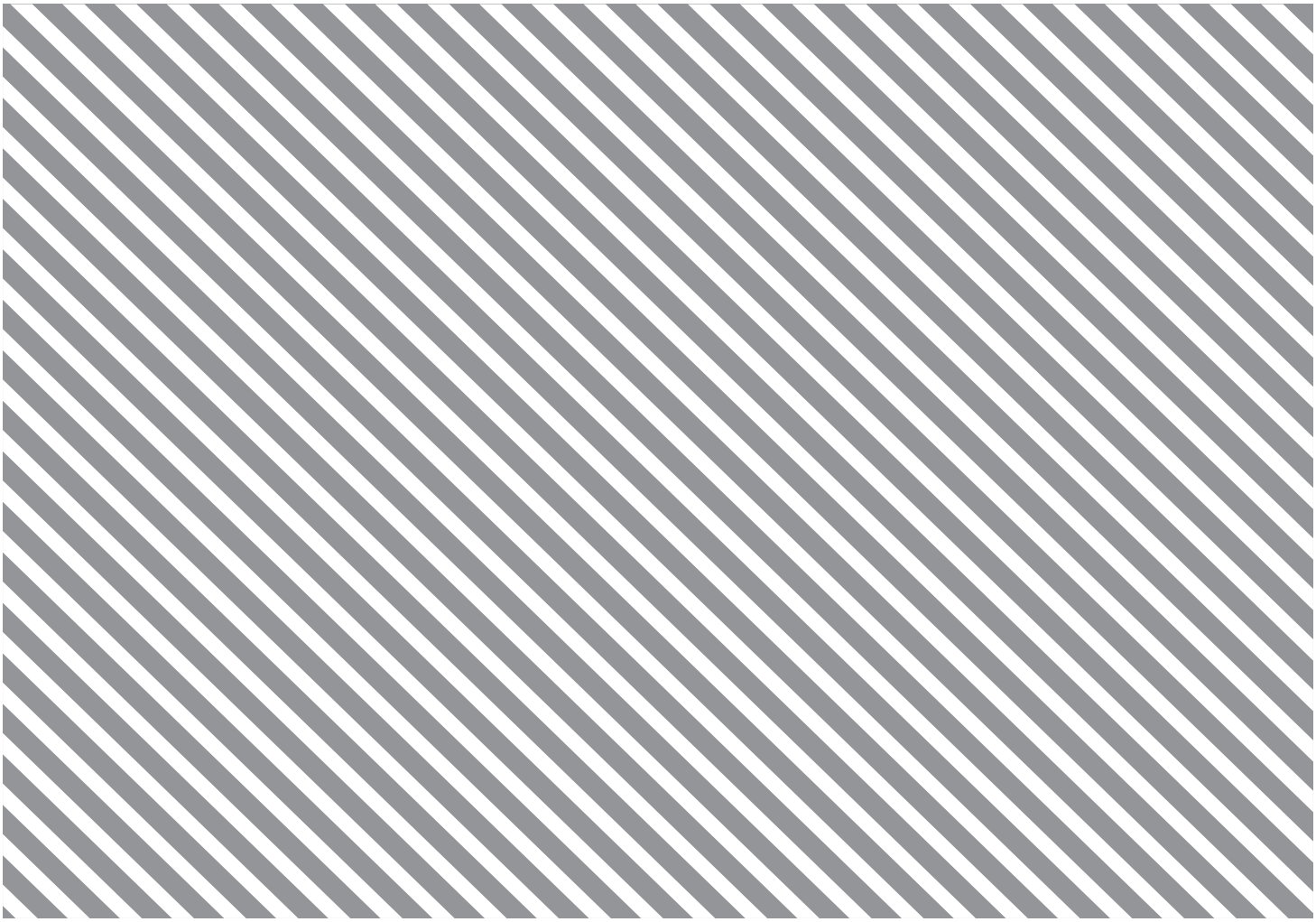
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Inclusive Deployment of Blockchain for Supply Chains: Part 3 – Public or Private Blockchains – Which One Is Right for You?

July 2019



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Lead Authors
Hanns Christian Hanebeck, Founder and Chief Executive Officer, Truckl, USA
Nadia Hewett, Project Lead Blockchain and DLT, World Economic Forum, USA
Peter A. McKay, Content Producer, Dispatch Labs, USA

Contents

Preface

Sheila Warren, Project Head, Blockchain and Distributed Ledger Technology, World Economic Forum

Nadia Hewett, Project Lead, Blockchain and Distributed Ledger Technology, World Economic Forum

Blockchain technology often elicits both fascination and confusion from leaders within organizations. Within the supply chain industry, the technology has now moved beyond the early proof of concept provided by bitcoin.[1] At the same time, the technical complexity of blockchain can be a barrier to entry for newcomers.

This report attempts to break one of those barriers as it pertains to global supply chains. Specifically, the report addresses important criteria to make sense of public versus private blockchains and looks at how each affects the eventual supply chain solution.

It is important that industry decision-makers can sort through the marketing hype to pick the best solution for their particular requirements. For instance, some blockchain technology providers in the industry have made claims such as "We're the first ever truly neutral system" or "We're the only public solution" or "Our private blockchain is best positioned to protect your data". Supply chain professionals understandably need help sorting through such claims, some of which are inevitably misleading or inaccurate.

While the focus of this white paper is on demystifying elements of the public-versus-private debate, it is important to remember that the blockchain structure is only one aspect of the technical solution. Although we outline some typical criteria in this white paper, decision-makers must look at the context of their selected use case and distinct requirements.

This paper is the third in a series covering the co-creation of new tools for the responsible deployment of distributed ledger technology (DLT) in supply chains. To produce this series, the World Economic Forum's Centre for the Fourth Industrial Revolution is working with a multistakeholder group to create a project that includes:

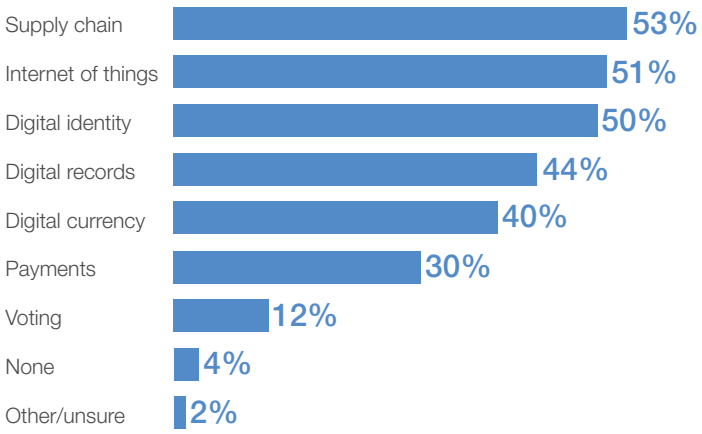
– A series of papers published in 2019. Collectively and individually, these papers will offer insights and thorough explorations of the specific considerations for decision-makers in harnessing blockchain technology effectively.

