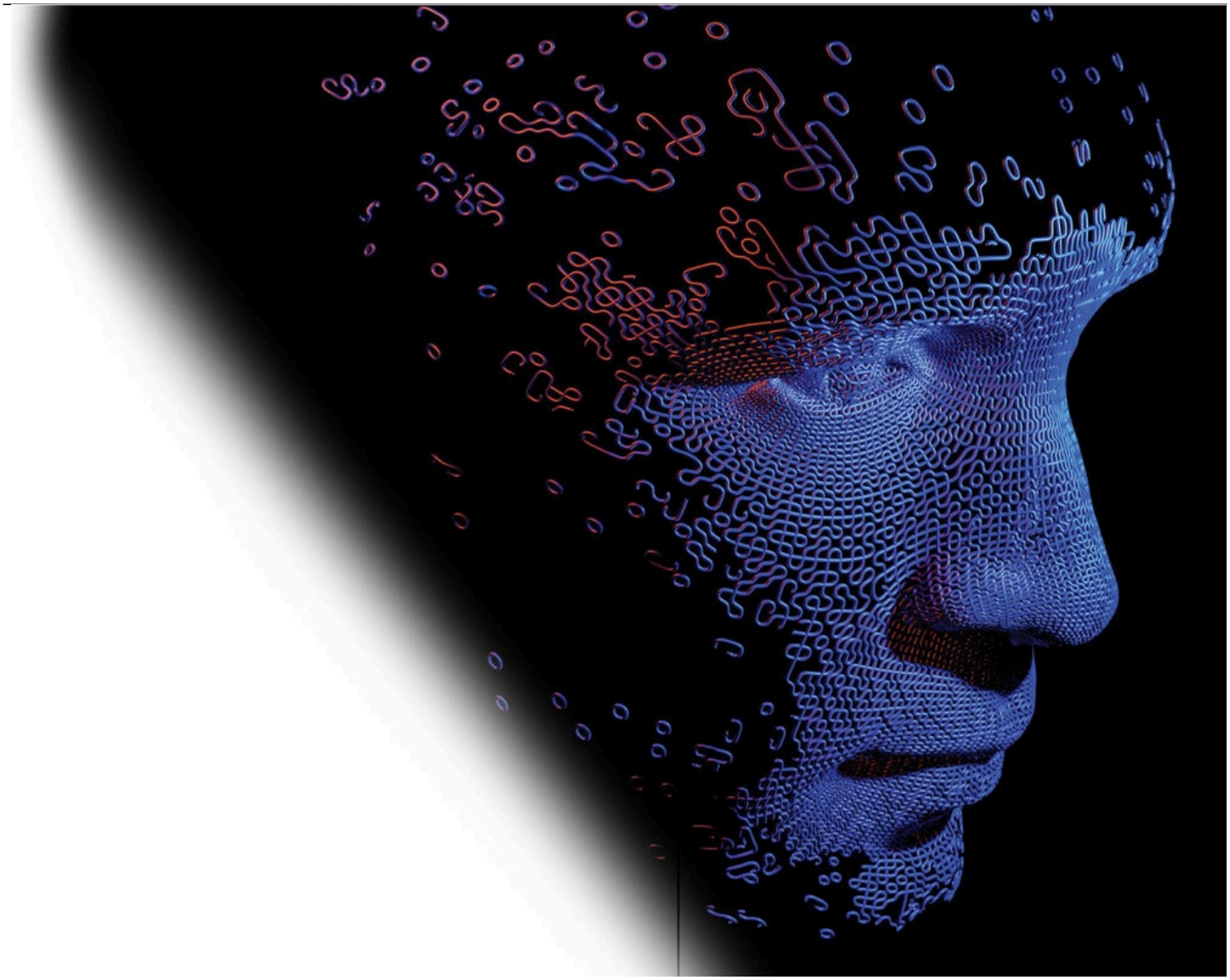
Legal Considerations in the Use of Blockchain Technology and Smart Contracts for Multinational Business

