Tokens as objects of property law: a technical approach

*Mr. L.D. van Setten**

The title of this article is meant as an invitation to those who want to understand how 'cryptographic tokens' operate, which will necessitate an introduction to the jargon of 'Web3' – 'blockchain', 'wallet', 'decentralized network', et cetera. At the same time, the title also seeks to convey that the objective of this article is not strictly to provide a Dutch property law analysis of cryptographic tokens. That would mean a walk down the familiar deterministic path that starts with an attempt to determine what type of 'asset' a token might be so that the set of existing and known rules of Dutch property law may operate on the token in a system-consistent manner, which is a journey that will not be undertaken, at least, not in full.[1] Instead, this article seeks to highlight the different operative features of tokens and how these features conceptually interplay with property and property rights.

The threshold question is: when is a token an independent object of property, and when not? On a strict analysis, tokens are no more than cryptographically protected information in the form of a book-entry on a ledger maintained by a decentralized network of independent computer operators. Whilst information may be the subject of intellectual property rights, information *per se* would not be capable of being the object of property. However, because of the cryptographic techniques used to create the tokens, the information exists independently and is exclusively controlled and manipulated by the person who controls the relevant private key. Consequently, the package of cryptographically protected information that comprises the balance of the tokens that is allocated to a certain blockchain address, has acquired permanence and independence, which does render it capable, in principle, of being an object of property.

If tokens are capable of being the object of property, regular questions of property law need to be answered. For example, how does property law operate on tokens in terms of transfer requirements, how can tokens be used as collateral to secure payment and other obligations, how can secured creditors realize the collateral tokens, and how must the tokens be dealt with in the event of insolvency, death, or other change of status of the owner of the token. And what happens in the event of adverse or conflicting proprietary claims on the token?

Separately and independently, token technology can be used to record property interests in all manner of 'real world' assets. That raises questions about the relationship between the token as a record of ownership and the property interests in the 'tokenized' asset. Such questions are, for example, whether the digital transfer of a token would automatically imply the transfer of the tokenized asset. That may occur either because the token transfer mechanics fulfil the ordinary transfer requirements of the tokenized property interest, or because the token transfer supersedes the ordinary transfer requirements.

Tokenization of 'real world assets' such as real estate, IP rights, et cetera, holds unlimited potential for future applications. In principle, any asset could be tokenized, which means that the recording, transferring, and collateralization of ownership could potentially be simplified. That in turn could solve all kinds of real-world frictions, such as the cost of maintaining a reliable public record of ownership and the ease, efficiency, and effectiveness, including finality, of transfers. It also permits low-cost fractionalization of ownership. Reducing such frictions is likely to lead to a broader and more liquid market for certain assets, which in turn would yield economic benefits.

As noted, this article does not aim to provide the answer to all questions. Rather, the objective is to frame the questions in a technical context, hopefully permitting critical assessment of the subject matter and any attempts to deterministically determine the status of tokens under Dutch, or indeed, property laws of other jurisdictions. The article starts with a general introduction to cryptographic technology developments that have led to the creation of tokens and decentralized networks. Section 1 introduces the concepts of 'Web3' and 'blockchain' with its different infrastructure components, such as the 'ledger', 'nodes', 'keys' and 'protocols'. Section 2 looks at the ways

* Mr. L.D. van Setten is Director & General Counsel at Trilitech, London. Certain parts of this article were first published in Lodewijk van Setten, 'Cryptographic tokens: three categories of personal property?', *Butterworths Journal of International Banking and Financial Law* (Feb 2023), and Lodewijk van Setten 'Tokenisation of Financial Assets and Decentralised Finance', in *The Twin Transition: Digital & Sustainable Finance* (I. Palm-Steyerberg et al. (eds.), Kluwer 2022).

1 For a Dutch property law analysis of tokens that classify as cryptocurrency, in particular, bitcoins, see *e.g.* Y.S. Beerepoot, 'Blockchain unchained: gevolgen van blockchain en cryptocurrency voor de faillissementspraktijk', *TvI* 2018/34; J.L. Snijders & Y. Tonino, 'Goederenrechtelijke status van bitcoin (kapitaalkracht)', *FIP* 2018/314.

 doi: 10.5553/MvV/157457672023033006002

in which users interact with a blockchain and its decentralized network, introducing the concepts of 'wallets', 'blockchain addresses' and 'network transactions'. Section 3 discusses the role of 'smart contracts', essentially program code that can be deployed on a blockchain network and may be used to automate or facilitate transactions. Section 4 describes the creation and roles of 'tokens' in blockchain technology. Section 5 analyzes several key questions that must be answered to arrive at a property law framework for tokens and linked off-chain assets.

1. Web3: the basics

'Tokens' are internet-based creations, more specifically, creations on the internet configuration commonly referred to as 'Web3'. Most of us will have some familiarity with 'Web2' internet applications, such as internet banking, e-commerce websites, et cetera. Web3 is a new iteration, expanding the reach of cryptographic technology. Web1, Web2, and Web3 are terms used to describe different stages of the evolution of the internet. While it cannot be said that consensus persists on the meaning of the terms, at a very core level it may be maintained that 'Web1' intends to refer to the original internet use that consisted of static web pages with basic HTML content.[2] Web1 was not interactive. Internet users were mainly consuming content that was posted by 'gatekeepers', *i.e.* people with sufficient knowledge of how to operate a web page.

