules. Contracts are created by the CSD through the smart contract factories to ensure that both instructions of a deal are posted to the ledger or none. In the system we propose, both securities and cash exist on the same ledger, so smart contracts can be used for atomic settlement. As can be seen from figure 6, an atomic settlement smart contract has an address through which it can be called, and through which it can receive/send euro amounts and security tokens. The contract is owned by the CSD that initially created the settlement contract. This CSD can also invalidate the contract by issuing a new one (to allow for upgrades).

Figure 6

Settlement smart contract



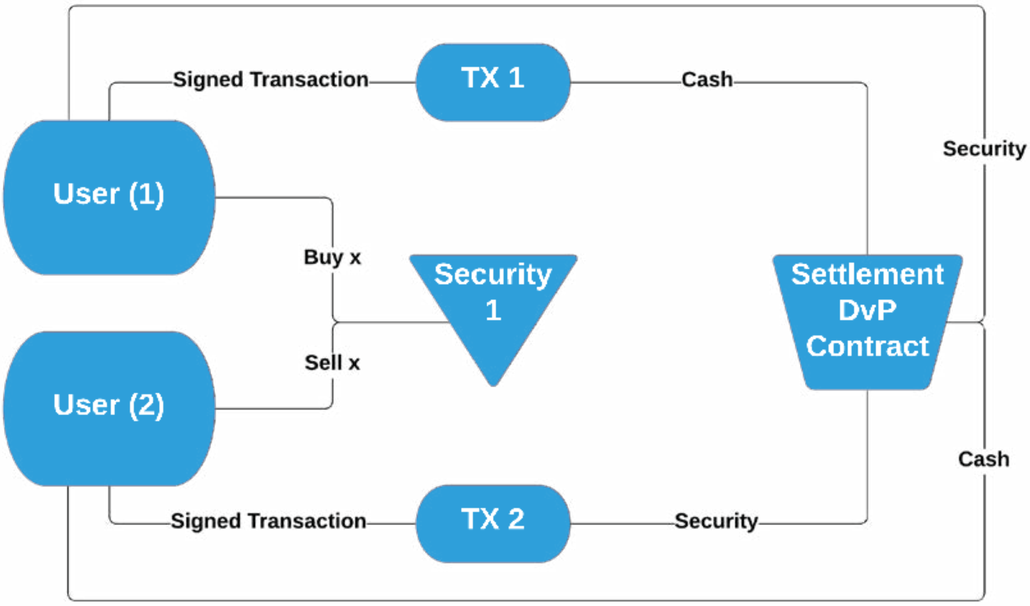
Source: OeNB/Vienna University of Economics and Business.

Such atomic transactions are implemented in permissionless blockchains as swap contracts or decentralized exchanges (see AirSwap or Schär, 2021). The standard contracts serve to trigger two transactions that need to be carried out:

- The first transaction is an initial calling of the contract, which includes the sender's instructions and signature. The instructions include a euro sender address and amount, a securities sender address and an amount and an exit transaction timestamp, which allows terminating the settlement unless both sides have sent their part by a defined time/blockstamp. A blockstamp specifies the settlement time in terms of the number of blocks that have been posted to the ledger following the creation or calling of the smart contract.
- The second transaction, in which the contract receives either euro amounts or security tokens, triggers the contract. The transaction necessitates a signature and a set of instructions that fits the one it references and which was received earlier. If the set of instructions or the amount sent do not fit the initial transaction received, the funds are returned to the sender.
- The contract's transactions are triggered if either the corresponding euro amounts or security tokens are sent, or the timestamp expires. When the correct amount of both settlement parties is received according to instructions sent and signed by both parties the contract fulfills the instructions by sending the respective euro amounts and security tokens to the respective receiver, thus settling DvP in the agreed-upon timeframe. If the correct amounts of both parties are not received by the timestamp recorded in the initial set of instructions, the contract invalidates the initial instructions and returns any funds sent earlier and according to instructions back to the respective sender. In such a case, the contract sends a settlement fail message to the central banks, which allows them to penalize the actor that failed to deliver.

Figure 7

Settlement mechanism



Source: OeNB/Vienna University of Economics and Business.

Figure 7 shows how the security and settlement smart contracts interact with the transaction processing mechanism for the example of a security delivered against cash. The two signed transactions trigger an exchange via the settlement contract if, and only if both parties send their side in full and in time. If either of those conditions is not met, the settlement contract returns any received assets back to the respective owner.