Technology, Privacy, and eCommerce



CHEAT SHEET

- ***Smart contracts***. A legal contract that is, in whole or in part, automated, complemented, or replaced by software code.
- ***Global chain***. Most countries appear willing to enforce electronic contracts as long as the usual rules of contract formation apply.
- ***Privacy, please***. Privacy laws to protect personally identifiable information (PII) vary by jurisdiction. Potential issues from transferring PII internationally can be mitigated by anonymizing or encrypting data.
- ***License to share***. Before using blockchain in a multinational context, intellectual property (IP) issues must be addressed. The IP rights and protections should reflect the regulations of the jurisdictions involved in the transactions

Blockchain was invented in 2009 by a person (or group) known as Satoshi Nakamoto, to support Bitcoin, a decentralized peer to-peer electronic currency. However, the technology itself is separate from Bitcoin and can be implemented to support myriad other uses. Although cryptocurrency has garnered significant attention, this article focuses on considerations applicable to the use of blockchain in multinational business, apart from cryptocurrency.

Timely, ongoing engagement is critical to conduct business on a global scale. Multinational enterprises and their clients are seeking consistency and integrity in the execution of international transactions. Differing local legal requirements, multiple stakeholders, language barriers, and time zone challenges inherent in cross-border transactions may result in disconnects among the transacting parties and even between a parent entity and its local affiliates. These disconnects can cause additional costs, delays, gaps in execution, and even regulatory noncompliance, increasing the risk to all parties involved.

Blockchain, a distributed ledger technology, has emerged as a potential global solution to these problems. As the technology is distributed by design, transaction records cannot be changed and are protected in the event of a single system failure. In addition to the immutable nature of its distributed architecture, blockchain technology provides a common view of transactions in real-time across computers, parties, and jurisdictions. With these characteristics, blockchain promises the operational transparency, availability, integrity, and security necessary to execute multinational transactions from beginning to end with significantly reduced risk.

In June 2017, AIG, IBM, and Standard Chartered Bank successfully piloted the first use of blockchain technology to implement various aspects of a multinational insurance program across the United Kingdom, the United States, Kenya, and Singapore. Blockchain enabled AIG, IBM, and Standard Chartered to provide direct notification of premium payment and policy issuance to the corporate and local stakeholders in real time.

The technology successfully enabled a “single view of truth” across all network participants on the critical aspects of multinational transactions: invoicing, payment, and contract certainty. It simultaneously provided selective visibility on these transactions to participants, based on their credentials. Corporate stakeholders had real-time visibility on the myriad transactions necessary to successfully implement a multinational insurance program across their organizations; local stakeholders saw this detail for their relevant jurisdiction.

The pilot demonstrated the potential for blockchain to create a new level transparency — reducing the delays or resources expended in communication across organizations, language barriers, and time zones to achieve consensus and visibility over the multinational process.

The visibility offered through blockchain is currently being used to track provenance and document

financial transactions in a variety of multinational arrangements, ranging from supply chain to trade finance. Businesses and regulators are increasingly using blockchain to conduct and provide oversight of cross-border banking and finance activities. The authentication necessary to execute and record a transaction, and the irreversibility of a transaction once it is recorded in the blockchain, provides a secure and auditable record of each transaction, reducing the time, labor, and costs traditionally associated with manually verifying, reconciling, and settling international payments or money transfers.

Traceability and control are also driving blockchain usage in other commercial contexts, where goods ranging from perishable agricultural produce to sophisticated electronics travel through a supply chain network before reaching the end consumer. This is especially true in multinational business when suppliers, manufacturers, transporters, storage facilities, distributors, and retailers are involved across multiple jurisdictions. Blockchain supplies a digital passport for each item or transaction in these complex value chains. Marine, ground, and air cargo transportation, food sourcing, real estate transactions, and machinery and vehicle sales are all examples of blockchain use cases in this context.