The next stage introduced asymmetric cryptography to the internet. It is a type of cryptography based on pairs of keys used for encryption and decryption. A message can be encrypted with the private key and can only be decrypted with the corresponding public key. Conversely, when a message is encrypted with the public key, only the corresponding private key can decrypt it. Asymmetric cryptography eliminates the need for a secure channel for private key exchange and allows the internet, an insecure network, to be used for secure communication via protocols such as HTTPS, SSL, and SSH. It enabled secure interactive web applications for commercial and financial services (*e.g.* mobile banking), social media (*e.g.* Facebook), and user-generated content (*e.g.* Twitter and Instagram) that have transformed the way people interact with each other via the internet, which is commonly referred to as 'Web2'.

'Web3' is taking asymmetric cryptography further to permit 'peer-to-peer' secure multilateral interactions among internet users. At the heart of the interactions sits a decentralized network of host computers, known as 'nodes', which facilitates the secure user activity. Pivotal in the Web3 space is blockchain technology, which enables decentralized network-based maintenance of a secure, publicly accessible transaction 'ledger'. The network can accept and validate transactions proposed by and executable between anyone with access to a blockchain address. The blockchain address is a unique publicly visible public key, a string of alphanumeric characters that is generated using a cryptographic algorithm, that can be utilized via the corresponding private key to interact with the network. Blockchain addresses, a user's public key, identify a user's account on the network,[3] but are not publicly linked to a user's identity. In other words, users can transact via the public network without revealing their identity.

Overall, blockchain technology allows users to record transactions in a secure and decentralized way, offering several advantages over traditional centralized systems. All sorts of applications are possible. For instance, blockchain enables secure and transparent peer-to-peer transactions without the need for intermediaries like banks. An important example is the blockchain and token known as 'bitcoin'. That facilitates digital payments, providing users with immediacy and transparency whilst reducing transaction fees. Blockchain's trusted golden source recording features could also be used to track the movement of goods across a supply chain, ensuring transparency, authenticity, and efficiency. The blockchain enables verification of the origin and quality of products, preventing counterfeiting and enhancing trust between participants. Each transaction or event can be recorded on the blockchain, providing an immutable audit trail. Blockchain technology can therefore be used in a range of different applications, not just for payment use cases. For instance, it could be used to protect intellectual property rights by registering creative works on the blockchain, creating an immutable, publicly accessible, verified record of ownership. This helps prevent unauthorized use and ensures proper attribution and compensation.

Typically, a reference to 'a blockchain' is a shorthand broad reference to all the components necessary to arrive at the output and distributed storage of transactions carried out via the validator network, the output being a transaction ledger created as a chain of cryptographically secured blocks that manifest as a journal of all the verified and accepted state transitions. This cryptographically protected transaction ledger is the actual 'blockchain'. It exists in distributed and immutable form, as the verified and accepted state of the blockchain cannot be changed. Each of the validator nodes has an identical copy of the verified and accepted state of that blockchain.

Critical to the Web3 designs is the notion of decentralization, which refers to the properties of the network of validator nodes that maintains the blockchain. A decentralized network architecture implies the absence of a central authority or point of control. Instead, control is distributed among the nodes in the network and decisions are made by the nodes cooperating in accordance with the network consensus protocol. As a result, decentralized networks, provided that enough independent nodes actively participate, are more resistant to censorship and are more resilient as there ought to be no single point of failure. If one or several validator nodes fail, the rest of the

2 For a more detailed overview of terminology and differences between the different generations, see *e.g.* T. Flew, *New Media: An Introduction*, 3rd edn, Oxford University Press 2008, p. 19.

3 Each blockchain network has its own unique address format and rules for creating and using addresses. For example, Bitcoin addresses start with '1' or '3', while Ethereum addresses start with '0x'.

network can still function and maintain its integrity.[4] A high number of independent and active validator nodes with meaningful geographic distribution normally indicates a good level of decentralization of the network.

In summary, a key benefit of internet-based permissionless blockchain technology is the ability of any internet user to effect the recording of a transaction at any time, automatically, at a low cost, securely, transparently, and without reliance on centralized intermediary intervention. Instead, the user relies on intervention by a decentralized network of independent validators, which significantly reduces the risk that anyone or a group of bad actors can censor the transaction, tamper with the data, or carry out fraudulent activities. Further, the decentralized nature of the blockchain protocol process and storage means that anyone with access to the internet can view all transactions in real-time, using software known as 'block explorers'. Block explorer software can offer visibility into transaction history, block information, and network statistics.