– A concise, easy-to-use toolkit to be released in 2020 covering important topics for supply chain decision-makers to consider for responsible blockchain deployment.

Introduction

As specific use cases take on an increasingly important role for blockchain and distributed ledger technology (DLT) deployments, one area that has already emerged as a fertile area for applications is the global supply chain. In a 2018 survey of 1,000 corporate executives, the consulting firm Deloitte found that more than half of respondents (53%) identified the supply chain as a use case their companies are exploring for blockchain. That topped relatively more "traditional" use cases of the technology such as internet of things (IoT) (51%), digital currency (40%) and payments (30%).[2]

Figure 1: Blockchain use cases



Percentage of respondents that are working on the select use-cases
Percentage equals more than 100% because respondents were allowed to submit more than one answer

Source: Deloitte's Global Blockchain Survey: Findings and Insights

For supply chain organizations launching new blockchain projects, one of the most fraught considerations typically is whether to use a public or private ledger and what permission models. This decision affects functionality, security, compatibility with other stakeholders' systems and, perhaps most important, competitive positioning for companies. This paper explores important considerations in making the public-versus-private decision, including arguments for and against each option. It is important to remember that the blockchain structure is only one aspect of the technical solution. While we outline some typical criteria in this white paper, decision-makers must look at the context of their specific use case and its distinct requirements.

The findings in this paper were gleaned from research as well as detailed interviews with blockchain users across diverse industries, geographies and applications. The findings are undertaken in simple terms to bring understanding of some key considerations. For these reasons, the paper will not delve into the multitude of technical layers, complexities and exceptions that exist with blockchain technology, though the authors recognize their existence and importance.

Blockchain terminology

It is important to pause here to note that the blockchain space is often subject to controversies stemming from the early maturity of the technology itself – this also applies to the concepts of public and private blockchains. This is often caused by a simple misalignment of definitions between speakers, with even the term “blockchain” meaning vastly different things to different people. Determining the facts, understanding the variants, and effectively communicating the capabilities of the technology can be challenging when terms are misleading or used out of context. In any discussion on the topic, it is hence important to align on the verbiage and terminology used for public versus private blockchains[3].

Some experts say a vital criterion in classifying a blockchain as “public” or “private” is whether it is truly decentralized. They may argue that a DLT is not “public” unless it is 100% decentralized. Others believe a more finely tuned spectrum of decentralization should exist. Unfortunately, there is no shortage of terminologies used to explain public versus private and related permission models. This dearth of objective material led Angela Walch, associate professor at St. Mary’s University School of Law, to caution regulators in her 2017 paper, The Path of the Blockchain Lexicon (and the Law). “It is essential,” she writes, “that regulators do not simply accept what they read or hear at face value; rather, they must adopt a critical point of view and act strategically to uncover the facts beneath the muddle of inconsistent terminology, misinformation and hype.[4]”

These semantic misalignment are unlikely to stop any time soon, so leaders are best advised to seek to clarify terms used to descibe a blockchain.

Taking stock of the supply chain landscape

In 2018 and 2019 research, The World Economic Forum dived deeply into the evolving discussion on whether public or private blockchains are typically best suited for the supply chain industry. Following are some of the key findings:

– To the extent that organizations in the industry have experimented with blockchain technology so far, both public and private versions have been useful in achieving different objectives and meeting project requirements.

– Many industry veterans believe the supply chain space is generally cautious in adopting new technology tools such as blockchain. Collaboration and data sharing among organizations have traditionally not been the norm, going back over many decades. Thus, new entrants aiming to encourage blockchain adoption are likely to face challenges and many see private technologies in the near term as the more likely path for the industry to begin using blockchain technology. This helps to acclimatize supply chain providers' organizational cultures to unfamiliar new technology. However, as the industry grows more comfortable with blockchain, there is hope it will open the way for increasing use of public chains in applications, where appropriate.

– As the industry explores private blockchain solutions, it is important to distinguish the benefits of blockchain technology from that of traditional databases. Being aware of the pros and cons of blockchain and understanding where its features really help to solve a problem, ensure that the new technology does not become just an expensive version of a centralized database. In use cases where the unique advantages of blockchain aren't particularly helpful, providers may opt to stay with, for example, an SQL or NoSQL database or similarly traditional solution.

– The public-versus-private blockchain debate has received much media and supply chain industry attention over the last two years in the supply chain space – to a degree that it can distract from what is really important. Many experts point out that for supply chain applications, it is also important that the industry move past the public-versus-private debate to one focused more keenly on deploying solutions where enterprise-specific requirements can be met. The requirements an enterprise specific blockchain solution must adhere to typically include:

– **Operational integrity:** Clear contractual agreements in any relationship that affects their daily operations, so organizations know who has liability if something goes wrong.

– **"Know your customer" compliance:** A crucial regulatory issue, especially for payment and financial services providers.

– **Interoperability:** Blockchain solutions have to interact with other existing processes and systems.

– **Security requirements:** These may include data segregation, control requirements, privacy and more.

– **Scaleability:** Of course, any new blockchain solution should be able to grow along with the enterprise if needed in terms of transaction volume, number of customers and other metrics.

A brief primer on blockchain

In the simplest terms, a blockchain is a shared, distributed and immutable transaction ledger. Transactions are added as they occur, either one at a time or in batches, depending upon the protocol being used, with each "block" of transaction data containing context such as date, time and so on. The transaction "blocks" are then linked, usually in chronological order, to form an audit trail that ensures transparency among participants. This series of linked transactions is referred to as a "chain", and thus the whole data structure is referred to as a "blockchain". Blockchain is a peer-to-peer network, so each node or participant maintains a replica of a shared ledger of digitally signed transactions.

Other blockchain concepts and an explanation of blockchain structure - public versus private and the different permissioned models - are available in the first paper in this series, *Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction* (April 2019).[5] The blockchain concepts are presented in simple terms and the paper does not delve into the many technical layers, complexities, hypotheticals and exceptions that exist with blockchain and distributed ledger technology, though the authors recognize their existence and importance.