2.4 Smart contracts for auto-collateralization

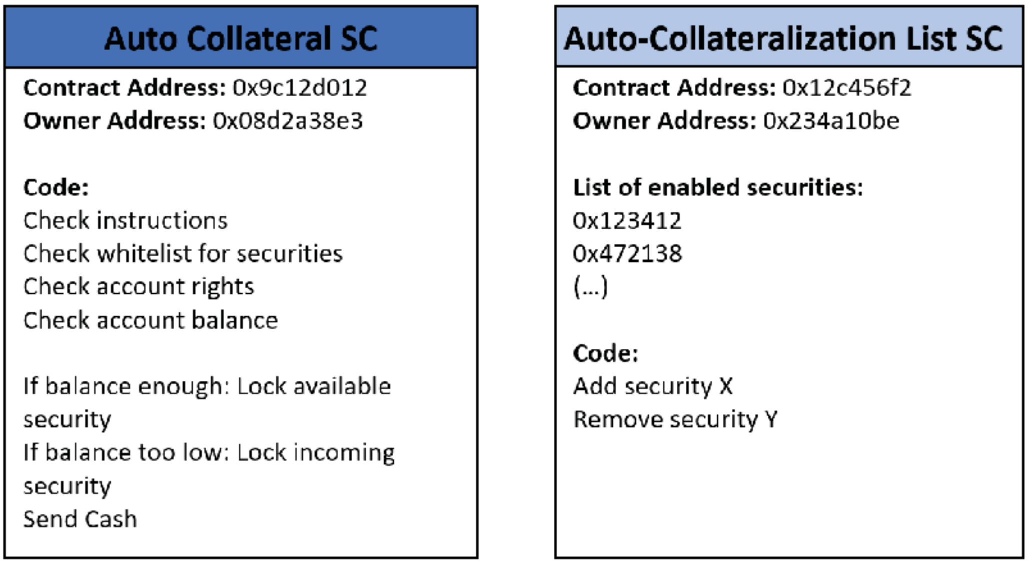
Another two types of smart contracts serve to accomplish credit provision through auto-collateralization via "auto-collateralization on flow" or "auto-collateralization on stock": auto-collateralization and the auto-collateralization list (see figure 8). Auto-collateralization locks securities which are already in the possession of the buyer or after they have been transferred and reverses the lock when the credit provided by the central banks via the respective smart contract has been repaid. Auto-collateralization is owned by the central banks via multi-signature control, meaning that changes must be signed by several central banks. This contract is prefunded by central banks and recovers its balance as needed to unlock funds previously used in auto-collateralization. To achieve auto-collateralization, the respective smart contracts check several aspects, including:

- the authorization of the address calling the contract to receive auto-collateralization
- the current balances (euro and tokens)
- the auto-collateralization list smart contract, to see if the requested security token is currently whitelisted to be used for auto-collateralization
- the instructions sent to the auto-collateralization smart contract

The contract then sends euro balances to cover the transaction and locks tokens in the respective security smart contract (see figure 9). In case of auto-collateralization on stock, the tokens locked are already in the requesting user's control and will be locked in the respective token contract. In case of auto-collateralization on flow, the respective share of the newly acquired security tokens is locked after the ownership change in the token contract. The smart contract can also be called to reverse the locks when the credit is repaid, where it again checks rights and instructions, and needs to receive the proper amount of euro to unlock the contracted tokens. The auto-collateralization list defines smart contract functions as a whitelist for auto-collateralization. It is owned by the central banks via multi-signature control and has a function that administers a dictionary containing the addresses of security smart contracts for securities that can be used for auto-collateralization on stock or flow.