2. Wallets, blockchain addresses, and network transaction fees

To interact with a blockchain, users need software applications known as 'wallets'. Blockchain wallet software serves as a user interface and tool for interaction with blockchain networks. Wallet software connects to the respective blockchain network, either directly through a full node or by utilizing an external Application Programming Interface (API).[5] During the wallet creation process, a cryptographic key pair is generated: a public key and a private key. The public key is then transformed into a 'wallet address' through a process called hashing,[6] which is carried out and generated by the blockchain protocol on which the address is to be created. Users can generate as many new addresses as they need. This may for instance be done to improve privacy and security by creating a new address for each transaction or interaction with the blockchain protocol. The term 'wallet' is mildly misleading as it suggests that the software functions as a container of sorts, which it does not. In essence, it is password management software.

The address generated by the blockchain protocol is also called the 'public address' or the 'blockchain address'.[7] These terms appear to be more helpful than the term wallet address, as they accurately avoid a reference to the term 'wallet' and thus, to the suggestion that the address generated by the blockchain protocol is something that is part of the wallet software, rather than something that is part of the blockchain protocol code itself. As integral components, the blockchain addresses are specific to each blockchain network, and the format and encoding may vary between different blockchain networks. Notwithstanding, the operating principle that a unique address is generated through a cryptographic hash function from a public key is the same in each case.

The private key is needed to 'sign' transactions and access the wallet address. If a user signs and generates a transaction, the user will typically need to compensate the network and the validator who selects the transaction for addition to a block for the service. The compensation is paid in the form of the protocol token of the relevant blockchain protocol. The specifics of fee calculation, pricing, and resource allocation vary from protocol to protocol.

3. Smart contracts

The Bitcoin protocol is programmed only to create, store, and send a cryptographic token known as 'Bitcoin', and accordingly, the protocol functionality is limited to accepting, validating, and executing Bitcoin token transactions and updating the state machine operated by the Bitcoin network. The Ethereum protocol, building on the Bitcoin protocol designs, innovated by introducing the concept of a 'smart contract'. A smart contract is a self-executing program that contains code that is written to allow, when specified conditions are met, for the automation and execution of certain defined actions. Consequently, smart contracts eliminate the need for intermediaries or trusted third parties to enforce or carry out the programmed actions. They operate autonomously, automatically executing actions as programmed, which can increase efficiency, reduce costs, and minimize the potential for human error.[8]

4 A decentralized network must be distinguished from a distributed network, which denotes a network architecture based on the spreading of data and computing resources across different nodes. In a distributed network, each node is responsible for performing a specific task or set of tasks and the nodes communicate with each other to complete the overall task. A distributed network is designed to scale task performance and engineer higher fault-tolerance.

5 Web APIs use standard protocols such as HTTP to enable communication between web applications or mobile apps and remote servers. An API is a set of rules and protocols that allows different software applications to communicate and interact with each other, enabling the exchange of data and the performance of specific actions. It abstracts the underlying application and allows integration of the application with external services, libraries, or platforms. APIs promote modularity, reusability, and interoperability, permitting leverage of existing functionalities. API documentation usually provides details on how to use the API, including the available endpoints, input parameters, expected responses, and authentication mechanisms.

6 Hashing has numerous applications in computer science, cryptography, and data structures. Blockchain technology uses cryptographic hash functions to generate hash values for blocks, transactions, and other data. A hash function produces a hash value of a fixed size, regardless of the input size, allowing for efficient storage of hash values. Given the same input, a hash function will always produce the same hash value, whilst a small change in the input data will result in a completely different hash value. Conversely, the clever mathematics behind the hash function ensures that it should be computationally infeasible to determine the original input data from the hash value, making it extremely difficult to reverse-engineer the input.

7 Note that the term 'network address' generally refers to an IP address or a MAC address used in computer networking to identify a device on a network. It is used for communication between devices within a network infrastructure.

8 See for a helpful analysis of how a smart contract functions in a decentralized Web3 application, colloquially known as a 'dApp', B. Ramamurthy, *Blockchain in Action*, Manning Publications 2020, p. 22-29.

 doi: 10.5553/MvV/157457672023033006002

Smart contracts can, for instance, be used to automate insurance claims processing. The code could be programmed to settle a claim automatically when independently verifiable claim conditions have been fulfilled (*e.g.*, flight delays or adverse weather events). Similarly, smart contracts can automate and improve supply chain processes, such as inventory management and payment settlements. For example, when goods are delivered and verified by sensors or internet-of-things devices, the smart contract can automatically initiate the payment to the supplier, thus improving efficiency. The same applies for *e.g.* royalty payments.

Once the smart contract code is written, it is deployed on the blockchain network at its own blockchain address. When deployed successfully, the smart contract program becomes an immutable part of the blockchain and is replicated across all nodes in the network. The immutability of the program code means that it cannot be changed or updated unless it is programmed to give certain permission to an administrator. Smart contract operations rely on the security and consensus mechanisms of the relevant blockchain network.[9] The decentralized nature of the blockchain network ensures that the smart contract's operations are not controlled by any single party, significantly reducing execution and non-performance risks.

Smart contracts are activated only when they are 'called', which happens when a transaction involving the smart contract is initiated from a blockchain address. For instance, a blockchain address holder who wishes to acquire certain tokens from a smart contract can initiate a transaction, which, if completed without fault, would result in the smart contract recording a new balance of the acquired tokens for the address that initiated the transaction. The network operated state machine will be updated accordingly so that the transaction in question is immutably recorded as part of the blockchain record.