Hashing vs open data

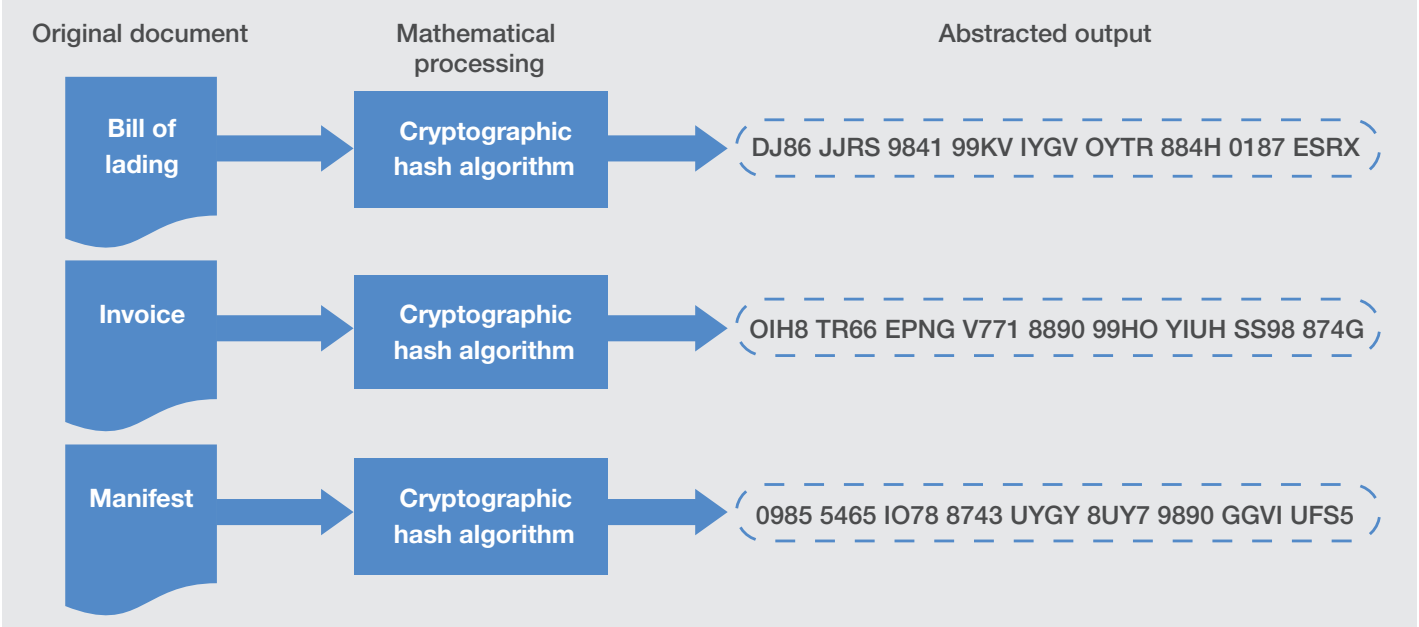
When deploying a blockchain solution, one vital consideration companies face is how visible their data should be. In particular, transactions on a public blockchain are available to be read not only by the whole supply chain network but also by non-industry internet users.

If a company decides to use a public chain, there are still some ways to protect critical data. For example (see Figure 2), information that needs to remain confidential can be passed through a cryptographic hashing algorithm (for better security), which takes a text input of any size and creates an output of fixed length. This output is called a hash, and is irreversible, meaning that given the output, the input cannot be determined. So, while other supply chain actors may see that a transaction occurred, they will see only a hash of the data and not the original sensitive information. With hashing, the original data needs to be stored off-chain.

On a blockchain network, hashes can be useful in proving that documents have not been altered over time and to also show that the documents have been in someone's possession at a particular time.

For example, when there are disputes over how many goods were ordered and delivered in a transaction, a validation of original documents through the generation of a second hash proves that original documents haven't changed and are reliable as a source for dispute resolution. Furthermore, the timestamp of the hash serves to confirm the date of the item's origin.

Figure 2: Hashing algorithms Ways to abstract data on the blockchain



Key considerations for blockchain structure

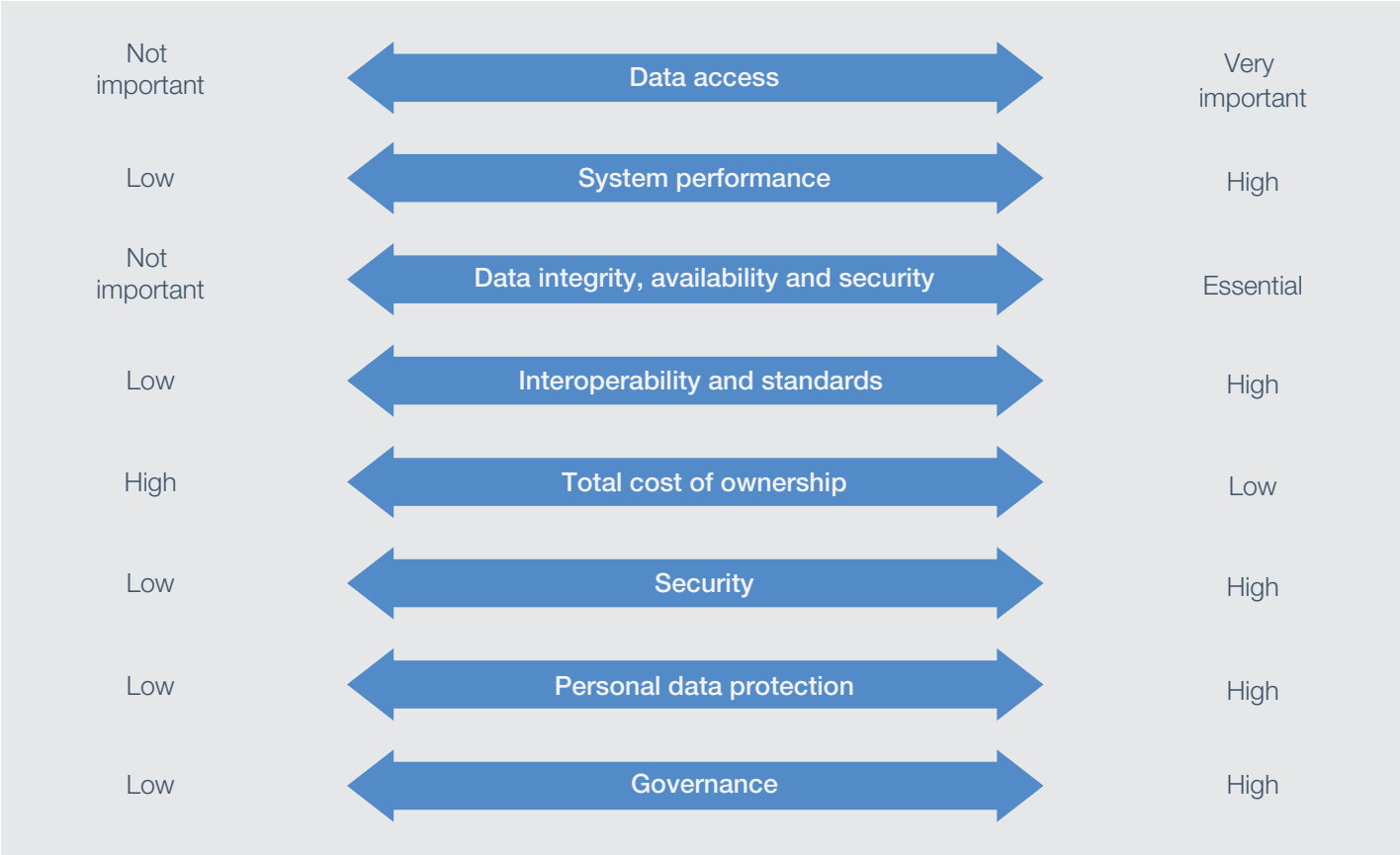
As supply chain stakeholders weigh the public-versus-private question, they must consider several factors that may vary greatly including how many partners are included or what types of goods and materials are involved. Other important factors include what primary customers and partners are already doing (perhaps join an established consortium) and whether standards organizations and government agencies have requirements of their own that must also be met for compliance purposes.