Figure 8

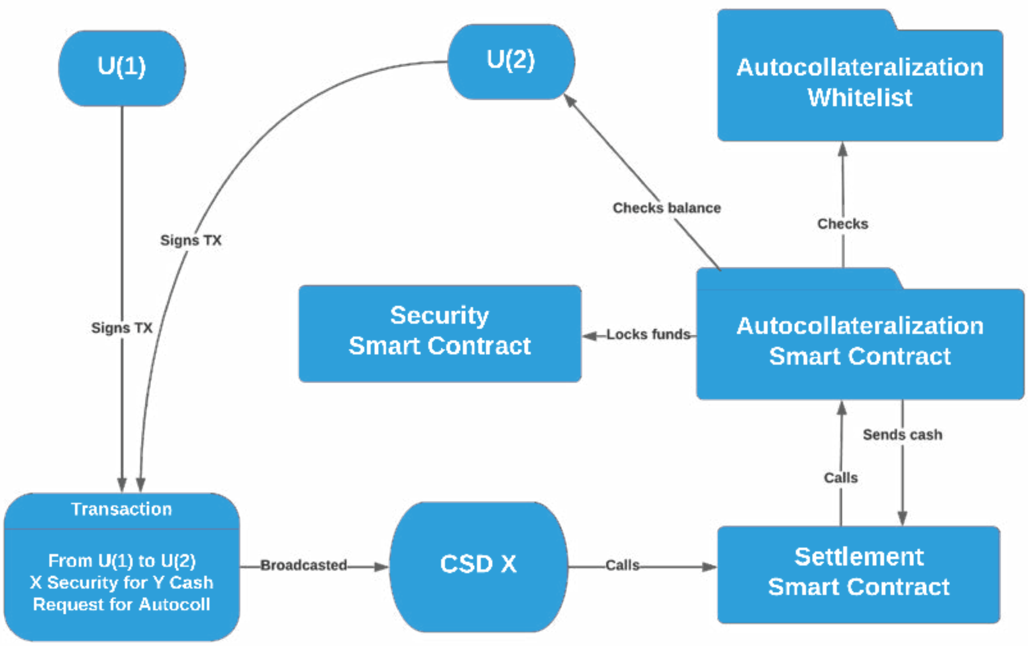
Auto-collateralization smart contracts



Source: OeNB/Vienna University of Economics and Business.

Figure 9

Auto-collateralization mechanism



Source: OeNB/Vienna University of Economics and Business.

3 Evaluation of the design

3.1 Architecture and governance

The system we propose better represents the federated structure of the Eurosystem than the current T2S architecture as every national bank has the same access in its capacity as an authority node – i.e. has access to data, voting rights and authorization possibilities. This means that the infrastructure and database are managed jointly on an equal footing. All participating central banks are thus granted the same rights. The central securities depositories are responsible for DvP and for the settlement of securities accounts. An effective separation of powers is achieved through role allocation and task assignment in the system. With regard to implications for the financial market architecture, the proposed system is evolutionary in the sense that it does not change the role of existing actors and procedures besides making securities settlement more efficient and effective. It is also innovative as it facilitates the integration of other assets in the settlement and allows for flexible settlement times. Moreover, new types of settlement workflows can be integrated in an incremental fashion via the smart contract factories.

3.2 Regulatory compliance

The architecture we propose provides advantages over the current system in the area of supervision possibilities. Banks, in the system as users, and their clients (not in the system) can be represented and controlled on the platform at a granular level and in real time. Auditing and supervision are possible in real time with granular data up to a direct holding level. With every status update of the system, the central banks have immediate access to information about the current state of the system, capital holdings, etc. Furthermore, automated reports are possible: At certain points in time or for certain events, reports are automatically generated – for example, on settlement failures – and automatically sent to the relevant stakeholders, perhaps even requiring a signature to confirm receipt. In this system, we can also program compliance checks to a certain extent. This means, for example, that one can program assets so that they can only be held by predefined (list) addresses or persons. This list can be updated at hourly, daily, or weekly intervals. This function is similar to the auto-collateralization process where users and/or assets are checked against an associated whitelist.

At the regulatory level, there are two identified hurdles, each of which can be solved by two options. First, paper certificates are regulated at the national level. Central securities depositories can continue to store documents first and then represent them digitally in the proposed concept. Alternatively, regulatory changes would have to be implemented for a purely digital securities certificate, as is currently being considered in Germany. Second, certain functions of central securities depositories are regulated EU-wide. In our case, this concerns, for example, the management of securities accounts and the execution of settlement. Current processes can also be replicated in this case. In the proposed concept, CSDs bundle the transactions to be carried out and propose them as a block, which would then be jointly signed off by the central banks, as required by regulatory standards.

3.3 Performance

Capacity: T2S currently settles 600,000 transactions per day on average. Settlement must also be possible within at least one day, and cash transactions (when the cash leg is included) must be completed in less than ten minutes.

