Blockchain:

six key risks to be aware of

Over the past decade, the use of so-called 'distributed ledger technology' has increased rapidly. One of the most well-known types of distributed ledger technology is 'blockchain'.

Blockchain (and similar technology) is often praised as being safe and 'unhackable', with the ability to bring a greater level of trust to transactions and data that may not be offered by traditional technology solutions. However, blockchain is not without its own risks and challenges. In this article, we consider the most common risks and challenges to be aware of when implementing a blockchain solution.

A reminder: what is blockchain?

Blockchain is a form of distributed ledger technology. At its simplest, a distributed ledger (also known as a general ledger, or distributed general ledger technology) is a database in which data is consensually held, controlled, shared, synchronized and validated by the network's stakeholders, also known as 'nodes'. In this sense it is often described as being decentralised. Once it has been stored, it is – in general – impossible to alter or remove the encrypted transactions and data on the blockchain. This results in a secure and self-verifying database.

Given blockchain's well-known potential to offer security and verification benefits to its users, introducing blockchain technology presents an attractive prospect. However, as with any technology solution, the technology behind blockchain is not infallible. In our view, the key risks and challenges to be aware of are:

01 Security and liability

Whilst security is integrated within blockchain technology, even the strongest blockchains can come under attack by cyber-criminals. Although blockchains are considered to be very secure, their security level is directly proportional to the amount of hash computer power that supports it, there are still several ways a blockchain can be attacked (such as a Finney attack, DDoS attack, routing attack etc...). Cyber-attacks are on the rise, with some cyber-analysists expecting global cyber-crime costs to grow by 15% per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD.

In this context, it is of utmost importance to ensure implementation of proper organisational and technical security measures to monitor potential (personal) data breaches, with robust policies in place. This includes having a robust business continuity plan and governance framework to mitigate such risks. It is also critical for organisations to understand where liability for cyber-attacks lie and whether existing insurance policies will provide adequate protection in the event of a cyber-attack.

02 Endpoint issues

The interface between each end user and a blockchain solution is often termed an "endpoint". Endpoints include computer systems and other devices that connect to the solution. Whilst endpoint vulnerabilities are not down to the blockchain technology itself, any blockchain solution is only as strong as its weakest endpoint.

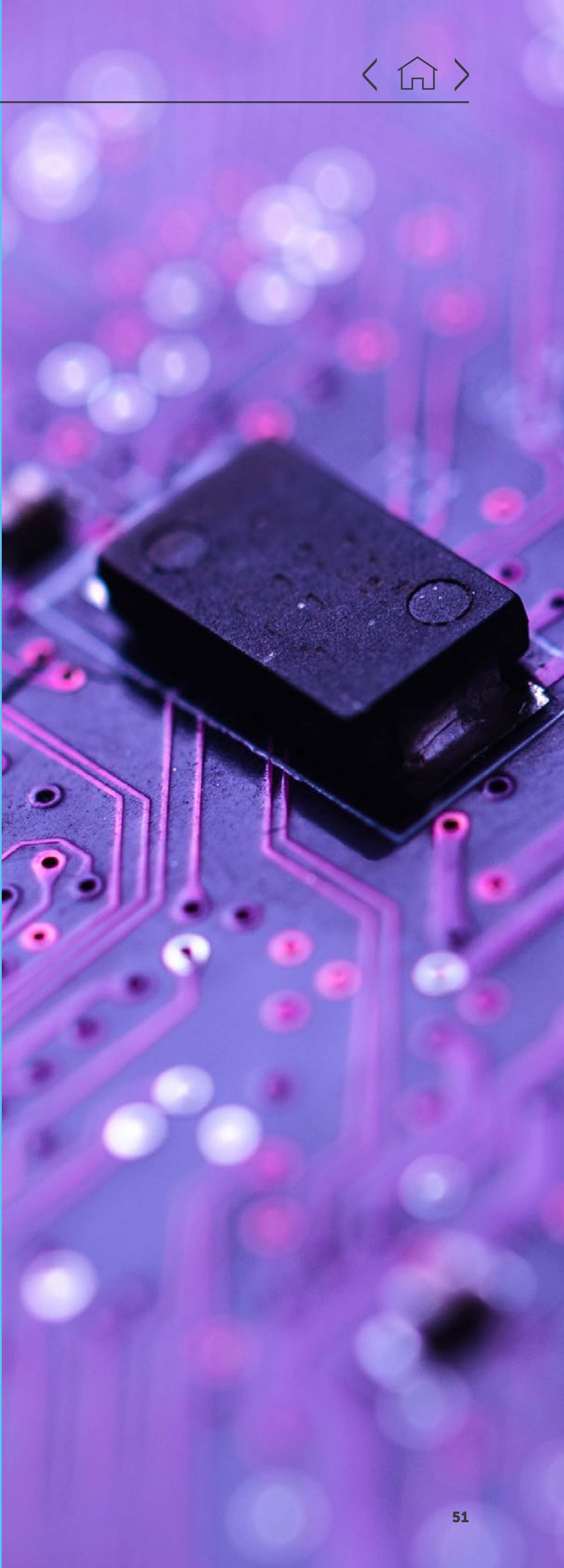
Endpoints can be vulnerable to cyber-attacks, whether that is due to human error or technical issues with firewalls and security patches. Blockchain providers and customers should ensure robust security protocols and requirements are in place for all end users of a blockchain based solution, given the potential of endpoint vulnerabilities.

