DIGITAL ASSETS (SCOTLAND) BILL

EXPLANATORY NOTES

INTRODUCTION

1. As required under Rule 9.3.2A of the Parliament's Standing Orders, these Explanatory Notes are published to accompany the Digital Assets (Scotland) Bill, introduced in the Scottish Parliament on 30 September 2025.

2. The following other accompanying documents are published separately:

- a Financial Memorandum (SP Bill 75–FM);
- a Policy Memorandum (SP Bill 75–PM);
- a Delegated Powers Memorandum (SP Bill 75–DPM);
- statements on legislative competence made by the Presiding Officer and the Scottish Government (SP Bill 75–LC).

3. These Explanatory Notes have been prepared by the Scottish Government in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by the Parliament.

4. The Notes should be read in conjunction with the Bill. They are not, and are not meant to be, a comprehensive description of the Bill. So where a section, or a part of a section, does not seem to require any explanation or comment, none is given.

OVERVIEW OF THE BILL AND GENERAL NOTES

Overview

5. The Bill confirms how Scots law applies in relation to certain digital things as objects of property. It is structured as follows:

- section 1 describes the digital things with which the Bill is concerned, labelling them "digital assets";
- sections 2 to 4 deal with the law's treatment of digital assets;
- section 5 defines what the preceding sections mean by "exclusive control" of a digital asset, and creates a rebuttable presumption that anyone with control of a digital asset has it exclusively;
- sections 6 to 9 are formal provisions of the kind found at the end of all Bills.

Interpretation of the Bill

6. The Bill falls to be interpreted in accordance with the Interpretation and Legislative Reform (Scotland) Act 2010.

Crown application

7. Section 20 of the Interpretation and Legislative Reform (Scotland) Act 2010 provides that the Crown will be bound by an Act of the Scottish Parliament or Scottish statutory instrument unless the provision expressly exempts it. The Act this Bill will become if enacted will apply to the Crown in the same way as it applies to everyone else.

References in these notes to particular technologies etc.

8. In order to explain the Bill, in places these notes describe how the Bill's provisions work by reference to particular existing technologies (such as Bitcoin and Ethereum). It is hoped that grounding the notes in real-world examples in this way will assist readers in understanding how the legislative principles, which are necessarily expressed at a relatively high level of abstraction in the Bill, will operate in practice. It is, however, important to be clear that whether and how the Bill's provisions operate as a matter of law in relation to any given technology can only be decided by a court. Therefore, while these notes discuss (for example) how the definition of "digital asset" could be applied to comprehend a bitcoin on the basis of the authors' understanding of how Bitcoin operates, it should not be inferred that the courts necessarily will, and for all time, recognise a bitcoin as being a "digital asset" within the meaning of section 1.

Glossary of technological terms

9. The following is a limited glossary of technological terms used in these notes. It is not intended to be a comprehensive explainer of digital technologies. Readers will find online many free explainers of the technologies mentioned in these notes describing them at different levels of technical depth.

Term	Meaning
Bitcoin (with capital 'B')	The Bitcoin network or system, the first major public, permissionless crypto-token system that uses blockchain technology to securely manage the issuing of, and transactions with, its cryptocurrency (i.e. bitcoin).
bitcoin (with lowercase 'b')	The native cryptocurrency manifested by the Bitcoin system.

Term	Meaning
blockchain	A type of distributed ledger technology in which changes to the ledger (transactions) are recorded in data structures called blocks. Each block is chronologically linked (chained) to the preceding block cryptographically which makes the ledger resistant to tampering because the computers on the network comprising the blockchain use a consensus mechanism to ensure each block is correctly linked to the one before.
cryptocurrency	A token manifested by a distributed ledger technology which is treated as a medium of exchange and a store of value.
distributed ledger technology	A way of connecting computers (referred to as nodes) so that each maintains a shared and synchronised set of records (referred to as a ledger).
ether	The native cryptocurrency manifested by the Ethereum system.
Ethereum	The Ethereum system is a public, permissionless blockchain system.
Ethereum Virtual Machine (EVM)	A computation engine running on the computers (nodes) that comprise an EVM-compatible blockchain (of which Ethereum is only one example) which is used to execute smart contracts.
non-fungible token (NFT)	Fungibility is a quality of things that describes parties' willingness to treat things of a similar kind as interchangeable (for example, a pound coin is highly fungible because people are generally willing to swap one pound coin for another, whereas portrait paintings of different people are typically non-fungible because someone attached to a particular painting will usually not be willing to swap it for any other painting). A non-fungible token is a token manifested by distributed ledger technology which is not generally regarded as interchangeable with any other token of the same kind (for example, bitcoins like pound coins are highly fungible and so could be characterised as a fungible token, whereas a Bored Ape (see paragraphs 22 and 23 below) is not fungible and so would be characterised as a non-fungible token).