These figures are feasible in the DLT system we propose. As a comparison, even the limited permissionless Ethereum blockchain can process 700,000 transactions per day on average. Performance tests of federated platforms are a more realistic comparison. Other platforms that make a tradeoff in decentralization are achieving much higher throughput than current public and permissionless platforms. Corda can handle more than 50 million transactions per day, with tests showing much higher, Quorum can handle over 60 million and Hyperledger Fabric can support at least 13 million, up to over 100 million in tests (see Creer, 2018, for Corda; Baliga et al., 2018, for Quorum; and Parth et al., 2018, or Chung et al., 2019, for Hyperledger Fabric). These results show that there is enough capacity also in peak times even in a net-settlement system and under the assumption of further restrictions (higher number of transactions per settlement with an external cash leg).

Speed: Meeting time restrictions is no problem from a technical point of view, either. Based on comparisons of existing platforms and the analysis of the technical tests mentioned, the concept assumes possible final DvP settlements under one minute, cash transactions under 30 seconds (see e.g. Baliga et al., 2018; Chung et al., 2019; Thakkar et al., 2018; and Creer, 2018). The proposed concept enables participants to use variable settlement times. This would make it possible to settle most transactions within seconds. In order to offer alternative processes, e.g. short sales, it is possible to integrate selected settlement periods (e.g. DvP+1) as well.

3.4 Cost efficiency

Development and operational costs: In terms of costs, there are very few comparable projects. For example, the Swiss project of the SIX Group is worth about

USD 100 million, including the first prototype and progress implementation (see SDX, 2019). The Australian Stock Exchange ASX project is valued at over USD 50 million with roughly comparable progress (see Australian Stock Exchange, 2020). Otherwise, there are hardly any comparisons for federated DLT projects. Ernst & Young (2019) estimates USD 1.5 million for a simple prototype. This does not take into account the costs of overcoming the regulatory hurdles – which are also a major cost factor when implementing the system we propose.

Based on these media reports on comparable projects, it can be estimated that a comprehensive settlement solution based on DLT would be implemented at much lower cost than the amount spent for T2S. Due to savings through lower complexity in monitoring as well as increased flexibility of the participants, lower costs than the current amount spent for T2S can be expected during operation.

Competition between CSDs can be stimulated by employing a market mechanism to determine the settlement fees. Similar to Bitcoin transaction fees, a maximum willingness to pay can be included in a settlement instruction, which will be collected by the CSD that includes the instruction in the block proposed to the central banks.

Cost of credit and liquidity management: A key benefit of the proposed architecture is the possibility of flexible settlement times. Here, the parties of a transaction can choose a settlement time depending on the conditions of the deal within the regulatory boundaries specified in the settlement smart contract factory. Our design is flexible enough to allow for the implementation of more complex schemes like the flexible failure to deliver penalties proposed in Khapko and Zoican (2020). This should provide for a substantial reduction of the cost of capital; the amount of savings could be determined via a market survey (e.g. Boston Consulting Group, 2012) and through prototyping.

Efficiency gains from automated contract tools: Corporate actions can be automated via security smart contracts. Similarly, all aspects of a settlement transaction including penalties, reporting etc. can be automated with settlement security contracts. Thus, operational costs may shrink substantially.

Users, such as banks, can control various addresses depending on their specific needs. Users, while not able to see the full ledger themselves, are able to request automatic reports on their holdings and history. Such reports are trivial to implement, as they can be easily generated from a full access ledger view (full history of the ledger); and authentication for a user account is given via signature.

Speed and transparency in reconciliation: As shown in figure 3, the system automatically keeps the ledger and the local databases of the CSDs in sync. Therefore, no additional reconciliation steps are necessary, which avoids costs and time for reconciliation. Due to the automatic reports, reconciliation with the users is improved too.

3.5 Operations and security risk

In general, the system we propose is highly resilient due to its federated structure, where nodes can be in every participating country instead of four operating sites in two regions. This can allow for resilience against attacks and prevent downtimes. In attacks attempting to remove certain actors from the system by blocking their infrastructure, the remainder of participating members will keep the system running and active. This allows for continued operations even when several nodes are attacked at the same time.

Introducing fraudulent transactions into the system would require control over the private key of the sender's address and could be rolled back later by CSDs and central banks. Cash leaving the system is controlled by central banks initiating the transfers to TARGET2. Additionally, since all members participating in consensus are known, verified, and bound by regulatory requirements, the potential damage by bad actors is limited. Since full control over the infrastructure lies with the central banks, the system can be halted or stopped if needed.