03 Third parties

Third party providers and vendors feeding into the system ought to be carefully vetted to ensure they have the capability to offer the level of security and resilience needed.

Also, as with any technology, blockchain providers and customers should, prior to the purchase and use of blockchain solutions, negotiate appropriate contractual rights and obligations, such as a contractual defects liability period, robust service levels, and key performance indicators. This is to ensure that it is clear where liability and responsibility for issues lies (security, programming defects) and how they will be addressed.

Where a provider offers standard terms and conditions, it is important to be aware of any standard provisions on limitation of liability, governing law and jurisdiction, termination, and the contractual possibility to block certain users that violate guidelines or breach the terms and conditions.



04 Intellectual property

There are two types of blockchain that can be distinguished: blockchain can be ‘permissionless’, which means that there is no special authority that is able to deny permission to participate in the blockchain and to add any transactions to the ledger (also known as “public blockchains”), or ‘permissioned’, which means that there is a limited group of participants that retain the power to add transactions to the ledger (also known as “private blockchains”).

In the context of an infringement of an intellectual property right, permissionless blockchains can give rise to issues. If an intellectual property protected work is recorded on the blockchain, it can be difficult in proving the relevant ownership and identifying any potential breaches, handling transfers or licenses to third parties.

Prior to using blockchain, it must be taken into account what type of data will be shared, and whether this data is, for example, subject to any intellectual property rights or trade secrets, and whether any contractual rights and obligations of the blockchain provider may apply.

05 Privacy

The decentralised nature of the blockchain makes it difficult to identify the person responsible for processing data, which in turn can cause issues in guaranteeing a whole range of data subjects’ rights. The distributed nature of the blockchain also requires a high degree of transparency, which conflicts with the principle of data protection by design and default settings.

As an example, the permanent nature of data within a blockchain prevents the possibility of guaranteeing the right to be forgotten, and clashes with the general principles, including data minimization and storage limitation. At a time when the litigation landscape in the field of data protection is evolving at a rapid pace (and depending upon the much-awaited judgment of the Supreme Court of the United Kingdom in the case of Lloyd v Google), claims may soon be allowed for loss of control of personal data, without the data subject arguably identifying any specific financial loss suffered, which could lead to substantial group claims against the blockchain and its users.

Our experience is that within the industry, for example the supply chain space, systems are most commonly permissioned and access is limited to designed participants (and may be subject to AML /KYC checks) and the roles of the participants is limited in what they can do and see on the blockchain. For example, platform participants can only access information related to their data and the interactions or transactions with other platform participants. This is absolutely critical for most of our clients, many of whom operate in highly regulated industries, where privacy and the security of the blockchain and the individual nodes in which transactions take place is its most critical feature.

06 Jurisdictional issues

If a dispute arises, for example between a blockchain provider and a customer, it is important to determine which rules of which country apply in disputes about blockchain. If a provider and a customer are located in different countries, international private law should be invoked. On the basis of international private law, it should then be determined i) which court is competent, and ii) which law is applicable. It is likely that there will need to be some developments in this area, with thought given as to what “place of performance” means in the context of blockchain. It may be that the courts will need to consider a number of elements, such as:

- where substantive performance (e.g. provision of an associated deliverable or service) occurs
- where relevant parties or the majority of users are located
- where anybody with responsibility for the blockchain is located
- what the choice of law is in any relevant associated/ underlying natural language contract

Potential issues can be prevented by explicitly entering into an agreement or accepting terms and conditions that designates a competent court and governing law.

The future outlook

Eversheds Sutherland have recently been involved in the **UK Law Commission's consultation on Smart Contracts** (focusing on legally binding contracts in which some or all of the terms are recorded in or performed by a computer program deployed on a distributed ledger) providing our views on the ways in which smart contracts are being used, and the extent to which the existing law of England and Wales can accommodate them. The UK Law Commission are analysing the responses to inform their scoping study, which is due to be published later on this year. The outcome of this study could have a wider ranging impact on the way in which blockchain technology is treated by the courts in England and Wales.

Additionally in the Netherlands, governmental and regulatory bodies, universities, research organisations and (multi)national private entities have formed a coalition called **'the Dutch Blockchain Coalition'**. Currently, the Dutch Blockchain Coalition is creating and facilitating an environment in which reliable blockchain applications can be developed, promoted and utilized in a secure manner. Also, the Netherlands Authority for the Financial Markets and the Central Bank of the Netherlands have jointly established 'the Innovationhub', which offers businesses support on queries regarding innovative financial products and services. We expect that such initiatives will lead to interesting use cases and collaborations, and could potentially provide the basis for new legislation and regulations.

Olaf van Haperen
Partner
olafvanhaperen@
eversheds-sutherland.com

Ridah Iqbal
Principal Associate
ridahiqbal@
eversheds-sutherland.com

Robbert Santifort
Senior Associate
robbertsantifort@
eversheds-sutherland.com

Sarah Zadeh
Associate
sarahzadeh@
eversheds-sutherland.com

Aimee Taroni
Associate
aimeetaroni@
eversheds-sutherland.com