Smart Contracts

Smart contracts programmed to execute on blockchain are equally promising in the facilitation of multinational transactions. The term “smart contract” has multiple meanings. It can refer to a software program that encodes performance conditions and outcomes and the instances of code used to create that program, or to a legal contract that is, in whole or in part, automated, complemented, or replaced by software code.

A smart contract program irreversibly automates performance of the parties’ obligations based on the fulfillment of a condition or set of conditions defined in the program. A legal contract can be made “smart,” either entirely or in part, through use of mart contract programs or other software automation using blockchain technology.

Consider purchasing insurance for global exposure and the various actions required at the global and local level across the insurer, reinsurer, broker, and insured organizations. Cash before cover, anti-money laundering (AML), and mandatory reinsurance retentions are examples of the many requirements to be fulfilled before one or multiple policies can be validly issued.

With blockchain, many of the steps required to fulfill these requirements can be automated. For example, if an insurer enters into a smart legal policy with an insured in a “cash before cover” jurisdiction, the commencement of coverage could be defined in code to execute automatically when the insured pays the premium (i.e., the condition of “cash” is fulfilled). Similarly, the issuance of certificates of insurance could be defined in code to execute automatically when policies are issued.

These are just a few aspects of an insurance policy, which may also include terms that cannot as easily self-execute, such as adjustment/valuation of losses or resolution of disputes. Self-execution or automation is more challenging for components that may require reversibility, interaction, or subjective analysis off-chain, which are antithetical to blockchain’s fundamental characteristics of transparency and immutability. These transaction elements need not be represented through “smart contract code” and instead may exist externally, either off-chain entirely or in a hybrid mode where information is brought on-chain through hashed pointer blocks linking to the off-chain data or transaction terms.

Overview of the blockchain and smart contract regulatory and legal landscape

While businesses are still pondering the technology in concept and practice, legislators and regulators throughout the world are similarly determining its governance. Below is a non-exhaustive overview of the global legal and regulatory landscape with respect to blockchain technology and smart contracts

Blockchain technology

Several US states have enacted or proposed legislation validating the use of blockchain technology in commerce. These include Vermont (blockchain to be considered a regularly conducted business activity establishing a presumption that the information in the blockchain is correct), Nevada (recognizing blockchain as a form of electronic records satisfying the requirement for a written record in city and county government), Delaware (authorizing registration of shares of Delaware companies in blockchain form), and Wyoming (permitting filings made for corporations, LLCs, and UCC financing statements to be made on blockchain).

In Asia and Australia, regulatory blockchain initiatives have been proliferating. Australia is currently implementing a blockchain-powered securities exchange. In March 2017, Japan's Ministry of Internal Affairs and Communications announced a blockchain/smart contract solution that will allow companies to interact with the government.

> Australia is currently implementing a blockchain-powered securities exchange. In March 2017, Japan's Ministry of Internal Affairs and Communications announced a blockchain/ smart contract solution that will allow companies to interact with the government.

The Monetary Authority of Singapore, in collaboration with a consortium of banks, launched "Project Ubin," the first phase of which focuses on digitization of the Singapore dollar on a blockchain. The second phase will test a real-time gross settlement system. The project currently has three additional phases and is planned to be completed in late 2018.

In the European Union, regulatory agencies are reaching out for help in navigating the evolving landscape. The United Kingdom's Financial Conduct Authority published DP17/3 asking for comments in order to start a dialogue on the potential for future development of blockchain in the markets they regulate. In France, Finance Innovation, an institution dedicated to fostering the financial sector, is establishing a working group to guide the government over initiatives they will need to lead in the blockchain sector. In June 2017, the European Commission announced the launch of its #Blockchain4EU Project to help industrial use cases for blockchain.

> With respect to the jurisdictions that were surveyed outside the United States, in the absence of specific legislation governing the rules surrounding the formation of a contract by electronic means, most countries appear willing to enforce electronic contracts as long as the usual rules of contract formation (offer-acceptance-consideration) apply.