At the same time, the code of the smart contract factories needs to be thoroughly checked and verified, and key management at the central banks and CSDs must be organized properly to prevent security breaks and attacks. Implementing proper management of cryptographic access to the system and its components will be necessary to limit potential attack vectors. This process does not differ significantly from other financial infrastructures. Yet, DLT systems are still emerging technologies that continue to be under development and need proper verification of all code, especially the logic determining the smart contract factories. Proper infrastructure upgrade processes need to be established early in order to determine a collaborative but secure infrastructure maintenance by the central banks. To achieve high quality levels and transparency, the system should be open source. Depository Trust & Clearing Corporation (2020) provides a comprehensive security framework for DLT applications in the financial industry that offers measures to minimize operational and security risk.

4 Conclusions and outlook

We have shown how the core functionality of the T2S system for securities settlement in Europe could be realized on the basis of DLT. We propose an architecture where the participating central banks provide the infrastructure and regulatory oversight on an equal footing in a federated way, replicating the ledger and providing the digital infrastructure via smart contract factories and signing off settlement transactions. Within this framework, the CSDs perform settlement. The cash leg may either be integrated but payment may also be effected via a separate payment system. The main advantages of the system are shorter and variable settlement times, increased regulatory compliance, reduced reporting, and reconciliation overhead and flexibility with regard to asset types and settlement procedures.

These features may be considered sufficiently attractive to detail the proposal further in the direction of a prototype that allows the assumptions to be tested in a realistic setting. Such a system would be an ideal basis for studying the impact of real-time 24/7/365 processing on the system design, for analyzing liquidity and credit risk in a realistic setting and for further investigating the possible changes in market structures.

References

Adams, H. 2018. UniSwap. https://hackmd.io/@HaydenAdams/HJ9jLsfTz.

Angelis, S.D., L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone. 2018. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. Italian Conference on Cyber Security, Milan, Italy. 11 pp.

Australian Stock Exchange. 2020. CHESS replacement. https://www2.asx.com.au/markets/clearing-and-settlement-services/chess-replacement/about-chess-replacement.

Baliga, A., I. Subhod, P. Kamat and S. Chatterjee. 2018. Performance Evaluation of the Quorum Blockchain Platform. arXiv preprint arXiv:1809.03421.

BIS, SIX Group AG, Swiss National Bank. 2020. Project Helvetia, Settling tokenized assets in central bank money. December.

BIS Committee on Payments and Market Infrastructures. 2017. Distributed ledger technology in payment and settlement – An analytical framework. CPMI Papers 157. February.

Bank of Canada, TMX Group, Payments Canada and Accenture, R3. 2018. Jasper Phase III – Securities settlement using distributed ledger technology. October. https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf.

Bech, M., J. Hancock, T. Rice and A. Wadsworth. 2020. On the future of securities settlement. BIS Quarterly Review. March. 67–83.

BNP Paribas. 2019. Why are we still talking about T2S?. 28/08/2019. https://securities.bnpparibas.com/insights/still-talking-about-t2s.html.

Buterin, V. 2013. Ethereum Whitepaper – A Next-Generation Smart Contract and Decentralized Application Platform. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Chiu, J. and T. V. Koeppl. 2019. Blockchain-based settlement for asset trading. The Review of Financial Studies. 32, 5 (2019): 1716–1753.

Chung, G., L. Desrosiers, M. Gupta, A. Sutton, K. Venkatadri, O. Wong and G. Zugic. 2019. Performance Tuning and Scaling Enterprise Blockchain Applications. arXiv preprint arXiv:1912.11456.

Committee on Capital Markets Regulation. 2019. Blockchain and security clearing and settlement. April. https://www.capmktsreg.org/wp-content/uploads/2019/04/CCMR_statement_Blockchain_Securities_Settlement-Final.pdf.

Creer, D. 2018. Performance testing of distributed ledger technology. October. https://www.gft.com/dam/jcr:808c4d20-64d8-4633-a0ec-5226b8049ff2/gft_pov_performance-testing-of-distributed-ledger-technology.pdf.

Deutsche Bank and Deutsche Börse. 2018. Blockbaster, Final Report. October 25, 2018. https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf.

Deutsche Bundesbank. 2017. Distributed ledger technologies in payments and securities settlement: potential and risks. In: Monthly Report. September. 35–49.