Like the term 'wallet', the term 'smart contract' presents as mildly confusing jargon. The deployed contract code *per se* does not normally create a legal relationship between certain parties. Also, the program is not 'smart' either. The code simply includes the logic that defines how the program functions, the actions that can be executed, and the conditions for those actions. For example, if a payment deadline specified in the code is reached, the smart contract program may automatically release the funds to the specified blockchain address of the intended recipient. Accordingly, the smart contract functions passively, not intelligently,[10] as a container that holds data and methods and executes deterministically in accordance with its program design.

4. Different ways of creating tokens

A smart contract can be used to create, record, and send cryptographic tokens. The smart contract defines the characteristics and properties of the token. Token smart contracts often also include contract ownership and access control mechanisms to manage token issuance and transfer. These mechanisms allocate permissions to create or mint new tokens and to transfer tokens between addresses. Once the contract is deployed, the token initialization process takes place. This usually involves setting initial parameters, including the total supply of tokens, assigning the token name and symbol, and allocating the initial token balances to specific addresses.

A token smart contract thus functions as a rights management tool, that is, it assigns permissions to the tokens, and so to the token holders. The token holder(s) is (are) the person(s) who control the blockchain address to which the token has been assigned by the token contract. The controller of an address who wishes to acquire or dispose of certain tokens supplied and administered by a smart contract can initiate a transaction, which, if completed without fault, results in the smart contract recording a new balance of the acquired tokens for the address that initiated the transaction. The network operated state machine will be updated accordingly so that the transaction in question is immutably recorded as part of the blockchain record.

Tokens supplied by a smart contract are also referred to as 'application tokens'. Application tokens must be distinguished from tokens supplied and administered by the blockchain protocol itself, such as Bitcoin or Ether. That type of token is typically referred to as a 'native token' or 'protocol token'. The protocol tokens are a critical component of the incentive scheme of the relevant blockchain protocol and balances are recorded as part of the blockchain address of the recipient of the protocol token. In case a protocol token is sent to a recipient's blockchain address, the state of that recipient's address changes as it will update the balance of protocol tokens recorded at that address. Application tokens, on the other hand, have moved one layer up in the technology stack. If an application token is sent to a recipient's address by the token contract, the state of the recipient's address does not change. Instead, the recipient's address is added to a map within the to-

9 Each blockchain protocol will have its own smart contract coding language and runtime environment. For instance, Ethereum introduced the 'Ethereum Virtual Machine' (EVM) and a programming language called Solidity as part of the smart contract innovation. The EVM is a runtime environment that enables the decentralized execution of smart contracts across the network of Ethereum nodes, ensuring consensus on contract outcomes and maintaining the blockchain state. Other blockchain protocols will use different virtual machines. *E.g.*, the Tezos blockchain uses a domain-specific programming language called Michelson that is specifically designed for Tezos smart contracts and operates a Michelson Virtual Machine (MVM). Michelson has its own syntax and features, distinct from the Solidity language used in Ethereum smart contracts. While the Michelson language and MVM are not directly compatible with Ethereum's Solidity and EVM, the Tezos protocol, through layer 1 and layer 2 upgrades, does provide interoperability solutions between the Tezos and the Ethereum ecosystems.

10 Although, inevitably, AI supported smart contracts will be developed that may eventually do justice to the name 'smart contract'.

ken contract itself and therefore, the transaction only changes the state of the token contract.[11]

In all cases, though, the reference to 'tokens' is a reference to an electronical record of a certain number of units or fractions of units that is associated with a certain network address, which electronic record can be manipulated, via the relevant network, only by the person or persons who control that address through its private key.

It should be noted that a 'token' does not exist independently, unless the balance allocated to a blockchain address is 1. This may be the case if only one unique token of a particular type and description has been created. Typically, however, tokens are created with a fungible supply of more than 1, in which case an address can show a balance comprising multiple tokens. For property law purposes, that balance of tokens would appear to be best described as a *confusio* because the recorded balance constitutes a single asset created out of the mixing of contributing elements. The balance of tokens should not be treated as a *commixtio* simply because individual receipts that contributed to the balance can be identified. Once the blockchain process results in the recording of a new balance of tokens at a certain address, the fungible units that make up that new balance have lost their individual integrity.

5. Tokens, tokenization, and property law

This section addresses certain legal questions surrounding the characterization of a token under principles of property law. The threshold question is whether a token is capable of being the object of property. The answer to that question may, or ought to, differ depending on the purpose for which a token is created and the way it is used. Tokens may exist *sui generis*, that is, they have no function outside the blockchain on which they are created. This type of token is commonly referred to as a 'function token'. Function tokens are protocol tokens and application tokens that are used only to facilitate the execution of a function within the relevant blockchain ecosystem, mostly to serve as a form of value transfer. Function tokens derive their economic value from their utility within the network. Prominent examples of function tokens are Bitcoin and Ether. Both are a form of protocol token that are typically also referred to as 'cryptocurrencies'.