Smart contracts law

The law around smart contracts is likewise evolving. There is a spectrum of architectural models through which the transactional aspects of legal contracts can be made “smart.” These range from replicating aspects of legally binding off-chain “natural language” transactions to coding legal transactions that fully exist as smart contract programs.

Various commentators have surveyed existing law in numerous jurisdictions and concluded that it forms a basis for providing legal effect to smart contracts. For example, in the analysis undertaken by Norton Rose and R3, the writers analyzing US law observed that consideration should be given to how the parties will give assent to the terms of the smart contract, what steps should be followed to ensure the parties have proper notice of the contract terms, and what must be done to bind a party to a contract that is executed electronically. The authors concluded that if these factors are considered and addressed, courts in the United States would be willing to support automatic contracting.

With respect to the jurisdictions that were surveyed outside of the United States, in the absence of specific legislation governing the rules surrounding the formation of a contract by electronic means, most countries appear willing to enforce electronic contracts as long as the usual rules of contract formation (offer-acceptance-consideration) apply. When examining laws around the formation of electronic contracts such as that of Australia (Electronics Transactions Act 1999), China (PRC Electronic Signature Law), and France (Article L223-12 of the French Monetary and Financial Code), further support for legal validity of smart contracts was found.

In addition, certain jurisdictions in the United States have recognized the enforceability of legal transactions that are fully or partially executed via smart contract programs. Arizona passed legislation prohibiting denial of legal effect or enforceability of a contract solely because the contract contains a smart contract term. The Arizona legislation specifically defines the terms “blockchain technology” and “smart contract,” and recognizes that smart contracts may exist in commerce. Nebraska and Tennessee have proposed similar legislation.

Aside from enforceability, there are other legal issues implicated by smart contract programs. For example, which law will govern and which jurisdiction will apply in multinational smart contracts that are silent on governing law and jurisdiction and where performance is replicated across a distributed ecosystem spanning multiple countries? Will tort concepts apply to contract interpretation when a smart contract goes awry due to bugs or errors in the programming, or in external information fed to the blockchain via an oracle that triggers a smart contract? What systems can be put into effect to remedy an irreversible result wrongfully or erroneously achieved? These issues and others will be addressed as the technology evolves and proliferates.

General multinational considerations for blockchain technology and smart contracts

It is critical to understand the geographic scope of each transaction. From a multinational legal perspective, privacy, data localization, and outsourcing tend to be the most salient considerations. As data is implicated in all blockchains and smart contracts, we should consider what information is being processed, how it is used, who is accessing it, and where it is being stored and transmitted.

The privacy of personally identifiable information (PII) is a concern in all regions, particularly with respect to certain types of consumer data and sensitive information. PII generally consists of information that can be used to identify, or is information about, a natural person. Sensitive information is a sub-category of PII and varies by jurisdiction. Laws in the United States generally

focus on health and financial information, while EU regulations treat race and ethnicity, political and religious beliefs, genetics and biometrics, health, sex life, and sexual orientation as special information. Privacy laws govern how and what PII can be collected (including consents), how PII can be used, the security and integrity of PII, if and how PII can be transferred between entities and jurisdictions, and when an individual's personal data must be deleted. These issues may be mitigated by redacting, anonymizing, or encrypting the data being processed in a blockchain ecosystem or storing personal data off-chain. Certain privacy laws, including the European Union's General Data Protection Regulation, (GDPR), have an extra-territorial effect that is of particular concern in multinational transactions.

Data localization laws confine or limit the collection, processing, storage, or hosting of certain data related to local activities or individuals in a particular country. This can be explicitly required by law or the result of policies that render data transfer impractical; such as requiring companies to store a copy of the data locally, requiring companies to process data locally, and mandating government approval or individual consent. The data impacted by this type of law ranges from PII to accounting, tax, and other business records. China, Israel, Indonesia, Korea, Russia, and Turkey are among several countries with data localization requirements.