Term	Meaning
private key	An alphanumeric code that is used as a password allowing the user to carry out transactions within a blockchain system in relation to tokens manifested by that system and which are associated by the system with the public address to which the private key corresponds.
public address	A cryptographic code that is mathematically derived from a private key in a way that renders it impossible (with current technology) to reverse the process so as to derive the private key from the public address. This means that a public address can be shared openly as the "location" at which the holder of the private key for the address wishes to receive digital assets.
satoshi	The smallest unit of bitcoin (as pennies are to pounds, but it takes 100,000,000 satoshis to make up 1 bitcoin).
smart contract	A self-executing computer program that is stored on a blockchain and automates actions on the blockchain when conditions written into the program are met.

BACKGROUND ON THE LAW OF PROPERTY

10. In Scots law, property (things) are classified in two different ways. In the first place, all things are either corporeal or incorporeal. In the second place, all things are either heritable or moveable. Corporeal things are physically tangible (like a book or a car). Incorporeal things are generally rights and have no physical presence (such as a right arising from a contract). The distinction between heritable things and moveable things is more complex but, for present purposes, the criterion for distinguishing between the two is whether the property consists of rights in or over land. If it does relate to rights in or over land then it is heritable (i.e. immoveable) property. Anything else (with a couple of discrete exceptions such as pensions and annuities) is moveable property.

11. Occasionally, new "things" come into being that, for one reason or another, might not seem to sit comfortably in the existing classification of things as property in law. Digital technologies may be considered to cast up many new kinds of thing. These putative new "things" range from traditional files (like images and documents) to more complex blockchain-based things like cryptocurrencies and non-fungible tokens (NFTs). Whether and how these "things" are to be treated, in law, as property is a matter of policy.

THE BILL

Section 1 – Meaning of digital asset

Purpose of section 1

12. Section 1 sets out what a digital asset is for the purposes of the Bill. As a matter of ordinary language, the term "digital asset" could be said to encompass all manner of things which are digital (such as text files on a computer, photos on someone's phone or data stored in highly sophisticated and cryptographically protected distributed ledger systems). Section 1 limits what counts as a "digital asset" for the Bill's purposes to a subset of the things that could, in general terms, be described as assets which are digital.

A thing arising from an electronic system

13. The first point made by the definition in section 1 is that a "digital asset", for the Bill's purposes, is a thing that arises from an electronic system. This means that the "thing" that is the digital asset is not merely some configuration of electrons on a network at a given point in time, it is the conceptual thing which humans believe that electronic network manifests (for example a bitcoin or a non-fungible token). To borrow the language of the Law Commission for England and Wales in its 2023 report on digital assets, the sort of "thing" that the Bill means by digital assets are:

> "notional quantity units, arising from a composite of technical form, technical function and social participation/recognition, that the market and the legal system treat as a thing, and to which society has chosen to attach legal consequences."[1]

14. It is not the digital asset per se that is electronic (or digital) in nature, what must be electronic in nature is the system that gives rise to the thing.

Made rivalrous by an electronic system

15. It is not the case, however, that every electronic or digital system (even if can be said to give rise to notional things) can give rise to a digital asset within the meaning of section 1. The second point made by the definition is that for something to be a digital asset as defined the electronic system giving rise to it must make it rivalrous.