Function tokens must be distinguished from tokens that are used to create records of ownership of property interests in all manner of 'real world', or 'off-chain' assets. Such tokens may be called 'asset tokens'. As noted above, at its core, a token is merely a cryptographically protected electronic record of a certain number of units or fractions of units that are allocated to a certain blockchain address. The recording functionality can be used to record interests in or rights in respect of tangible property such as commodities, or intangible property such as intellectual property rights. The process of creating ownership records relating to an off-chain asset by way of token issuance is commonly referred to as 'tokenization' of the relevant off-chain asset.

The reason why the answer to the threshold question may differ depending on whether a token is an asset token or a function token is that asset tokens relate to other assets, where function tokens do not. If an asset token, independently, were an object of property, the question must be answered how the token relates in property law terms to the asset to which that asset token is supposed to be linked. Logically, if the asset token itself is characterized as an independent object of property, there would then exist two assets, which are somehow meant to be intrinsically linked. One asset should ideally not be capable of being owned or transferred without the other asset simultaneously being owned or transferred. As the two assets are legally distinct and of a different type and description, it is, at least under general principles of property law, challenging to imagine facts and circumstances in which that symmetry could hold true. It raises the question, therefore, whether the asset token should indeed be characterized as an asset, or should it instead be characterized as a form of ownership record that can be amended by way of a token transfer process, which affects the status of the linked off-chain asset. The amendment of the ownership record would have the effect of transferring the asset to which the asset token is linked, not because the linked asset follows the token, but because the token transfer complies with transfer requirement applicable to the linked asset.

For instance, if the shares in private company were tokenized using a smart contract that creates application tokens that are intended to represent evidence of the tokenholder's title to the shares in that company, it would not be such a giant step to conclude that the smart contract constitutes the company's register of shareholders. A transfer of a token would require the transferring tokenholder to use their private key, which could constitute an electronic signature. The adoption by the blockchain network of the block that records the change state of the smart contract to the effect that the transferring tokenholder is entitled to a reduced number of tokens and the transferee to a correspondingly increased number of tokens could be concluded to constitute the written transfer instrument and the update of the smart contract could constitute notice to the company. The *lex societatis* will in many jurisdictions contain certain formal obstacles to smart contract-based shareholder registers, such as *e.g.* the requirement to produce paper share certificates. Whatever the statutory obstacles, these would not appear to be fundamental.

Notwithstanding, even if these obstacles are removed through statutory intervention that introduces the notions of blockchain powered shareholder registers and transfer instruments, the question whether the tokens are assets that are separate and independent from the shares as assets, or whether tokens

11 See A. Antonopoulos and G. Wood, *Mastering Ethereum – Building Smart Contracts and dApps*, O'Reilly 2018, p. 242.

 doi: 10.5553/MvV/157457672023033006002

are only a record-keeping and transferring mechanism, must still be answered.

In this context, it is instructive to note that a recent EU regulation that seeks to permit securities market infrastructure operators to use tokenization technology to facilitate securities settlements powered by distributed ledger technology,[12] also referred to as 'DLT', does not address the distinction between the token and the linked security at all. The DLT Regulation aims to allow for the testing of DLT market infrastructures that develop tokens that are linked to financial instruments. Article 2 of the DLT Regulation defines 'DLT Financial Instrument' as 'a financial instrument that is issued, recorded, transferred and stored using distributed ledger technology'. As a financial services regulation, one would not ordinarily expect the statutory instrument to intervene in domestic property laws. However, the conflation of the token and the financial instrument to which it is linked in the definition of DLT Financial Instrument is surprising. One would have expected at least some recognition of the distinction between the token and the financial instrument and maybe some direction on the expectation regarding the treatment of the DLT Financial Instrument as a composite of a token and an issued security. By ignoring that complexity and, in doing so, by framing regulatory asset safeguarding requirements by way of a broad reference to the need to safeguard the compound, i.e. the DLT Financial Instrument,[13] the DLT Regulation stores a lot of uncertainty about how a tokenization structure can be compliant with the DLT Regulation.

Contrary to the DLT Regulation, the 2022 Amendment to the Uniform Commercial Code (UCC) proposed by the American Law Institute and the Uniform Law Commission is very specifically focussed on the transfer of property rights in a 'controllable electronic record', a 'CER', such as a cryptographic token. Through the definition of a CER, the legislation excludes any digital assets that are not subject to 'control' and those that are already subject to other commercial laws, including other parts of the UCC. The UCC steers clear of reforming common principles of property law and confines itself to removing uncertainty around enforceability of transfers of the token itself, including the taking of security, known as collateralization. The rules of the new Article 12 UCC specifically take the distinction between function tokens and asset tokens into account. The Prefatory Note to Article 12 observes:

> 'The adoption of DLT has underscored two important trends in electronic commerce. First, people have begun to assign economic value to some electronic records that bear no relationship to extrinsic rights and interests. For example, without any law or legally enforceable agreement, people around the world have agreed to treat virtual currencies such as bitcoin (or, more precisely "transaction outputs" generated by the Bitcoin protocol) as a medium of exchange and store of value. Second, people are using the creation or transfer of electronic records to transfer rights to receive payment, rights to receive performance of other obligations (e.g., services or delivery of goods), and other rights and interests in personal and real property.
>
> These trends will inevitably result in disputes among claimants to electronic records and their related rights and other benefits. Uncertainty as to the criteria for resolving these claims creates commercial risk. The magnitude of these risks will grow as these trends continue.'