For example, when primary business partners have already joined a blockchain consortium such as R3, Energy Web Foundation or B3i, it may be made moot for individual companies to ponder a solution that deviates from the consortium's collective action.

Ultimately, supply chain management is a team sport that forces each party to draw a clear line on how much information it is willing to share.

The research identified typical requirements that supply chain operators have for blockchain solutions. The importance and priority of these features differ depending on the use case in question. The following features were identified as required:

Figure 3: Key considerations for blockchain structure in supply chain use cases The importance and priority of these considerations differ depending on the use case in question.



Other important considerations include how readily a certain blockchain technology may be integrated into existing systems, switching cost, how easy it is to train primary users, and expectations about the long-term viability of the technology or its provider.

The following review the performance and benefits of public versus private blockchains with these key considerations:

Data access

In a public blockchain, anyone can access and take part in the ledger, while, in a private blockchain, only selected parties can access and make changes to the distributed ledger. In a public blockchain, transactions are broadcast to every single participant (node) and every node thus keeps acomplete record of the entire transaction history. Private blockchains limit access to the blockchain to only those organizations that have been admitted into the network.

Different types of permissions can be granted to participants of a blockchain network.

Read: Who can access the ledger and see transactions

Write: Who can generate transactions and send them to the network

Commit: Who can update the state of ledger

Most data found in supply chain transactions today is confidential. To address such concerns, operators often either store a hash of their data on the blockchain, encrypt data before writing it to the chain or are forced to use a permissioned chain.

More commonly, data protection concerns have made organizations more willing to deploy private solutions in lieu of using public blockchains.

Public blockchains are also exploring innovative privacy measures, which means that their value proposition can develop over time as stakeholders prioritize data protection. Zero-knowledge proofs are one such example.

Zero-knowledge proof:
Sharing of secrets without their disclosure

Zero-knowledge proofs (ZKPs) are an important add-on of some blockchains since they guarantee the validity of data without the need to disclose the actual data openly. This is important when the details of a transaction such as prices or terms need to remain confidential or when the party writing data to the blockchain needs to stay anonymous.

ZKPs essentially allow one party to ask the other a series of questions about the data without needing to know what the secret is by focusing on outcomes instead. If the issuing party can answer all questions reliably, then it must know the secret and the requesting party should be satisfied.

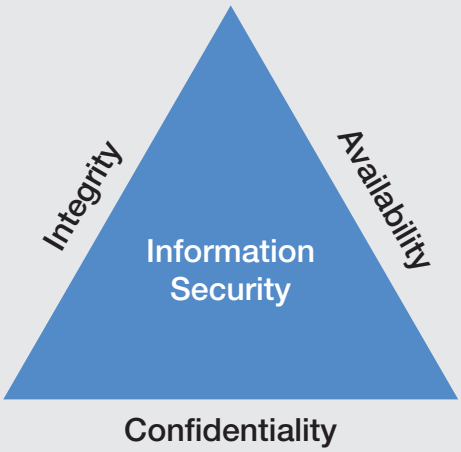
System performance

Performance, or the speed with which transactions are written to the blockchain, is another important consideration in that public blockchains in general tend to be slower than private versions (this can be due to e.g. wider polling to achieve consensus and, in some cases, outright limits on transactions or block sizes). If users need to store large amounts of data on the blockchain, a public chain can thus be problematic.

Data integrity, availability and security

A much-used term in the industry, supply chain stakeholders generally refer to ‘data integrity’ when talking about the need for accurate and timely data input along the supply chain from trustworthy sources. However, data integrity from a technological standpoint has broader considerations that ties with the field of information security. There, data accuracy relates to information integrity, while timely data input and access relates to data availability.

Figure 4: The CIA triad model to guide information security policies



While the topic will be further developed in a future white-paper, in evaluating integrity features and trade-offs offered by public versus private blockchain solutions, it is important to remember:

– First, blockchain enhances the integrity posture. Whether public or private, blockchains offer additional guarantees compared to traditional databases when it comes to ensuring that the rules are being followed. It can identify, and resist attempts to modify data on the chain through the hashing, chaining, distribution, consensus process, and rules implementation. It does not assure accuracy of the data entered on the chain, but it does ensure the integrity of the data stored on-chain through different consensus mechanisms. Where the blockchain is the initial source of information—for example, when transactions are recording the activity of a native token, like bitcoin or other cryptocurrency, on the blockchain system—the data can be verified. However, in a supply chain implementation where information such as tracking data or weights and measures is external to the system, the data cannot be verified by the blockchain alone.

– With that being said, a public and well-established blockchain could be more appropriate to achieve information integrity goals. Getting sufficient control to rewrite the ledger over a public blockchain is more difficult for an attacker than in a private chain with less nodes.

– On timely data input and access, something that relates primarily with information availability, which requires both security and reliability at the same time across the chain of related IT services, network, and systems. This objective could be partly achieved either with a private or public chain; in a private chain where the processing power allocated to the business case can be fine-tuned to meet particular processing time constraints, while a public potentially incorporates higher level of redundancy. It is also noted that some public blockchains tend to be slower in transactions than private versions.

– Many, if not most of the purported features and capabilities of blockchain are design- and implementation specific. It is not because one design implementation includes a particular feature (privacy, transparency, strong user authentication, and so on) that others will share that feature. Security, and hence integrity and availability, should be looked at holistically. It is totally possible to achieve one's integrity goals using a private blockchain, and one's availability goals, using a public blockchain.

– There are plenty of implementation choices that would impact data integrity beyond the choice of public or private blockchain, such as smart contracts coding, wallet management, key generation and key management, off-chain activities, etc.

Interoperability and standards

Public blockchains are more interoperable today since they are based on widespread consensus about how networks should operate. By contrast, private blockchains are always dependent on different parties within a system coming together to agree on their own shared standards from scratch. It remains to be seen whether private blockchain providers can garner sufficient support to cover broad industry requirements in this way.

In parallel, organizations such as the International Standards Organization (ISO) and industry groups such as the Blockchain in Transportation Alliance (BITA), Digital Container Shipping Association (DCSA), W3C and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) are driving standardization and the development of quasi-standards as well. These efforts will help to proliferate not just technical standards but also effective methodologies for use in public and private blockchains.

Total cost of ownership

The cost per transaction, often referred to as "gas" in public blockchains, is a fee paid to the creator of a block for writing data. This cost can vary substantially and can depend on traffic, so that users may pay more per transaction as volumes go up. Private blockchains typically do not involve gas fees or limits on usage or block size, however it takes resources to maintain and support the infrastructure.