16. What is meant by a system making an asset rivalrous is set out in section 1(2). At a high level, what is meant is that the system has to solve the "double-spend problem". A difficulty with treating digitally stored information, such as a text file or a jpeg image, as an object of property rights is that the file is just information and therefore infinitely replicable. If person A gives person B a copy of a jpeg photograph of a coin, person A's original jpeg of the coin is not destroyed. Person A and person B both end up with identical jpegs of the coin and this replication of the data can carry on infinitely. This is unlike the position if person A had given person B a physical coin. In that case, person A's spending the coin by giving it to person B would mean person A no longer had it and so could not spend it again. A physical coin can therefore be said to be rivalrous. In order for the Bill to recognise a notional digital coin as a "digital asset", the electronic system giving rise to it must ensure that the digital coin, like its physical counterpart, cannot be spent and

[1] Law Commission, *Digital assets: Final report* (Law Com No 412, 2023).

spent again infinitely by the same person. Thus section 1(2) states that the system must, by reference to an immutable record of transactions, ensure that a person's use of the notional thing within the electronic system in a certain way results in the person losing the ability to use it again in the same way (just as person A's using a physical coin by giving it to person B prevents person A from then giving the same coin to person C).

17. Solving this "double-spend problem" is one of the key breakthroughs of blockchain technologies. It is what makes the fungible and non-fungible tokens they manifest fit to be the subjects of property rights. But it is important to note that section 1(2) is not necessarily only describing tokens arising from blockchain-based systems, nor will every token built on blockchain technology necessarily be a digital asset within the meaning of the Bill. Section 1(2) is technology neutral in that it describes the result that a technological system must achieve if it is to give rise to digital assets for the Bill's purposes; whether a given system of whatever kind achieves the required result is a matter of fact which will ultimately be determined by the courts.

18. Section 1(2) requires that the system use an immutable record of transactions in order to render the notional things that it manifests rivalrous. The significance of this insistence on the immutability of the system's record is that it distinguishes systems in which no actor has the technical ability to tamper with the record (which is the case with, for example, a blockchain system where each block is cryptographically linked to the one before) from more conventional systems that may create a complete record of transactions but can, at least in principle, be altered by the person in control of the system. For example, a cloud services company might provide a system for its users that allows them to create documents stored on the company's servers and to manage permissions in relation to them such as who can view or edit the documents. The company's servers might keep a comprehensive record of every operation (or transaction) that users have performed in relation to each of those documents. Supposing, for the sake of argument, that the recorded data for each document could be said to make the documents notional things that have their basis in the electronic system, and further supposing that the company's record of operations on the documents is used by the system to control who can carry out further operations on a given document, without the stipulation about the record having to be immutable those documents could potentially be thought to fall within section 1's definition of digital assets. The documents will not be digital assets for the Bill's purposes, however, if (as is usual with such services) the company's record of operations in relation to the documents is not secured in a way that prevents the company from making alterations to the historical record of operations in relation to the documents. To be recognised as such under section 1, a digital asset cannot arise from an electronic system if its record of transactions is mutable.

19. In describing how an electronic system has to solve the double-spend problem, section 1(2) refers to transacting in relation to a digital asset "in a certain way" being the cause of the transactor losing the ability to use the asset again in the same way. Some electronic systems only allow for the digital assets to which they give rise to be transacted with in one way. There is, for example, nothing that can be done with a bitcoin within the system giving rise to it besides transferring it. However, for other types of digital asset there may be multiple ways in which they can be used within the system, some of which may not result in the user losing some or all of the ability to use the asset again in the same way. For example, a governance token might allow a user to cast a vote through a smart contract on some decision facing an organisation. Using the token in the system to cast the vote may not destroy the token; the user may be able to use the token in relation to other smart contracts to vote on other decisions facing the organisation. If, however, the user can also

transfer the token to another user in the system so that the transferor can no longer use it then, notwithstanding that there is one way of using the token in the system that does not result in the user losing the ability to use it again, it can nevertheless qualify as a digital asset for the Bill's purposes because there is at least one other way of using it in the system that does have that effect.

Illustrations of things being made rivalrous by electronic systems

Example 1: UTXO-based blockchain systems (e.g. Bitcoin)

20. The application of section 1(2) in relation to UTXO-based systems (such as Bitcoin) merits some further elaboration. In such systems, what is recorded permanently in the blockchain's ledger are unspent transaction outputs (these are referred to as UTXOs). In the case of the Bitcoin system, a UTXO represents a certain quantity of bitcoin (denominated in the smaller unit called satoshi). The blockchain records a UTXO as being at a certain public address, which means that a person with the cryptographically linked private key for that public address can use the UTXO, and by implication the satoshi it represents, as a transaction input. If person A has a UTXO representing 5 satoshi and wishes to transfer 5 satoshi to person B, person A uses that UTXO as a transaction input and the transaction's output is a new UTXO recorded in the ledger as representing 5 satoshi at a public address linked to person B's private key. As person A's UTXO is now recorded as having been used as a transaction input, it cannot be used again as a transaction input. In the language of section 1(2), it can be said that by having carried out the transaction in relation to the notional things that are the 5 satoshi, person A has lost the ability to transact with them again.