Section 12-104 of Article 12 UCC makes tokens negotiable, in the sense that a qualifying good faith purchaser for value could take a token free of third-party claims of a property interests, known as the 'take-free rule'. The Official Comment to Section 12-104 notes that where a token is 'tethered' to another asset, for example, goods or rights to payment, one might argue that by taking an asset token free of property claims under the take-free rule, one takes not only the asset token itself but also all rights that are 'carried' in the asset token free and clear. However, negotiability, the take-free rule is explicitly limited so that it does not extend to property interests in any asset linked to that asset token. Subsection 12-104(f) restricts the application of the take-free rule to the asset token itself only. Therefore, the transferee takes rights to payment, rights to performance, and interests in property that are evidenced by the asset token subject to third-party property claims, unless law other than Article 12 UCC provides to the contrary.

However, Article 12 UCC does not answer all the questions arising as a matter of property law. Importantly, it leaves the transfer requirements that apply to the transfer of the token, or indeed in case of an asset token, whether the tethered asset is transferred by the transfer of the asset token in the absence of third-party property claims, to be determined separately. Section 12-104(c) provides that law other than the rules of Article 12 'determines whether a person acquires a right in a controllable electronic record and the right the person acquires'.

The objective of asset tokens is to trade, transfer, and store fractional ownership rights in the linked off-chain asset as tokens on the blockchain, providing benefits, apart from fractional ownership, such as increased liquidity, simplified trans-

12 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU ('DLT Regulation').

13 See, *e.g.*, Art. 7(5) of the DLT Regulation, which provides, among other matters, that 'Operators of DLT market infrastructure shall segregate the funds, collateral and DLT financial instruments of the members, participants, issuers or clients using the DLT market infrastructure, and the means of access to such assets, from those of the operator as well as from those of other members, participants, issuers and clients'. It is not clear whether this means the asset tokens need to be segregated, the underlying security, or both. Presumably, both.

ferability as well as transparency and traceability using blockchain technology. The technique for establishing the legal link between an asset token and an off-chain asset varies depending on the jurisdiction and the nature of the asset being tokenized. For instance, a token may be issued to evidence that the token holder has the benefit of the license to an intellectual property right in creative content, *e.g*. digital art. In essence, that involves creating a direct contractual agreement between the issuer and each token holder separately, through an open offer made by the issuer. In English law, the principle that a person may validly and effectively offer to contract with any person who cares to fulfil the obligations specified in that offer was established in *Carlill v. Carbolic Smoke Ball Company*.[14] The owner of the intellectual property rights in the digital art could, for example, offer a licence to any person who agrees to a transaction resulting in the transfer of tokens to that person. If the token is an NFT, the meta data of that NFT can specify the terms of the licence, including, for instance, the obligation to pay a royalty to a specified blockchain address. On normal contractual principles of English law, agreement to the transaction on those terms would amount to acceptance of the offer and, provided there was an intention to create legal relations, this will result in a binding contract between the issuer and the transferee token holder.

If the off-chain asset must be held in some form, *e.g*. in the case of registered property, physical property, or an account-based asset such as securities or bank money, a special purpose vehicle can be appointed to hold the asset for the benefit of the asset token holders subject to an escrow or trust or some other form of undertaking. This entity acts as an intermediary holder and ensures the proper custody and management of the asset. The legal link is established through the legal relationship between the intermediary entity and the token holders. Sometimes, this is done through tokenization of the shares in the special purpose vehicle. But it may also be achieved through tokenization of the contractual or other claims against the issuing vehicle. In each case, the token contract essentially functions as the share/claim holder register. The set-up would have to be structured so that it will comply with the applicable company law or the applicable contract law. That will typically require the 'permissioning' of blockchain addresses, meaning identification of the holders/controllers of each address that will be the recipient of a token that represents the share or claim against the issuing intermediary entity. The permissioning of an address at blockchain level will be carried out via a separate smart contract – a permissioning contract – that will communicate with the token contract and confirm that an address is permissioned or that permission has been revoked.

Many of the potential efficiency gains of tokenization are dependent on the possibility that upon transfer of an asset token the rights or interests associated with it, *i.e*. the linked asset, might simultaneously and automatically be transferred, without the need for further act or formality. English law illustrates how that may be achieved without treating the asset tokens itself as the object of property. In English law, the legal mechanism whereby the holder of a legal right or interest in an asset is identified by reference to a token is called 'stapling'.[15] In case of stapling, the token, or indeed any other reference digital record of property or ledger record, would not itself be an object of property in the case of registered or similar structures. Where rights or interests are stapled to a ledger, such as a token, the required result is that the rights or interests are transferred to the person in whose favour the securities are recorded on the relevant ledger. If the ledger is a blockchain record that person would be the holder from time to time of the relevant token.[16] If the tokenization token were itself the object of property, the reference asset would be stapled to the token, which would transform the reference asset so that it is embedded in the token and ceases to be the object of property in its own right. This might be feasible in the case of a reference asset that is capable of being embedded into a bearer instrument, such as *e.g*. a bond. On the whole, however, it must be assumed that tokenization technique must be characterized as the stapling of rights or interests to the token as a ledger record so that the result is that the rights or interests can be transferred by way of transfer of the token so that the new holder is recognized as the person in whose favour the rights or interests are recorded on the relevant ledger. In other words, in the case of tokenization of registered assets, the asset token would be a mere record of ownership and would not itself be the subject of property rights.