Outsourcing is particularly important in Asia, where several jurisdictions, including Indonesia, Malaysia, Taiwan, and Thailand, may prohibit transferring certain activities to another jurisdiction. Where permitted, outsourcing is often subject to stringent requirements. In addition to service agreement and security measure requirements, the regulator must also be allowed the right to audit and otherwise inspect the financial records of the entity performing the outsourced activities. Hong Kong, Malaysia, Singapore, and Taiwan all require a risk assessment, as well as board and regulatory approval, before outsourcing can occur.

Transactions that involve employees in the European Union may also require prior engagement with the corresponding country's Works Council and other trade unions. These representative bodies must be consulted by law before the implementation of any changes to process or technology impacting employment terms or working conditions. This would include changes to processes and technology. France is particularly worth mentioning since failure to consult is a criminal offense punishable with large fines and imprisonment.

Careful consideration should also be exercised in joint ventures when introducing new processes and technology. These changes should be considered against pre-existing agreements with local management and typically require the consent of business partners.

When building a private blockchain ecosystem or operating within a blockchain consortium, antitrust and competition laws may apply. Issues of concern include limiting competition between participants, price fixing among participants, and the rules surrounding membership restriction. Although collaboration is key to implementing a successful blockchain ecosystem, it is important to be aware of issues that may expose a member to antitrust or competition law violations.

Last but not least, a global company looking to effect cross-border financial transactions through blockchain must also comply with applicable AML laws where it operates or accepts such currencies. Many jurisdictions do not specifically contemplate blockchain technology at this stage, and regulators in those that do may have concerns around its use to transfer funds from another country. These countries may either prohibit the receipt of such funds or require additional due diligence on the source.

Intellectual property considerations

Businesses using blockchain in a multinational context should consider and examine the numerous intellectual property issues. Whether engaging in blockchain ecosystems formed by consortia or outside of that context, ownership and licensing of both newly created and pre-existing materials should be addressed up front. For example, the parties to the ecosystem should consider whether the newly created work should be solely owned (and if so, by whom) or jointly owned, in which case the parties will need to determine how they act as joint owners. In each case, an agreement should also expressly state what licenses and intellectual property infringement indemnification will be provided to each party, and whether there will be any periods of exclusivity or other competitive advantage. The intellectual property rights and protections should reflect the jurisdictions covered by the transactions encompassed by the ecosystem.

Parties who participate in beta testing of blockchain products may be asked to provide the consortium or vendor developing the product with ownership or a broad license to any feedback or suggestions provided by the testing participant. The testing participant may wish to consider whether retaining ownership of its feedback and suggestions is necessary in this context and carefully monitor what information it actually provides to ensure protection of any trade secret or other confidential information.

> Transactions that involve employees in the European Union may also require prior engagement with the corresponding country's Works Council and other trade unions. These representative bodies must be consulted by law before the implementation of any changes to process or technology impacting employment terms or working conditions.

It is also important to remember that most blockchain technologies are open source. While in many cases this does not raise issues, certain blockchain technologies, including applications in Ethereum, are subject to "viral" or so-called "copyleft" licenses, whereby software may be used by, modified, or distributed freely on condition that anything derived from it is bound by the same condition. An example is the GNU General Public License, in which code linked to the copy-lefted code is then made subject to the copyleft license.

Standards initiatives are emerging to grapple with intellectual property issues implicated by blockchain. The Chamber of Digital Commerce created the Blockchain Intellectual Property Council to promote innovation in blockchain by addressing intellectual property rights issues, including combating the proliferation of patent trolls in this space. The council has provided blockchain-specific patent information and is focused on implementing various intellectual property protection models, such as "non-aggression agreements" where industry players agree not to assert patents against each other. Other models include the creation of developing patent pools where cross-licensing options are available to all pool participants, and the "reducing inventory" approach under which subscribing groups (like the LOT Network) require members to agree not to sell patents without first granting a license to all group members.

ACC has launched a global Blockchain Initiative, which will offer programming and tools to assist in-house practitioners with the wide variety of legal issues arising from the use of blockchain and smart contracts.