21. Suppose, on the other hand, that person A wanted to transfer 5 satoshi to person C but only had the private key to a live UTXO worth 10 satoshi. The 10-satoshi UTXO is used as the transaction input, and therefore becomes unusable again, and the transaction outputs are two new UTXOs recorded to the ledger: one, worth 5 satoshi, recorded as being at a public address linked to person C's private key, and the other (also worth 5 satoshi, representing person A's "change") recorded as being at a public address linked to person A's private key. In this scenario, by carrying out a transaction in relation to the notional things that are the 10 satoshi, one could take the view that person A has only lost the ability to carry out a further transaction in relation to 5 of them, having received in change from the transaction a new live UTXO worth 5 satoshi. It might be thought that this means it cannot be said that this transaction has, in section 1(2)'s terms, resulted in person A losing the ability to carry out the same transaction again with 5 of the satoshi used in carrying out the first transaction. That thought supposes that one has to view the 5 satoshi returned as change from the transaction as 5 of the same satoshi that formed part of the 10 used as the transaction input. One need not take that view. The alternative view is that the 5 satoshi returned in change are distinct from the ones used as inputs to the transaction, in the same way as if someone pays with a £10 note and gets a £5 note back in change, the £5 note is a completely distinct thing from the £10 note. Even if, however, one does take the view that the 5 satoshi returned to person A as a transaction's output are 5 of the same satoshi as were used as the transaction's input, the fact that there are some ways of transacting with satoshi within the Bitcoin system that can be said not to result in the transactor losing the ability to transact with them again does not mean that the Bitcoin system as a whole fails to render satoshi (or the bitcoin they comprise) rivalrous as there are other ways of structuring a transaction within the system that more obviously would have that result.

Example 2: Non-fungible tokens (NFTs)

22. In the context of digital assets, an NFT differs from a fungible token (such as a bitcoin) in that whereas one bitcoin will generally be accepted as entirely interchangeable with another, system participants tend to see each NFT as a unique thing. For example, Bored Ape Yacht Club (or Bored Apes) are a popular form of NFT. Each Bored Ape is a unique cartoon ape and thus many users will not feel that one cartoon ape is just the same as any other.

23. A smart contract running on the Ethereum system handles the recording on the blockchain of which account owns a given Bored Ape by mapping the current owner's address to the token ID of the Bored Ape. When one user wishes to transfer a Bored Ape to another, a transaction is carried out on the Ethereum Virtual Machine using a function of the smart contract's rules, which creates a transaction record on the blockchain as part of the smart contract's state that records that the mapping of the owner's address has been updated to point to the address of the transferee's account. In terms of section 1(2), the system has updated its immutable ledger to ensure that the transferee is now recognised by the system as the owner of the Bored Ape and the transferor is not and, because the transferor is not, the transferor cannot carry out another transaction of the same kind (i.e. a transfer) in relation to that Bored Ape.

Must exist independently from the legal system

24. The third point made by section 1 is that for a notional thing to be a digital asset for the Bill's purposes it must exist independently from the legal system. The purpose of this stipulation is to distinguish digital assets from other forms of incorporeal property, such as legal rights and their correlative obligations. A debt obligation, for example, cannot be said to exist independently from the legal system because it is inherently an obligation that exists because the legal system recognises its existence. If the legal system stopped recognising the debt's existence, the debt would effectively cease to exist. It is a notional thing created purely by the legal system. In contrast, the existence of a digital asset, as defined, is not dependent on its recognition by the legal system in this way. This point, that a thing must be independent from the legal system in order to be a digital asset, is probably implicit in the proposition that to be a digital asset the thing must arise from an electronic system. Cryptocurrencies, non-fungible tokens and so forth can exist, and indeed have existed, as notional things on the basis of their manifestation by electronic systems regardless of whether or not their existence is recognised by any legal system.