With a private blockchain the upfront costs are typically higher. Public blockchains tend to require a substantially lower upfront investment to launch a new project or application, especially when organizations deploy hash-based solutions.

Cost considerations are usually easy to resolve with side-by-side comparisons that focus on the total cost of ownership over longer periods of time.

Compliance on personal data protection

For supply chain operators considering public blockchains, personal data protection is a critical concern.

The European Union's General Data Protection Regulation (GDPR), for example, presents a robust global standard for the storage and processing of the personal data of persons living in EU member countries (for more on GDPR and blockchain, see the next white paper, Part 4, in this series, which will be released in August 2019). In addition, data protection and privacy laws in other jurisdictions may present compliance challenges.

Also, governments often demand that certain sensitive information should not be revealed on the grounds of trade and/or national security. Because anyone can join a public blockchain, it is difficult to ensure participants agree to the necessary rules on the protection of personal data. As a result, private blockchains are typically better suited to working towards a GDPR-compliant blockchain solution.

New innovations in public blockchains are pushing technical boundaries, and some public blockchains are starting to do more sophisticated ID management with obfuscation – they are initiated or linked to an organization that has greater ability to put a data policy in place. However, a robust data protection impact assessment is a must for GDPR compliance with public chains.

Immutability
The inability to change data at later points

Immutability is an essential criterion often referred to in conjunction with blockchain technology. It is a key characteristic that made the original bitcoin blockchain possible since it helped to solve the problem of documenting who had spent money and who had received it.

There is considerable discussion about whether private blockchains are immutable. Technically, they function in the same ways as public ones. However, so long as there is an entity who controls the network there is no true certainty that a record or agreement hasn't been changed after the fact. Proponents of private blockchains will argue that any system loses its value once trust has been breached, while advocates of public versions tend to argue that only true decentralization offers immutability.

Governance

Public blockchains are often governed by all, or a majority of, participants, which can lead to decisions that oppose the interests of supply chain operators. In private chains, there tends to be closer alignment of objectives among participants to begin with, so ongoing governance is often less of a concern.

That said, private chains can also experience challenges in relation to governance when the interests of diverse supply chain nodes do not align – for example, between shippers and carriers or intermediaries. The owner of a private blockchain may also make decisions counter to the interests of other participants, such as raising such as raising prices orimplementing new transaction fees.

Some of these conflicts can be avoided if the initial setup of a consortium for a private blockchain is handled properly. All parties need to have general alignment on objectives, benefits and processes. They need to agree on underlying technologies, and there needs to be a negotiation when when trade-offs occur

Other considerations

Above overview focused on important aspects of the decision-making process. It is not an exhaustive list of considerations.

Decision-makers must look at the context of their specific use case and its distinct requirements. Within heavily regulated industries, for instance, private chains will tend to be more prevalent, since data can be protected in a more tightly controlled way for compliance purposes. But for some applications that require open distribution of records or where public verifiability is required – for instance government agencies that must respect public-records laws – a public chain (public with some permissions if governments want to control certain aspects) would probably be a better fit.

MOBI (Mobility Open Blockchain Initiative) provides a case for how use case requirements drive the selection of a blockchain's structure. The organization is a non-profit consortium among carmakers and other mobility providers that defines standards for the global automotive industry. While some of its members favor private chains, there are use cases where using a public one becomes unavoidable. For example, certain use cases require public access to data, such as information that consumers may need or when insurance carriers calculate premiums. On the other hand, when supply chain or manufacturing operations are involved, most data written to the blockchain needs to remain hidden from public view.

Hybrid blockchains
Combining public and private

A hybrid blockchain is a term that organizations will come across frequently. What if you want the immutability and pervasiveness of a public blockchain, but also control over who gets to write data as well as increase in transaction speed?

The answer is a "hybrid" blockchain that combines benefits of both types. On the one hand, actual data can be stored on a private blockchain, where it is accessible to invited parties, and on the other a hash of the data can then be written to a public blockchain to ensure that no one central authority can alter or delete data. The hybrid blockchain can be a complex solution and it is not for everyone.

Case studies: Choosing a public blockchain solution

The following examples of public ledger deployment for supply chain solutions highlight the primary criteria used to select a public blockchain:

Truckl: eliminating costly mistakes along the supply chain[6]

Description of solution: In Truckl's solution, all participants in a transaction share the required documents while carriers collect data before, during and after a load is delivered. Information updates are made available on a dashboard and when exceptions occur, they are documented and all parties receive instant alerts and notifications. Every aspect of a transaction ranging from documents to photos, signatures or location data is recorded in a transaction file, which is then hashed and written to the blockchain. This provides visibility focusing on eliminating errors, miscommunication and exceptions in transport transactions.

Users capture several benefits from the use of blockchain, amongst other that participants are encouraged to act honestly and openly, there is a single source of truth for documents, and transaction files are valuable as soon as disputes or insurance claims occur. Each authorized party has access to the documents and can audit transactions using Truckl's blockchain features.

The company determined early on that its users do not need to share information directly on the blockchain and subsequently implemented a hash-based solution so that customers and business partners can validate documents (proof of existence) on the public Ethereum blockchain. The solution is censorship-resistant, and the public nature of blockchain means that Truckl has no power to interfere.

Key considerations: Data access, data integrity and security, performance

dexFreight: using Bitcoin as an underlying blockchain

Another case with a different approach is dexFreight, based in Florida and still in the beta-testing stage. The solution is built on RSK technology that adds smart-contract functionality to the public Bitcoin blockchain. DexFreight handles payments between different parties in cryptocurrency and uses smart contracts to help verify identity and create an objective reputation system among shippers, brokers and carriers. DexFreight stores hashes of sensitive attributes such as bills of lading, rate confirmations and proofs of pickup/delivery/payment on the public Bitcoin blockchain and keeps the original information stored in the enterprise cloud.

Dispatch: a new public chain for apps and analytics[7]

Description of solution: Dispatch is a new blockchain protocol, upon which applications are built. The Dispatch network uses a public chain to store transaction hashes, but it also allows transactions to link to encrypted data stored off-chain where necessary for enterprise security.

To mitigate against the slower speed typically associated with the earlier public blockchains, Dispatch uses a novel consensus algorithm called delegated asynchronous proof of stake (DAPoS).[9]

Supply chain applications building on the Dispatch platform include an item offering manufacturers blockchain-based authentication to provide proof of authenticity and proof of ownership for the goods they produce. The XY Oracle Network is experimenting with the Dispatch chain for sharing geolocation data gathered from its global network of Bluetooth and GPS/cellular beacons.

Dispatch is also developing an analytics platform that will allow companies to glean operational insights by querying datasets that they don't actually hold in custody. That solution, called zero-knowledge analytics, aims to offer the analytics to enterprises concerned about sharing sensitive data with competitors.

