

**Baker
McKenzie.**

BLOCKCHAINS AND LAWS. Are they compatible?

A white paper championed by Baker McKenzie
in collaboration with R3



CONTENTS

**EXECUTIVE
SUMMARY**

04

INTRODUCTION

05

**DEFINING
BLOCKCHAINS
AND DISTRIBUTED
LEDGERS**

07



**GLOBAL DATA
PROTECTION LAW**

13

**BLOCKCHAINS
VERSUS
DISTRIBUTED
LEDGERS**

16

**DATA PROTECTION
LAWS IN VARIOUS
JURISDICTIONS**

18

CONCLUSION

20

EXECUTIVE SUMMARY

Any distributed ledger used by an enterprise or industry needs to conform to data requirements in the countries in which it operates. Existing blockchains based on Bitcoin and Ethereum codebases can indiscriminately broadcast private data to all participants of a network, and therefore may not always be suitable for use in financial services.

Distributed ledgers have been developed that share certain data only with participants who need to see it, most notably R3's Corda. These distributed ledger technology implementations are more flexible and can more easily meet existing and potential future data requirements.

Legal requirements are evolving rapidly and it is important to ensure that the implications of new technologies are reviewed by appropriate counsel.

INTRODUCTION

Blockchains have given way to other distributed ledger technologies (DLT)

Distributed ledger technology has evolved significantly since 2009 when the first bitcoin was mined and the Bitcoin blockchain was created. Today, two notable public blockchains exist: Bitcoin and Ethereum.

However, neither of these blockchains target the problems specific to the financial services industry. Bitcoin was designed to facilitate the exchange of unstoppable, uncensorable digital cash, and Ethereum was designed as an unstoppable, uncensorable “world computer.” Neither of these goals are fully aligned with the requirements of the regulated financial services industry.

During the blockchain hype in 2013-15, banks and other financial institutions ran experiments, many of which used private

“forks” or clones of Bitcoin and Ethereum software. They pointed the software inwards, creating private blockchain networks inaccessible from the outside world, rather than pointing outwards to the public databases.

Over time, these clones were adapted to try to meet institutional needs. However, it has become apparent that blockchains where transaction data is broadcast indiscriminately to all members of a network do not meet the needs of financial institutions.

One of the issues with a broadcast blockchain is the lack of privacy of the shared data. In Bitcoin and Ethereum, each computer on the network receives a record of every single transaction and update, and each computer validates these transactions according to a set of pre-programmed rules. The transactions contain details in clear, unencrypted text, including sending account, receiving account, amount, and any other details that are necessary for a computer to judge whether a transaction is valid. Intuitively, in an industry network, particularly financial services, it is not necessary or acceptable for all transactions to be revealed to all participants in real time.

However these experiments have created a new wave of enthusiasm for developing newer, more appropriate technology that helps to solve problems of cost, replication, risk, errors, and inefficiencies pervasive in the financial services industry.

The goals of public blockchains are divergent from the goals of the regulated financial services industry.

The financial services industry is ripe for DLT

The financial services industry consists of a network of parties who know each other, but each control their own books and records. They are not allowed to trust each other to maintain this, nor would they want to. Therefore, they individually record, process, and store data, then verify with each other that their versions of the numbers are correct.

Distributed ledgers can bridge the gap between these data silos to create a system of shared facts that evolve as commerce happens. These ledgers can be trusted to be accurate from the beginning, reconciling

as they go, without the need for multiple reconciliation handshakes after every calculation, or becoming beholden to third-party golden sources that own and control the valuable data.

The next generation of distributed ledgers

The next generation of distributed ledgers is not blockchains. They are being designed and created to address the needs of regulated financial institutions. They are inspired by blockchains, but solve for the privacy and scalability needs of the industry.