25. It may be that some digital assets become tokenised as representations of legal rights, which is to say that it may come to be accepted that transferring a certain kind of digital asset will be treated as an effective proxy for transferring the legal right that is "stapled" to it. Tokenisation of digital assets is a new form of an old idea in the law. Traditional negotiable instruments use pieces of paper as proxies for debt obligations. The fact that a class of notional things arising from electronic systems have been tokenised to represent legal rights does not mean that those things can no longer to be said to exist independently from the legal system, just as a piece of paper being used as a negotiable instrument would still exist as a piece of paper even if the law stopped recognising it as a token representing a legal right. For the avoidance of doubt, the Bill has nothing to say about whether and how digital assets can be tokenised.

Section 2 – Nature of digital assets in Scots law

26. Section 2 provides that digital assets are incorporeal moveables for the purposes of Scots law. It further states expressly the natural implication of that, which is that the law is generally to apply to them on that basis. However, the latter point is qualified in two ways.

27. First, the law is to apply to digital assets on the basis of their being incorporeal moveables only insofar as that is consistent with their nature. This underscores that in developing the law's treatment of this new type of thing the courts can depart from the general principle that the law is to treat them like other incorporeal moveables if the courts find that unworkable or inappropriate in any particular regard as a result of their novel features.

28. Second, the law's application to digital assets on the basis of their being incorporeal moveables is subject to anything said about them in other enactments. (The word "enactment" in this context is defined in schedule 1 of the Interpretation and Legislative Reform (Scotland) Act 2010.) This proposition emphasises that section 2 is a rule of general application about the treatment of digital assets that will cede to any specific statutory rule that provides for them to be treated on some other basis for particular purposes (for example, section 4 of the Bill itself provides that for the purposes of transfers of ownership, digital assets are to be treated like corporeal moveables).

Section 3 – Presumption of ownership

29. Section 3 creates a rebuttable presumption that the person who has exclusive control of a digital asset owns it. Section 5 defines what it means for someone to have exclusive control of a digital asset.

30. The presumption created by section 3 is analogous to the one that applies in relation to corporeal things, whereby the person in possession of a thing is presumed to be its owner. This is, of course, only a presumption. A person may be in possession of a thing that the person does not own for legitimate reasons (for example because the owner has loaned it to them) or illegitimate ones (for example because the possessor has stolen it from the true owner).

31. A person who is not in possession of a corporeal thing, but who wishes to assert a claim to be its true owner, must show that possession was given up or lost in a way consistent with an intention on the person's part to retain ownership. For example, person A, claiming to be the owner, may be able to show that she only lent the thing to person B who is now in possession of the thing. Or person A may be able to show that she lost it without intending to abandon it, or that it was stolen by person B.

32. As with corporeal things, it is possible to imagine scenarios in which exclusive control over a digital asset is separated from legal ownership of the asset. For example, having exclusive control of a digital asset will in many cases turn on having a private key that is required in order to carry out transactions in relation to the asset. In practice, people will often keep their private keys with a third party which provides software for the purpose of keeping them secure and initiating transactions using them. The fact that a third party and not the owner holds the private key, and therefore has exclusive control over the digital asset within the meaning of section 5, does not

necessarily make the third party the legal owner of the asset just as a bank that places someone's jewels in its vault to keep them secure does not become the owner of the jewels. In such a case, the true owner may be able to show that, under an agreement, the third party held the private key on his behalf and was neither given it, nor took it, with anyone intending legal ownership in the asset to pass as a result. (This is a vastly simplified discussion of the concept of intermediated holding arrangements offered merely to illustrate how control and ownership of a digital asset might become separated, for a fuller analysis of the subject technically as well as legally, albeit in the context of the law of England and Wales, readers are referred to Chapter 7 of the 2023 report on digital assets by the Law Commission of England and Wales.[2])

Section 4 – Acquisition of ownership

Purpose of section 4

33. Section 4 deals with how legal ownership of digital assets is acquired. It creates two broad rules about this:

- Scots common law rules applicable to the acquisition of ownership of corporeal moveables apply (with necessary modifications) in relation to digital assets;
- a limited exception to the usual rule for the transfer of most corporeal moveables, which will allow someone who acquires a digital asset in good faith and for value to become the owner of it despite the person who transferred it not being the owner.