Key considerations: Data access, system performance, personal data protection

Public permissioned blockchains

Sovrin: the need for public permissioned

Description of solution: The Sovrin ledger is publicly readable. Sovrin is run by "stewards", organizations that have volunteered to operate one of the nodes. Each node has a copy of the Sovrin ledger and maintains consensus of it. It is considered a public blockchain because anyone can read from and write to the ledger. Yet, it is also permissioned in that stewards must agree to a set of rules defined by the Sovrin Foundation. These rules ensure that no single group of stakeholders can become too powerful, leaving flexibility to change stewards quickly to ensure that a diversity of industries and regions is represented. This ensures "designed decentralization".

Key considerations: Data access, security, personal data protection

Wave: public networks with permissioned mining

Description of solution: The start-up Wave offers a document solution that allows members of a supply chain to directly negotiate and transfer bills of lading and other trade documents on a decentralized network. While the solution is built on public networks to ensure negotiability and transferability, the mining validation is done in a permissioned way to eliminate know your customer (KYC) and anti-money laundering (AML) exposures and reduce energy use.

Key considerations: Data access, data integrity and security, system performance.

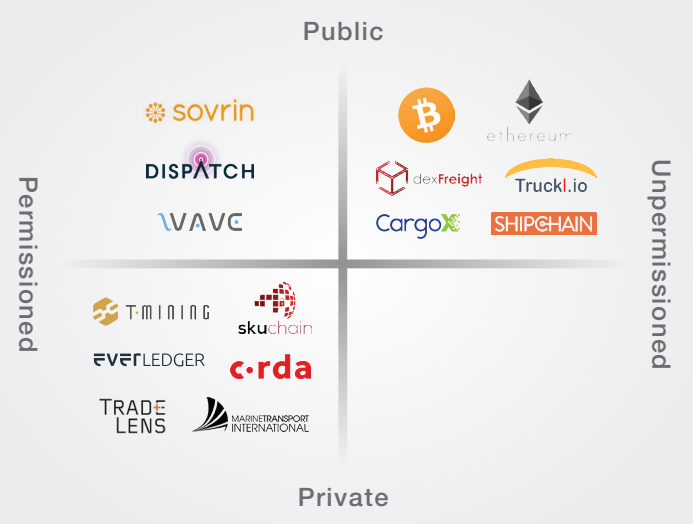
Governments: examples of public permissioned

While both public and private blockchains are prevalent in government blockchain solutions, for many, some form of permission is required, though an element of public disclosure is also a must. Land registries, for example, should not be open to anyone who wants to update them, yet the data they hold should be readable to everyone. For a blockchain application, such requirements often mean there should be a public verification process to ensure that ledger entries are correct, while only a select few nodes can add new entries over time. Lacking this capability can quickly lead to a false sense of security and ultimately to public distrust.

The 2018 report Blockchain and Suitability for Government Applications by the Department of Homeland Security (DHS)11 sees supply chains as an area of government interest in which DLT appears to be well suited to delivering real benefits. The report highlights that: "A permissioned blockchain may be a better option for government use since all parties afford some degree of trust to a central authority, permitting selection of a consensus mechanism that is more efficient and less expensive compared to a permissionless blockchain."

The following quadrant structure is a simplified representation of public/private and unpermissioned/ permissioned orientation for some applications, services, networks and protocols.

Figure 5: Blockchain structure How are companies



Examples of private blockchain solutions: factors that influenced decision making

The following are examples of private ledger deployment for supply chain solutions that highlight important criteria used in the selection of a private blockchain:

Marine Transport International (MTI): data privacy compliance

Description of solution: MTI, a UK-based digital logistics enabler, selected a private permissioned blockchain to ensure adequate access control and thereby reduce data liability. MTI's solution helps to manage personal identifiable information (PII) under the GDPR regulations or prohibited data as per the network's governance framework from entering a distributed ledger.

"Our approach has been to create the necessary digital infrastructure through middleware that allows actors to control their own data without storing it," explains Jody Cleworth, founder and chief executive officer of MTI.

Key considerations: Data access, personal data protection, security

Port of Valencia: improving container management

Description of solution: The Port of Valencia solution, called GESPORT 4.0, aims to digitize documentation, increase process efficiency and ease communication. The port experimented with private and public chains and recently developed a private permissioned solution for container management that is based on Hyperledger Fabric. The organization selected a private permissioned blockchain solution for several reasons, including the existence of sensitive data, the need for governance via a community of stakeholders, the ability to store data and the avoidance of convoluted consensus mechanisms. In addition, decision-makers looked into performance, transaction volume, system scaleability and security prior to their commitment to Hyperledger Fabric.

Key considerations: Data access, governance, personal data protection, system performance

Port of Genoa: introduction of blockchain in its port community system

The Port of Genoa, a complex business community in which a number of private and public entities cooperate in modal shift operations, is supported by an information and collaboration platform called the Port Community System.

In 2018, the Genoa Port Community launched a project aimed at the introduction of blockchain in port processes. The project includes the creation of a private blockchain and the instrumentation of the Port Community System to have it issue blockchain transactions in correspondence of inter-entity port operations while software interfaces allow port operators to feed the blockchain directly.

The choice of a private blockchain was justified by the need to create a blockchain rapidly to focus on applications rather than on technology. At the same time, a parallel line of research was activated to investigate the possibility of migrating to a public blockchain as well as the integration and the interoperation of multiple blockchains.

Key considerations: Governance, personal data protection, system performance, interoperability

Everledger: making a private chain a diamond's best friend

Description of solution: Everledger, a private blockchain solution focused on diamond traceability, uses high-resolution imagery at every touchpoint along the supply chain to uniquely identify each stone and record its characteristics, serial number, chain of possession, location and condition, along with certificates of authenticity and payment documents. The solution requires privacy, not least because the whereabouts of high-value items needs diamond traceability, uses high-resolution imagery at every touchpoint along the supply chain to uniquely identify each stone and record its characteristics, serial number, chain of possession, location and condition, along with certificates of authenticity and payment documents. The solution requires privacy, not least because the whereabouts of high-value items needs to remain concealed.

Key considerations: Data access, system performance, data integrity and security

Key questions

It is clear that there is no silver bullet to enable organizations to choose between public and private blockchain. Users first need to understand the characteristics, advantages and drawbacks that each type of chain offers before making an educated decision.

A proactive approach to understanding the technology is a must. Companies that truly grasp how to use a new technology early on are the ones that capture its benefits before competitors do. They realize cost savings or increases in profitability first, which they can use to pull further ahead of the pack.

Selecting the right blockchain configuration plays a major role in situations in which the vision of an organization extends to bringing multiple partners, vendors or customers together. One major advantage of blockchain technology is its ability to furnish data as a single shared version of the truth.

Throughout its end-user and technology-provider interviews, the Centre for the Fourth Industrial Revolution at the World Economic Forum has found there are seven vital questions that lead up to defining the answer about blockchain configuration.