Deutsche Bundesbank. 2021. DLT-based securities settlement in central bank money successfully tested. Press Release, 24.03.2021 DLT-based securities settlement in central bank money successfully tested | Deutsche Bundesbank.

Depository Trust & Clearing Corporation. 2020. SECURITY OF DLT NETWORKS- A Distributed Ledger Technology Security Framework for the Financial Services Industry, White Paper. February.

Dossa, A. 2018. ERC 1400: Security Token Standard. https://github.com/ethereum/eips/issues/1411.

Ernst & Young. 2019. Total Cost of Ownership for Blockchain Solutions. https://github.com/EY-Blockchain/fundamental-cost-of-ownership.

EquityClear. 2020. The Settlement Discipline Regime of CSDR. https://www.lch.com/system/files/media_root/equityclear-ltd/EquityClear%20Service%20Description%20-%20CSDR%20SDR%20v1.0.pdf.

ECB. 2021a. 2019 T2S Annual Report. https://www.ecb.europa.eu/paym/intro/publications/html/ecb.targetsecar202005.en.html#toc2.

ECB. 2021b. T2S financial statements for the fiscal year 2019. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.targetsecfs200603.en.pdf?decf5895f4cc2440981ccc0974af8b9b.

ECB and Bank of Japan. 2018. STELLA: Securities settlement systems: delivery-versus-payment in a distributed ledger environment. March. https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a1.pdf.

Fontaine, S. and C. Whinfrey. Authereum contracts. https://github.com/authereum/contracts.

Khapko, M. and M. Zoican. 2020. How Fast Should Trades Settle? Management Science 66(10). 4359–4919.

Mainelli, M. and A. Milne. 2016. The Impact and Potential of Blockchain on the Securities Transaction Lifecycle. SWIFT Institute Working Paper No. 2015–007.

Monetary Authority of Singapore, Singapore Stock Exchange, Anquan Capital, Deloitte and Nasdaq. 2018. Delivery versus Payment on Distributed Ledger Technologies Project Ubin. https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-delivery-versus-payment-on-distributed-ledger-technologies.pdf.

Nakamoto, S. 2009. Bitcoin: A peer-to-peer electronic cash system

OeNB. 2017. OeNB T2S Leitfaden. Version 3.0. https://www.oenb.at/dam/jcr:a1266b32-ea7e-49e5-a9a2-33d2ce0356ca/T2S-Leitfaden-v3.0.pdf.

Oved, M. and D. Mosites. 2017. Swap: A Peer-to-Peer Protocol for Trading Ethereum Tokens. https://www.airswap.io/whitepaper.htm.

Optimism. Understanding the Optimistic Ethereum Protocol. https://community.optimism.io/docs/protocol/protocol.html#introduction.

Pavliva, H. 2013. Moscow Targets March Move to 2-Day Settlement: Russia Overnight. https://www.bloomberg.com/news/articles/2013-02-25/moscow-targets-march-move-to-2-day-settlement-russia-overnight.

Pinna, A. and W. Ruttenberg. 2016. Distributed ledger technologies in securities post-trading revolution or evolution? ECB Occasional Paper 172.

Poon, J. and T. Dryja. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf.

Schäffer, M., M. Di Angelo and G. Salzer. 2019. Performance and Scalability of Private Ethereum Blockchains. 10.1007/978-3-030-30429-4_8.

Schär, F. 2021. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review. Second Quarter 2021. 153–74. https://doi.org/10.20955/r.103.153-74.

SDX. 2019. SIX Digital Exchange (SDX) Launches DLT-based Trading and Settlement Prototype. September 23. https://www.six-group.com/en/newsroom/media-releases/2019/20190923-six-sdx-update.html.

Shabsigh, G., T. Khianoarong and H. Leinonen. 2020. Distributed Ledger Technology Experiments in Payments and Settlements. IMF Fintech Note 20/01. June. https://www.imf.org/-/media/Files/Publications/FTN063/2020/English/FTNEA2020001.ashx

Szabo, N. 1994. Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks. First Monday, 2(9).

Thakkar, P., S. Nathan and B. Viswanathan. 2018. Performance benchmarking and optimizing Hyperledger Fabric blockchain platform. In: 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS) (264–276). IEEE.

Vogelsteller, F. and V. Buterin. 2015. ERC-20 Token Standard. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

Whitehat, B. 2018. Roll_up: Scale Ethereum with SNARKs. https://github.com/barryWhiteHat/roll_up.