Ownership of digital assets is acquired like ownership of corporeal moveables

34. Subsection (1) of section 4 provides that, for the purposes of Scots common law rules on acquiring ownership of things, digital assets are to be treated as though they were corporeal moveables. This represents a break with the general position established by section 2 which is that digital assets are incorporeal moveables as a matter of law.

35. Merely stating that the law is to treat digital assets like corporeal moveables when it comes to transferring ownership in them would present a problem to the extent that possession of a thing is relevant to the law's treatment of how ownership transfers. Digital assets are unlike corporeal moveables because they are not corporeal (i.e. tangible). They therefore cannot be physically possessed. Accordingly, subsection (1) goes on to provide that having "exclusive control" of a digital asset is to be treated, for this purpose, as equivalent to having physical possession of a corporeal thing. Section 5 defines what it means for someone to have exclusive control of a digital asset.

36. It should be emphasised that subsection (1) of section 4 is exclusively concerned with applying in relation to digital assets the common law rules on the transfer of ownership, it does not affect enacted (which is to say, legislative) rules. As is typical in legislation, subsection (1) uses the phrase "rule of law" to mean law that is not enacted (e.g. Acts and subordinate legislation made under them). Subsection (3) makes the point explicit. The upshot is that section 4 will not cause any legislation concerning the transfer of ownership in things (such as the Sale of Goods Act 1979) to apply in relation to digital assets as though they were corporeal moveables. For the

[2] n 1.

purposes of enactments therefore, digital assets will be treated as incorporeal moveables in accordance with section 2 (see paragraphs 27 and 28 above on the caveats within section 2).

37. At common law, ownership of a corporeal moveable can be acquired by original acquisition (which is to say, loosely, being the first person to take and lay claim to the thing, although it can also occur where the law extinguishes a previous owner's title) or by derivative acquisition (which is to say by the thing's previous owner transferring ownership of it). Both forms of acquisition may be relevant to digital assets.

38. Newly minted crypto-coins (such as bitcoins) are created by the protocol and may be assigned to users by the protocol as rewards for on-system activity such as "mining". (In the context of blockchains, "mining" refers to providing the processing power on the blockchain's network required to solve the cryptographic puzzles that the system uses to validate and verify state changes in the blockchain.) This would be an example of original acquisition in the context of a digital asset.

39. Derivative acquisition in the context of digital assets is, as it is in the context of truly corporeal things, a matter of one person's ownership of the thing transferring to another. In broad terms (and leaving to one side transfers following death and involuntary transfers in the transferor's lifetime), for the law to recognise ownership of a corporeal thing to have been transferred, there must be both an intention on the part of the parties that ownership should pass and delivery of the thing.

40. There are many subtleties belied by the superficially simple statement above about how ownership of corporeal moveables transfers. The transferor must be legally competent to give ownership and the transferee competent to receive it. It may be, for example, that an individual lacks capacity to transfer an asset due to age (see section 1(1)(b) of the Age of Legal Capacity (Scotland) Act 1991) or an incapacity within the meaning of section 1 of the Adults with Incapacity (Scotland) Act 2000. Even where both parties have the necessary competencies, and intend ownership to pass, matters may not be entirely straightforward. For example, a lack of consensus between the parties about to whom the ownership is being passed can render a purported transfer void[3] (meaning the law will treat it as having never taken place), whereas a transfer tainted by one party's fraud may be merely voidable (meaning it is valid unless and until a party with title has it reduced in court).[4] Moreover, the law has long recognised many more ways of effecting delivery of a thing than the straightforward physical act of the transferor handing the thing over to the transferee that the word "delivery" may call to mind. As Carey Miller observes "Scots law has developed a distinctive classification [of modes of delivery] based upon the categories of actual, symbolical and constructive."[5] Section 4(1), by providing that for the purposes of acquiring ownership of them digital assets are to be treated like corporeal moveables, attracts all of the subtlety of analysis that the common law has accreted over centuries in handling corporeal moveables and its capacity to continue to adapt to novel fact patterns.