1. **Is there a blockchain consortium or trade partnership that is already active in your industry or specific to the use case?** If so, decision-makers need to think hard about whether they wish to deviate from it. It is often substantially cheaper and less time-consuming to accept an imperfect existing solution over a custom-made one. After all, the latter tends to become useless in cases in which a consortium solution eventually evolves into an industry standard. Obviously, if organizations believe they can mount a credible challenge to existing solutions, gain critical mass to make their alternative successful and possibly establish it as a dominant solution, this is a viable strategic option.

   To a lesser degree, the same is true for initiatives within organizations. If there are ongoing blockchain projects or deployments within a company, it is often easier and faster to exploit the underlying technology before embarking on a second or third initiative that uses a new platform or protocol. In this manner all previous investments can be employed.

2. **Is shared data proprietary and confidential?** If this is the case, the decision turns to which data should be kept on-chain and how much needs to be kept there. As soon as shared confidential data is written to a blockchain, a private configuration or hash-based solution on public blockchains is usually the only way to handle this situation. In cases in which proprietary databases can keep shared and confidential data secure, a public configuration may be better for an organization's needs.

   With confidential and proprietary shared data, is public verifiability still required? If yes, a public permissioned system will likely be required.

3. **Does the data contain personal information?** In cases in which personal data is written, data protection and data privacy laws such as GDPR need to be considered. Because anyone can join a public permissionless blockchain, it is impossible to ensure that participants agree to the necessary rules on the protection of personal data. As a result, if data must be kept on-chain, the permissioned blockchains can be employed to work towards a GDPR-compliant blockchain solution.

4. **Is proof of existence enough for your use case?** Proof of existence (the ability to show that a document has not been changed since it was written to the blockchain) builds trust, enables higher levels of accountability and serves as a great way to resolve conflicts and disputes. If so, a solution in which a hash is written to the blockchain and used to ensure that documents have not been altered is ideal. In these situations, a public blockchain is much faster to implement and the variable cost of writing data can be contained through the aggregation of entries. For instance, many hashes can be combined into a single hash that is subsequently written to a public blockchain, which saves fees for block creation.

5. **Does your solution require smart contracts, for example, to settle payments in ways that are faster and cheaper than currently available means?** The use of smart contracts itself is not limited to private blockchains; however, public configurations often need to be augmented through an additional technology layer to add smart contract capabilities where they do not exist on public blockchains – similar, for instance, to the way in which RSK manages the Bitcoin blockchain. The Ethereum protocol is a good example of public blockchains that allow smart-contract capabilities.

6. **Does your solution require near real-time processing or does it need to handle large datasets?** In either case, private configurations are usually a better solution. Public blockchains, at least as they exist today, are severely constrained when it comes to file size, processing speed, number of transactions and the cost of processing them.

7. **Do you require a high degree of control over blockchain governance?** If you do not, because the way in which the current blockchain configuration works is sufficient, then reputable public blockchains are often superior and also typically less prone to drastic changes since large numbers of users need to agree to any form of alteration. In cases in which your organization deviates noticeably from standards or requires complete control over business processes, data formats and transaction processing, a private solution is likely the better choice.

Conclusion

When the internet was invented in the 1960s, its objective was to serve as a communications backbone in case of national emergencies. When the world wide web was invented in 1989, its main purpose was the efficient sharing of academic findings and research. When blockchain became known because of bitcoin's invention in 2008, its sole purpose was the avoidance of double-spending for bitcoin.

It is fair to say that all three technologies have slightly deviated from their plotted path, the internet and web obviously more so than blockchain. Yet the latter is still in its infancy, and it is difficult to predict where it will be in ten or 15 years.

Is blockchain a new application programming interface (API) that not only addresses challenges around data sharing, but secures and immortalizes data at the same time? Will there soon be blockchain solutions that write transactions to two or more blockchain types simultaneously? Are large-enterprise application vendors going to develop the capacity to instantiate blockchains for projects or even specific types of transactions through easy and fast configuration of business processes and underlying technology components? Will all of us become accustomed to higher levels of privacy and control over our own data to ensure that decentralized IDs become mainstream? Is it conceivable that enterprise resource planning (ERP) providers such as SAP or Oracle will eventually offer blockchain kits that will allow fast configuration of private blockchains on an as-needed or project basis as long as everyone adheres to the same standards?

The industry is still in the infrastructure-building phase of the technology, in which it can be largely cost-prohibitive for small players to innovate or to build comprehensive solutions. Yet there are more open-source components to blockchain than was the case for many other technologies, which could lead to a faster diffusion and adoption cycle.

The answers to these and many more pressing questions are determined by what is useful, technically viable, supported by the ecosystem ("ecosystem attractiveness") and desired by a large number of users. Given this uncertainty, decision-makers would be best advised not to get distracted by the public-versus-private debate and to stay focused on the context of their selected use case and distinct requirements.

Time will tell.

Appendix

Glossary of terms

Anti-money laundering (AML): a set of laws and regulations designed to ensure that financial services companies do not aid in criminal and/or terrorist enterprises, also known as the rules in place to deter the next *Breaking Bad* car wash. Efforts to combat money laundering and terrorism finance include KYC requirements, suspicious activity reports and currency transaction reports, all of which require financial institutions to investigate and report any customers or transactions that could be furthering a criminal enterprise. AML obligations can be burdensome, but failure to comply can result in heavy criminal and civil penalties. Global AML obligations differ by jurisdiction.[8]

Consensus protocol: a set of rules and process(es) that determines how nodes reach agreement about a set of data and whether to approve (validate) transactions in the network. As per the MIT Center for Information Systems Research's definition, it is defined as the algorithm used to validate transactions and blocks. Consensus may rely on cryptography and a percentage of participant votes (nodes) to validate a block. Consensus protocols must also provide a mechanism for resolving block conflicts. At the other end of the spectrum, in some privately owned blockchains the owner may decide that only the transacting parties and one other node are required to validate. The amount of time and computing power necessary to run a blockchain vary significantly based on the consensus type and percentage of nodes required.

Cryptocurrency: generic term for any digital asset or "token" that can be mined, purchased or transacted within a blockchain or distributed ledger network. The most famous cryptocurrency is bitcoin and others include ether, Litecoin and NEO, in addition to more than 1,000 others.

Cryptographic hashing functions and pointers: cryptography tools used in blockchain networks. Hashing functions turn any input (e.g. a password or jpeg file) into a string of characters that serves as a virtually unforgeable, unique and encrypted digital fingerprint of the data, called a hash. A hash pointer records where a certain amount of information is stored. Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs) and other forms of authentication.

Cryptographic techniques/cryptography: the methods of using mathematical ciphers (codes) to protect or "encrypt" transactions as they are being stored or shared.

Distributed ledger technology: software that uses a blockchain or similar data structure shared over a network of participants who distribute and verify information about transactions.

General Data Protection Regulation (GDPR): a regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.[9]

Immutability: data stored in a blockchain is very hard to change, even by administrators. However, absolute immutability does not exist.