The category of tokens that are not linked to off-chain assets – function tokens – consists of protocol tokens such as Bitcoin and Ether and application tokens that are 'on-chain' utility tokens only. Protocol tokens are used as a medium of exchange within the relevant blockchain' ecosystem and permit participation in the operation and governance of the relevant blockchain network. They may be required to pay transaction fees for activities, such as staking, block validation, consensus mechanisms, and may also be used for voting on protocol upgrades. Protocol tokens enable economic activity within the ecosystem. Application tokens that are utility tokens, , are primarily as the name suggests, designed to provide utility or access to a specific product, service, or platform.

Where property law questions concerning asset tokens can be addressed based on the characterization of the reference asset using well-established principles, property law questions in relation to function tokens are challenging as they must be answered by characterizing the function token as an asset of some type and description. Although the on-chain environment regarding the transfer, et cetera of function tokens will

14 [1893] 1 QB 256. See on this topic, UK Jurisdiction Taskforce of LawTech UK (UKJT*), Legal Statement on the issuance and transfer of digital securities under English private law* (Feb 2023), paras 101-103.

15 See UK Jurisdiction Taskforce of LawTech UK (UKJT*)*, nt 18, para. 84.

16 *Ibid*., paras 86-87.

 doi: 10.5553/MvV/157457672023033006002

be well-defined by the core protocol and/or the smart contract code, off-chain there may still be questions between the sender, the recipient, and potential third parties who may have an adverse claim based on fraud, breach of trust or other fiduciary duty, et cetera. Also, principles of property law will need to operate on function tokens if the owner of the function token is bankrupted or liquidated, or indeed, deceased.[17]

To arrive at the conclusion under Dutch law that a token is an object of property, the concept of a token would need to be reconciled with the definition of the concept of 'assets' (*goederen*) set out in the Dutch Civil Code. The Civil Code conceptually divides 'assets', that is objects of property, into (1) tangible objects that are capable of being controlled by humans (*zaak*) and (2) transferable rights or rights that aim to provide the holder with economic benefits, or that have been obtained in exchange for economic benefits (*vermogensrecht*). The blockchain network is not a person against whom or which a right can or even needs to be enforced. Enforcement of any entitlement to a function token, as against the network, is exercised *de facto*, not *de jure*, via the private key. A function token is an object capable of being controlled by a human, so it corresponds to the core of the definition of a *zaak*. A function token, however, *prima facie* is not tangible and could therefore not be a *zaak*, at least not technically, unless the courts would reinterpret the word tangible (*stoffelijk*) in the context of the Civil Code to include controlled records such as function tokens that are provided by a decentralized network of nodes. The network of nodes is most certainly tangible. It may be argued, perhaps, although perhaps not a claim (*vorderingsrecht*), that the token is a *vermogensrecht* nevertheless on grounds that it is a transferable interest – a *recht* – in the controlled cryptographic record that provides the holder with an economic benefit. However, if that is true, Article 3:83(3) of the Dutch Civil Code may prevent transferability of that interest in the absence of specific legislation.[18] Should, somehow, the interest in the token be treated as a *vorderingsrecht* for purposes of the Dutch law transfer requirements, it is not inconceivable that the requirements of Article 3:94(1) of the Dutch Civil Code, if applicable by reason of analogy, could be considered to have been complied with in case of a token transfer if it is accepted that (i) the smart contract action recorded as part of a block on the blockchain serves as the transfer instrument (*akte*) and (ii) the public recording of the block could serve as the requisite notice. Having said that, it seems unavoidable that some legislative intervention is required to support that outcome.

The common law jurisdictions experience fewer formal obstacles to the application of existing principles of property law to function tokens. The traditional restatement of the legal classification of objects as personal property in English law is that of Fry LJ in *Colonial Bank v. Whinney*, where he said: 'All personal things are either in possession or action. The law knows no tertium quid between the two'.[19] Conceptually, a token cannot be characterized as an intangible right of action as the blockchain network is not a person against whom or which a right can be exercised, unless one would wish to indulge in theories involving constructive partnerships or multi-party agreements, which would appear to be at risk of stretching technical and economic reality. No participating node in the network agrees or commits to anything with anyone. It merely downloads the blockchain protocols and uses that for its own benefit without obligation to anyone, not even the user whose transaction is added to a block and who must pay the transaction fee. The absence of a legal relationship between the nodes or indeed, between a node that selects a transaction from the mempool for addition to the next block and the user, therefore, seems quite plain.[20]

An argument could perhaps be made that the token is capable of possession via possession of the private key and, therefore, should be treated as a chose in possession. It would, indeed, seem unsatisfactory to limit the notion of possession to tangible assets, which is an argument made recently by the Law Commission in relation to electronic trade documents.[21] Notwithstanding, as the law stands, the point made by Fry LJ in *Colonial Bank* presents a doctrinal conundrum in relation to the classification of cryptographic tokens as personal property.

