UK Government. Electronic Trade Documents Bill.
Call for Evidence

This submission is made by XinFin Fintech Pte Ltd. XinFin is an eminent and reputable open-source 'hybrid' blockchain that aims to solve cross-border payment inefficiencies and facilitate secure, transparent, and fast transactions. It is powered by the XDC01 Protocol, has fast and low-cost transactions, is developer friendly, and has a native utility token called XDC. XDC has been used for a wide variety of applications and is continuing to build mainstream adoptions in important areas including trade finance and government activities. The author of this document is a British citizen and therefore also has a personal vested interest in this Bill.

Notwithstanding any specific legal aspects in respect of the application of this Bill in the different legal domains that collectively make up the United Kingdom of Great Britain and Northern Ireland, it is critical that the technical aspects of the technology and its adoption be clarified and explained in detail. If this is satisfactorily achieved then adoption of the Bill will rest entirely on specific points of law and not on any technological aspects.

As an organisation and leading proponent of the proposed technologies, it is our considered opinion that the recommended reforms achieve what they are intended to, that the interoperability of the Bill and particular elements including electronic signatures can be assumed to be reliable and secure within the appropriate architecture and based upon the most suitable core technologies. We will set out our motivation on specific points here-below.

<u>Interoperability</u>
Digital documents can be made highly interoperable, in that they can be easily shared and accessed across different platforms and systems. However, the degree of interoperability can vary depending on the specific standards and protocols being used and the levels of support for those standards within different systems.

At a national level, the interoperability of digital documents can be limited by different standards and systems in different countries. However widespread efforts are being made to promote and accelerate the use of internationally recognised standards such as the International Organisation for Standardisation (ISO) to improve the interoperability of digital documents on a global scale.

A particularly significant development is the Model Law on Electronic Transferable Records (MLETR) referred to in the Call for Evidence. This legal framework facilitates the use of electronic records for the creation and transfer of interests in moveable property (such as goods, securities and money). The MLETR provides a set of rules and guidelines that countries can adopt or adapt in order to create a legal framework for the use of electronic records in their domestic legal systems. The MLETR aims to create a consistent and predictable legal environment for transferable electronic records, which will facilitate cross-border trade and promote the use of electronic records in place of paper documents. The MLETR is designed to be flexible and adaptable so that it can be adopted and implemented in a variety of different legal and business contexts.

Already, interoperability has improved significantly in recent times and is expected to continue improving towards perfection as more systems and platforms adopt standards and protocols that facilitate the sharing of digital documents.

Immutability of electronic documents

An electronic document that is immutable cannot be modified or altered in any way once it has been created. This is an important feature of electronic documents because it allows them to be used as a reliable source of information that can be trusted since all information is cryptographically protected in that cryptography is used to secure the entire ledger against alteration or manipulation.

Blockchain technology is being universally adopted to enable the creation of an immutable record of any changes made to a document and a common method of ensuring the immutability of electronic documents is the use of digital signatures which allow the authenticity of a document to be verified.

Electronic signatures

Electronic signatures can be unquestionably reliable when they are created and verified using secure methods. Modern electronic signature systems are designed to ensure the authenticity and integrity of the documents that are signed and provide a tamper-evident record of the signing process. Digitally anonymous signatures are also possible where the signatures do not reveal the identities of the signatories. However, like any system, electronic signatures can be vulnerable to errors or misuse, so it is important to carefully evaluate the specific electronic signature system you are using to determine and then guarantee its reliability. It is vital to understand that advanced technology may be required by all parties and such technology will need to be evenly distributed. The efficiencies and other benefits of electronic signatures come at the cost of investment in

and constant oversight of the best available technologies required to achieve and protect total system integrity.

Smart contracts can be used to protect digital signatures. In layman's terms, a smart contract is written code that says "if "x" then "y". A smart contract can be set up to require multiple parties to sign a document before it is considered valid. This can help ensure the authenticity and integrity of the document, as it would be difficult for any one party to forge the signatures of the other parties. Overall, smart contracts can provide a secure and efficient way to manage digital signatures and other aspects of contract management.

According to the Law Commission, "smart contracts can also be used to define and perform the obligations of a legally binding contract". Smart legal contracts can take a variety of forms with varying degrees of automation; different forms of smart legal contract give rise to different legal considerations. Where the degree of automation in question takes the smart legal contract out of the realm of legal familiarity, novel legal issues may arise for consideration, particularly in the context of contract formation, interpretation and remedies.

Much work has been undertaken around smart contract security and the formal verification of smart contracts in particular since these are safety-critical elements and should be treated as such.

Future proofing electronic trade documents

Yes, electronic trade documents can be designed to be future proofed. This means that they can be created in a way that allows them to be easily read, understood, and processed by software and systems even if the technology changes in the future. There are several ways to achieve this:

1. Use open standards: By using open standards, you can ensure that your electronic trade documents will be able to be read by a wide range of software and systems, even if they are using different technologies.
2. Use machine-readable formats: Machine-readable formats, such as XML and JSON, are designed to be easily read and processed by software and systems. This makes it easier to extract and use the data contained in the documents.
3. Use clear and concise data structure: A clear and concise data structure makes it easier for software and systems to understand and process the data contained in the documents.

4. Regularly update and maintain the documents: Regularly updating and maintaining the documents will help to ensure that they continue to be compatible with new software and systems as technology evolves.

By following these best practices, you can help to ensure that your electronic trade documents will be future proofed and able to be used effectively for years to come.

Technologically, this ensures the future proofing of the Bill and legally, any alterations and amendments to the Bill could be incorporated by smart contracts without the need for any changes to the architecture of the core technology.

In summary and with reference to the specific topics addressed above, a typical enterprise blockchain architecture consists of six or more layers and two of these would be a privacy layer and a governance layer. The privacy layer is a core feature of a blockchain and there are various methods of achieving privacy, including off-chain privacy managers or on-line algorithmic privacy. The governance layer is an enterprise grade access control mechanism used to control membership of a consortium network.

Blockchain privacy can be divided in to two primary elements. Those are the anonymity of all users and the confidentiality of all transactions. These are fundamental requirements and there are different methods used to achieve privacy which can overlap through the different layers of a blockchain to ensure complete coverage. The essence of a blockchain can provide for privacy of all users and all data, in addition to the numerous widely acknowledged efficiencies enabled by this technology.

Douglas I. C. Brooks
09 January 2023