[3] See for example *Morrisson v Robertson* 1908 SC 332.
[4] See for example *MacLeod v Kerr* 1965 SC 253.
[5] DL Carey Miller with David Irvine, *Corporeal Moveables in Scots Law* (2nd edn, W. Green & Son Ltd 2005) para 8.15.

Protection for innocent acquirors

41. There is a legal principle in Scots law known, in consequence of its Roman law origins, by the Latin brocard *nemo dat quod non habet* (no-one can give what he does not have) or, in another formulation, *nemo plus juris ad alium transferre potest quam ipse haberet* (no-one can give a greater right than he himself has). In the context of the transfer of ownership, this basically means that if you do not own a thing you cannot validly transfer ownership of it to someone else. The law does admit some exceptions to this principle (see for example section 29 of the Bills of Exchange Act 1882). The purpose of the exceptions is to protect innocent acquirors. While an exception to the principle means the innocent acquiror can become the true legal owner of the thing, the wrongfully dispossessed previous owner will have a remedy (potentially both civilly and criminally) against the person who took and transferred the thing despite not being its owner.

42. Subsection (2) of section 4 creates such an exception to the *nemo dat quod non habet* principle for digital assets. It means that if person A, despite not owning a digital asset, purports to sell it to person B, provided that person B has entered into the agreement to buy in good faith (that is, without knowing that person A is not the true owner) and pays value for it (that is a fair price for the asset), then the fact that person A was not the asset's owner, does not prevent person B from acquiring valid title (ownership) of the asset as a result of the sale. There would, in this event, be legal remedies available to person C (the owner of the asset prior to its transfer to person B) on account of having been deprived of the asset. But those remedies would lie against person A, they would not include reducing (voiding) person B's ownership of the asset. Person C would only be legally entitled to recover possession of the asset from person B if person C could prove that person B did not take it from person A in good faith (for example because person B knew that person A had taken the asset nefariously) or that person B had not paid value for it. If person C were able to show either, or both, of those things, person B's acquisition of the asset would not come within subsection (4), the *nemo dat quod non habet* principle would therefore apply, and so person B's title to the asset would be voidable at the instance of person C.

Section 5 – Exclusive control: meaning and presumption

Purpose of section 5

43. Section 5 has two purposes:

- it explains what "exclusive control" in relation to a digital asset means, which is an important concept elsewhere in the Bill as it forms the basis for determining, and acquiring, ownership of digital assets;
- it creates a presumption that a person with control of a digital asset has that control exclusively.

The limits of section 5

44. Subsection (1) simply underscores that section 5 deals with the meaning of exclusive control, and the presumption of it, for the Bill's own purposes only. Other enactments may for their own purposes have different definitions and presumptions.

Meaning of exclusive control

45. Subsection (2) sets out what is meant by "control" of a digital asset. Some types of digital asset may be capable of being "used" within the system manifesting the asset in different ways, so different people may be able to exercise different levels of control over the same asset. The person who is to be treated as having control of the asset for the Bill's purposes is, in effect, the person who has the paramount level of control over it within the system giving rise to the asset. In the case of many, and probably most, digital assets this will mean the person who can transfer the manifestation of the asset within the system giving rise to it from one person to another. This is referred to in section 5 as the ability to initiate a transfer transaction. In defining a transfer transaction, subsection (5) refers to the consequence of such a transaction being that the transferee gains control over either the asset or some quantity of that type of asset. The reference to gaining control over a quantity of the asset, as opposed to the asset itself, allows for the possibility that what a transferee is perceived to receive is not exactly the same asset as the transferor parted with (for a discussion of this point, in the context of a bitcoin transaction, see paragraph 21 above, and for fuller consideration see the discussion of the "persistent thing analysis" versus the "extinction/creation analysis" in chapter 6 of the Law Commission's 2023 report on digital assets[6]).

46. It is at least conceivable that some systems might not allow users to transfer assets amongst themselves within the system. To accommodate this possibility, section 5 provides that in the context of such a system, the person with control of an asset is the person with the ability to initiate a divestiture transaction. This, in effect, means a transaction that results in nobody being able to "use" the asset within the system ever again. If a system does not even allow a divestiture transaction (as so defined) in relation to a digital thing, that thing cannot be a "digital asset" for the Bill's purposes anyway as the thing would not be rendered rivalrous by the system according to the terms of section 1(2).