Bryan J faced this conundrum in the context of Bitcoin tokens in *AA v. Persons Unknown, Re Bitcoin* [2019],[22] but dismissed it, saying that 'it is fallacious to proceed on the basis that the English law of property recognises no forms of property other than choses in possession and choses in action'. He cited the observations of the UK Jurisdictional Task Force (UKJT) in a paper published in November 2019, *Legal statement on crypto assets and smart contracts*, and concluded that 'for the reasons identified in the [UKJT] legal statement, I consider that a crypto asset such as Bitcoin are property. They meet the four criteria set out in Lord Wilberforce's classic definition of property in National Provincial Bank v Ainsworth [1965] 1 AC 1175 as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having

17 See D. Fox, 'Cryptocurrencies in the common law of property', in D. Fox and S. Green, *Cryptocurrencies in public and private law*, Oxford 2019, p. 6.01-6.07.

18 Art. 3:84(3) provides: '*Alle andere rechten zijn slechts overdraagbaar, wanneer de wet dit bepaalt*'.

19 *Colonial Bank v. Whinney* (1885) LR 30 Ch 261, 285-86, adopted (1886) LR 11 App Cas 426 (HL).

20 See also the 'Initial VAT reflections on non-fungible tokens', observations of the Value Added Tax Committee (Art. 398 Of Directive 2006/112/Ec), *Question Concerning The Application of EU Vat Provisions* (Working Paper No 1060), 10 ('However, identifying the existence of a direct link between the gas fee paid and the publication on the digital ledger is not straightforward due to the difficulty in establishing the existence of a legal relationship between the one requesting minting to be done and the network validators involved in the said publication.')

21 Law Commission, *Electronic trade documents: Report and Bill* (Law Com No 405, February 2022), 7.3.

22 *AA v. Persons Unknown, Re Bitcoin* [2019] EWHC 3556 (Comm), 55.

some degree of permanence'.[23] Accordingly, function tokens can be personal property under English law.[24]

Courts in the common law world globally have generally unreservedly recognized that at least certain function tokens are capable of being the subject of property rights. Perhaps, the intellectual distinction between a data object and things in action or indeed a thing in possession is a red herring, as Justice Gendall observed more generally in *Ruscoe v. Cryptopia Ltd (In liquidation)*, a New Zealand case, in relation to the idea that a token must necessarily fall into one of the two categories of personal property to attract property rights.[25] Bryan J, in *AA v. Persons Unknown*, was not detained for long on the dogmatic distinction between choses in action and choses made in *Colonial Bank v. Whinney* and applied Lord Wilberforce's classic definition of property effectively and efficiently without much ado.

Traditional notions of objects of property did not contemplate intangible objects that operate in many respects as tangible. It may be concluded that modern property law can conceptually incorporate function tokens into the system, all be it that civil law systems appear to be constrained dogmatically by historical definitional precision predicated on a desire to categorize different forms of property with deterministic detail, whereas common law systems appear to be dogmatically less hemmed in, thus allowing intellectual flexibility to fit new forms of economic value into the existing law of property. However, even where the courts determine that function tokens are objects of property, it still leaves difficult questions to be answered such as the role of transfer formalities, if any, and perfection of security interests. The Law Commission has sought to address the conundrum in relation to English law in a July 2022 Consultation Paper.[26] The Law Commission proposes to introduce a new category of personal property, but this may cause more uncertainty than that it reduces.[27] Statutory intervention can be effective and welcome if done surgically and may in the case of function tokens be in the interest of legal certainty.

23 *Ibid*., 59.

24 Similar conclusions were reached regarding NFTs by the court in *Osbourne v. (1) Persons Unknown and (2) Ozone Networks Inc trading as Opensea*, [2022] EWHC 1021 (Comm), observing also that several cases had consistently held that crypto assets are to be treated as located at the place where the owner of them is domiciled.

25 [2020] NZHC 728, [2020] 22 ITELR 925 at [69].

26 Law Commission, *Digital Assets: Consultation paper* (Law Com No 256, 28 July 2022), p. 4.94 (The Consultation Paper reviews the taxonomies of the notions of things in possession and things in action and concludes, provisionally, as certain digital assets do not fall neatly within either category, that 'the law of England and Wales should explicitly recognise a third category of personal property to allow for a nuanced and idiosyncratic approach to the legal characterisation of new things'.).

27 *Ibid*., p. 5.10 (The Consultation Paper introduces the term 'data object' as an 'overarching descriptive term for objects that fall within our proposed third category of personal property', which a thing does if: '(1) it is composed of data represented in an electronic medium, including in the form of computer code, electronic, digital or analogue signals; (2) it exists independently of persons and exists independently of the legal system; and (3) it is rivalrous').

 doi: 10.5553/MvV/157457672023033006002