> ACC has launched a global Blockchain Initiative, which will offer programming and tools to assist in-house practitioners with the wide variety of legal issues arising from use of

blockchain and smart contracts.

Conclusion

Given the complexities and numerous legal issues implicated by the use of blockchain and smart contracts in multinational business, in-house lawyers should be engaged as business clients begin planning these initiatives, and proactively assist in defining the scope of blockchain use cases and architectural parameters. This early involvement will enable the in-house lawyer to better advise their clients on the regulatory, compliance, and commercial implications of using these technologies, including the potential need to engage applicable regulators and other governmental bodies.

References

Satoshi Nakamoto, Bitcoin: A Peer-to- Peer Electronic Cash System, (Oct. 31, 2008).

A distributed ledger is a database held and updated independently by each participant (or node) in a network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network. Blockchain is used herein to refer generally to distributed ledger technologies, although it is but one type of distributed ledger technology.

The term “off-chain” is used to refer to data or transactional activity that is related to but takes place outside of a blockchain. The term “on-chain” refers to data or transactions recorded within the blockchain. Off-chain and on-chain data and transactions can be linked through various means, such as APIs and hashed blocks referencing off-chain data.

12 V.S.A. § 1913.

Nevada S.B. 398 (2017).

8 DE Code § 219 (2017).

Wyoming H.B. 0101 (2018).

Nikkei, Japan looks to blockchains for more secure e-government systems, (Jun. 29, 2017).

Arjun Kharpal, Singapore aims to finish its own cryptocurrency trial next year, (Oct. 26, 2017).

John Salmon & Winston Maxwell, Blockchain: facing up to the regulatory challenges in multiple jurisdictions, (Jan. 19, 2018).

Sean Murphy et al., Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright White Paper, (Nov. 2016). (Enforceability of smart contracts under the laws of England, the United States, Australia, Canada and China).See also Alan Cohn et al., Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids, 1 Geo. L. Tech. Rev. 273, 285 (2017) (existing laws, including the federal Electronic Signatures in Global and National Commerce Act and the Uniform Electronic Transaction Act form basis for enforcing smart contracts).

A.R.S. § 44-7061(c).

“Blockchain technology” means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.

“Smart contract” means an event-driven program, with state, that runs on a distributed, decentralized, shared, and replicated ledger, and that can take custody over and instruct transfer of assets on that ledger.

Nebraska L.B. 695 (2018). (To authorize and define smart contracts, to authorize use of distributed ledger technology in the Electronic Notary Public Act and the Uniform Electronic Transactions Act and for purposes of digital and electronic signatures).

Tennessee H.B. 1507 (2018). (Recognizes the legal authority to use blockchain technology and smart contracts in conducting electronic transactions and protects ownership rights of certain information secured by blockchain technology).

Articles L.2323-20 and L.2328-1 of the French Labor Code.

Chamber of Digital Commerce, Chamber of Digital Commerce Forms the Blockchain Intellectual Property Council, (Mar. 16, 2016).

Ehab Samuel & Matthew Bottomly, Looking Through an IP Lens at Blockchain and Cryptocurrency, (Sep. 28, 2017).

Wendy Callaghan

Chief Innovation Legal Officer and Associate General Counsel

AIG

Wendy Callaghan is chief innovation legal officer and associate general counsel, heading AIG’s Innovation Legal Group. In this role, she leads a team of attorneys providing legal support to AIG’s businesses and function areas with respect to innovation, including blockchain, AI/machine learning, IoT, autonomous vehicles, and sharing economy.

Rajika Bhasin

Assistant General Counsel, Multinational

AIG

Rajika Bhasin is associate general counsel, multinational, and also serves on AIG’s Global Legal Compliance & Regulatory Innovation Stakeholders Forum. She advises on cross-border business, legal, operational and tax issues, supports global knowledge management and related technologies, and structures global transactions using innovative technology.