47. Subsection (2) refers to a person being able to "initiate" transactions. It may be that person A cannot, alone, cause an end-to-end transaction within the system to be effected without person B "co-signing" it (which is to say that both person A's private key and person B's is required for the transaction to be carried out). But so long as person A can initiate the transaction within the system, person A can be recognised as having control of the asset being transacted with for the Bill's purposes. Conversely, if person B has the ability to "co-sign" a transaction in relation to the asset but does not have the ability within the system to initiate a transaction in relation to it, person B will not be recognised as having control over the asset. This sort of tiered signing arrangement is analogous to arrangements found in traditional banking and corporate-authorisation settings.

48. Subsection (3) provides a person has "exclusive control" of a digital asset if the person is the only one who has control of it within the meaning of subsection (2).

Presumption that control is exclusive

49. Subsection (4) creates a rebuttable presumption that control of a digital asset is exclusive. In practice, it is likely to be very difficult if not impossible to prove the negative: that no other person can control a given digital asset. Commonly, the ability to control a digital asset will be

[6] n 1 118ff.

restricted by the requirement to have a cryptographically secure private key for it. Without a presumption of exclusivity, the challenge for anyone claiming to have exclusive control of an asset would be how to prove as a matter of fact that no other person had the private key.

50. The presumption of exclusivity is rebuttable so if, for example, person A is claiming in a civil court action to have exclusive control of a digital asset and therefore to be, by virtue of section 3 its presumptive owner, and person B can satisfy the court that she too can initiate in relation to the asset a transaction of the kind that subsection (2) says a person must if they are to be treated as having "control" of the asset, person A's claim to have exclusive control will be defeated.

Section 6 – Ancillary provision

51. Section 6 empowers the Scottish Ministers to make, by regulations, various types of ancillary provision for the purposes of, in connection with, or to give full effect to the Act that the Bill will, if enacted, become or any provision made under the Act.

52. The power is stated to include the power to modify any enactment (including the Act that the Bill, if enacted, will become). The word "enactment" is defined in schedule 1 of the Interpretation and Legislative Reform (Scotland) Act 2010 and includes primary legislation (e.g. Acts of the Scottish and the UK Parliament). This statement that the power can be used to modify any enactment therefore overcomes the general presumption that a power to make subordinate legislation cannot be exercised to modify primary legislation.

53. Section 6 is to be read alongside section 7.

Section 7 – Regulation-making powers

54. Section 7 makes further provision about the regulation-making powers conferred on the Scottish Ministers by sections 6 (ancillary provision) and 8 (commencement).

55. Subsection (1) makes clear that those powers can be used to make different provision for different purposes. For example, the power conferred by section 8 can be used to appoint different days for the coming into force of different provisions of the Act that the Bill, if enacted, will become.

56. Subsection (2) sets out that regulations under section 6 that amend the text of an Act are subject to parliamentary scrutiny under the affirmative procedure (as defined by section 29 of the Interpretation and Legislative Reform (Scotland) Act 2010). Otherwise, they are subject to the negative procedure (as defined by section 28 of that Act).

Section 8 – Commencement

57. Section 8 deals with when the provisions of the Act that the Bill will become if enacted will come into force (i.e. take effect).

58. It provides for sections 6 to 9 to come into force automatically on the day after the Bill becomes an Act by receiving Royal Assent. The process by which a Bill becomes an Act is set out in section 28 of the Scotland Act 1998.

59. For the Bill's other provisions, it confers on the Scottish Ministers a power to appoint the day on which they come into force by regulations. Those regulations will have to be laid before the Scottish Parliament in accordance with section 30 of the Interpretation and Legislative Reform (Scotland) Act 2010. The power conferred by section 8(2) is to be read alongside section 7.

Section 9 – Short title

60. Section 9 provides for the Act that the Bill will become, if enacted, to be known as the Digital Assets (Scotland) Act 2026.

This document relates to the Digital Assets (Scotland) Bill (SP Bill 75) as introduced in the Scottish Parliament on 30 September 2025

DIGITAL ASSETS (SCOTLAND) BILL

EXPLANATORY NOTES

Produced and published in Scotland by the Scottish Parliamentary Corporate Body.

All documents are available on the Scottish Parliament website at: www.parliament.scot/documents