Know your customer (KYC): the requirement, pursuant to the US Bank Secrecy Act, that financial institutions conduct due diligence on their customers prior to engaging in transactions with them. The goal is to avoid inadvertently engaging in criminal activity by furthering money laundering, terrorism finance or other criminal enterprises, or engaging in business with persons on the Office of Foreign Assets Control sanctions list.[10]

Network nodes: nodes represent network agents or participants, such as banks, government agencies, individuals, manufacturers and securities firms within a distributed network. Depending on the permissions set in the network, they may be able to approve/validate, send or receive transactions and data. They may validate transactions through a consensus protocol before committing them to a shared ledger (though not all nodes perform validations depending on the system, architecture and other elements).

Proof of existence: the ability to show that a document has not been changed since it was written to the blockchain.

Token (for a blockchain network): a digital asset used in a blockchain transaction. A token can be native to the blockchain, such as a cryptocurrency, or it can be a digital representation of an off-chain asset (known as tokenized asset), such as the title to a house.

UN/CEFACT MMT model: the foundation underlying message structures that are currently being developed to reflect the current interests of our sector for exchange-syntax independent data-exchange structures and standardized APIs.

Acknowledgements

The World Economic Forum's Centre for the Fourth Industrial Revolution Blockchain for Supply Chain project is a global, multi-industry, multistakeholder endeavour aimed at co-designing and co-creating frameworks to encourage deployment. The project engages stakeholders across multiple industries and governments from around the world. This report is based on numerous discussions, workshops and research, and the combined effort of all involved; opinions expressed herein may not necessary correspond with those of each one involved with the project.

Sincere thanks are extended to the generous commitment of the lead authors – Chris Hanebeck and Peter McKay; also to those who contributed their unique insights to this report. We are also very grateful for the support of the Fellows at the Centre for the Fourth Industrial Revolution dedicated to the project: Soichi Furuya from Hitachi and Francis Jee from Deloitte.

Lead Authors

Hanns-Christian Hanebeck, Founder and Chief Executive Officer, Truckl, United States

Nadia Hewett, Project Lead Blockchain and DLT, World Economic Forum, United States

Peter A. McKay, Content Producer, Dispatch Labs, United States

Contributors

Adrien Ogee, Project Lead for Cyber Resilience, World Economic Forum, Switzerland

Avi Dutt, Assistant Director, Ministry of Shipping, India

Andrew Ballinger, Project Specialist, World Economic Forum, United States

Ashley Lannquist, Project Lead Blockchain and Distributed Ledger Technology, World Economic Forum, United States

Ben Duto, Art Director, Dispatch Labs, United States

David Treat, Managing Director, Accenture, United States

Dominique Guinard, Founder and Chief Technology Officer, EVRYTHNG, Switzerland

Francis Jee, Manager, Deloitte (and World Economic Forum Fellow), United States

Gadi Benmoshe, Chief Information Officer, Israel Ports Development & Assets Company, Israel

Henrik Hvid Jensen, Senior Blockchain Advisor, Trustworks, Denmark

Jake Kuczeruk, Director of Partnerships, Dispatch Labs, United States

Jason Spasovski, Senior Consultant, Deloitte, Denmark

Jens Munch Lund-Nielsen, Head of Global Trade and Supply Chains, IOTA Foundation, United Kingdom

Jesper Nielsen, Manager, Deloitte, Denmark

John Choi, Chief Executive Officer, MarkAny, Republic of Korea

Lucy Hakobyan, Head of Program, Mobility Open Blockchain Initiative, United States

Madhav Durbha, Group Vice President, Industry Strategy, LLamasoft, Inc., United States

Massimo Maresca, Professor of Computer Engineering, Port of Genoa, Italy

Matt McGraw, Chief Executive Officer, Dispatch Labs, United States

Milly Perry, Professor, Tel Aviv University, Israel

Raghu Kiran N, New Venture Consultant, World Food Programme, Germany

Rasmus Moelbjerg, Director, Deloitte Digital, Denmark

Robert Maslamoney, Managing Director, Maersk Angola

Sara Golden, Independent Researcher and Sr. Compliance Associate, USA

Soichi Furuya, Senior Researcher, Hitachi (and World Economic Forum Fellow), United States

Sumedha Deshmukh, Project Specialist, World Economic Forum, United States

Tae-il Kang, Director General, Korea Customs Service, Republic of Korea

Wolfgang Lehmacher, Senior Supply Chain Executive, Hong Kong

Young-mi Kim, ICT Project Manager, Korea Customs Service, Republic of Korea

Yusuke Jin, Senior Researcher, Hitachi, Japan

Commentators

Alexander Varvarenko, Chief Executive Officer, SHIPNEXT, Germany

Max Fang, Adjunct Professor at University of California, Berkeley - School of Law, United States

David Libatique, Deputy Executive Director, Stakeholder Engagement, Port of Los Angeles, United States

Jaka Mele, Chief Digital Officer, CargoX, Slovenia

Jody Cleworth, Chief Executive Officer, MTI, United Kingdom

Kazue Sako, Distinguished Researcher, NEC, Japan

Rene Alvarenga, Senior Director of Product Management, GE Transportation, United States

Robert Learney, Lead Technologist – Blockchain and Distributed Ledger Technology, Digital Catapult, United Kingdom

Sridhar Thati, Chief Technology Officer, Everledger, United States

Tomaž Levak, Co-founder, OriginTrail, Slovenia

Žiga Drev, Co-founder, OriginTrail, Slovenia

Zvika Krieger, Head of Technology Policy and Partnerships, World Economic Forum, United States

Endnotes

1. Satoshi Nakamoto's 2008 Bitcoin whitepaper: https://bitcoin.org/bitcoin.pdf

2. Deloitte: https://bit.ly/2z6dnpS

3. Federal Reserve Bank of Minneapolis, February 2019, Ten troublesome blockchain terms: What's accurate? What's not?

4. For a discussion of the pitfalls of the shifting blockchain lexicon, see: Walch, Angela. The Path of the Blockchain Lexi con (and the Law) (March 24, 2017). 36 Review of Banking & Financial Law 713 (2017). Available at SSRN: https://ssrn.com/abstract=2940335

5. Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction (World Economic Forum, April 2019): https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply chains-part-1-introduction

6. Hanns Christian Hanebeck, Founder and Chief Executive Officer, Truckl, is a co-author of the report

7. Peter A. McKay, Content Producer, Dispatch Labs, is a co-author of the report

8. Latham & Watkins, The Book Of Jargon® – Cryptocurrency & Blockchain Technology: https://www.lw.com/bookofjargon-apps/boj-CryptocurrencyandBlockchain

9. European Union (EU) Regulation 2016/679

10. Latham & Watkins, The Book Of Jargon® – Cryptocurrency & Blockchain Technology: https://www.lw.com/bookofjargon-apps/boj-CryptocurrencyandBlockchain

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org