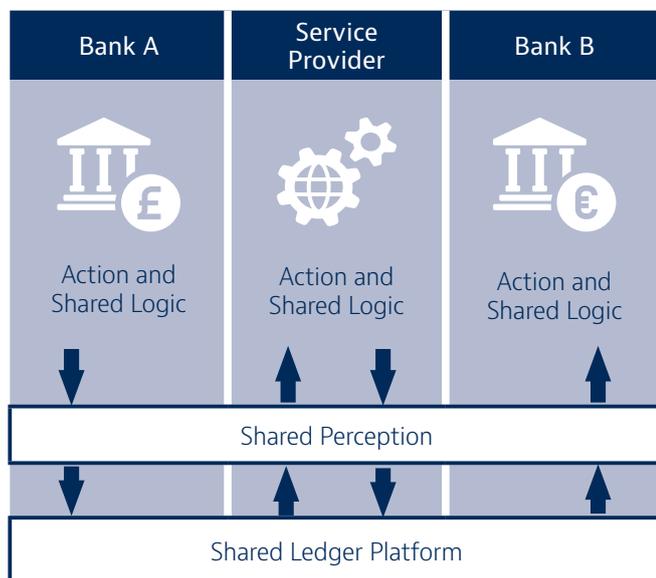
Distributed ledgers can be trusted to be accurate without the need for multiple reconciliation handshakes after every calculation.



DEFINING BLOCKCHAINS AND DISTRIBUTED LEDGERS

Both blockchain ledgers and non-blockchain ledgers fall under the general category of distributed ledgers, or shared or peer databases, where control of data is shared only by relevant participants in the network.

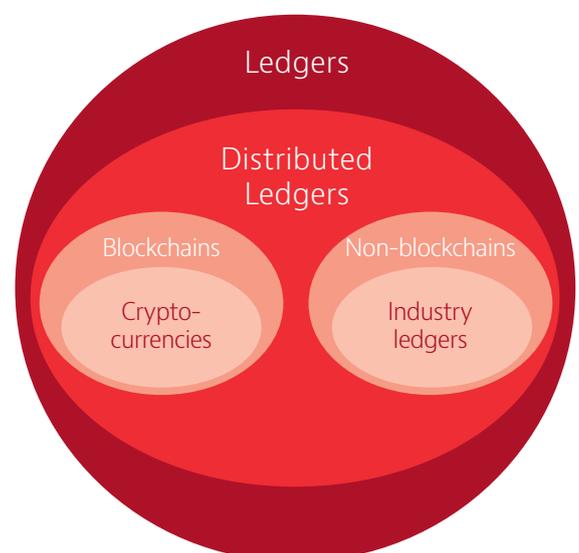
Shared Ledger Vision



Public blockchain networks ensure that all participants run a full identical database representing every single transaction bundled in blocks — everyone sees every transaction. This is a design solution that meets the requirement for public blockchain networks to have unidentified, untrusted data-writers and validators who do not

need to be vetted by an administrator. The financial services industry does not have this requirement. In fact, it has the opposite requirement — entities must be known, identified, and vetted.

Emerging shared ledgers replace this with a more nuanced model where only those who need to agree on the specifics of a particular transaction see and agree on it — certain people see certain transactions. This resolves a major privacy issue that is prevalent in public blockchains given that a disinterested third party on this type of network does not need to know that a transaction has taken place or need to validate it.



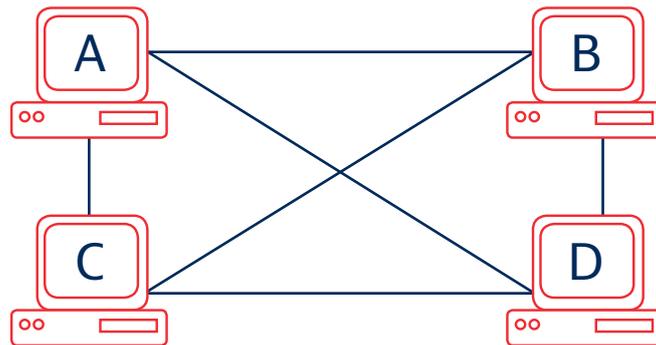
Broadcast Blockchain

Bank A's Ledger

ID	Fact
1	Bank A pays bank B \$5.
2	Bank B purchases bond X from issuing bank A.
3	Bank C purchases bond X from bank B.
4	Bank C enters a credit default swap with bank D.
5	Bank D owes bank B \$10.

Bank B's Ledger

ID	Fact
1	Bank A pays bank B \$5.
2	Bank B purchases bond X from issuing bank A.
3	Bank C purchases bond X from bank B.
4	Bank C enters a credit default swap with bank D.
5	Bank D owes bank B \$10.



Bank C's Ledger

ID	Fact
1	Bank A pays bank B \$5.
2	Bank B purchases bond X from issuing bank A.
3	Bank C purchases bond X from bank B.
4	Bank C enters a credit default swap with bank D.
5	Bank D owes bank B \$10.

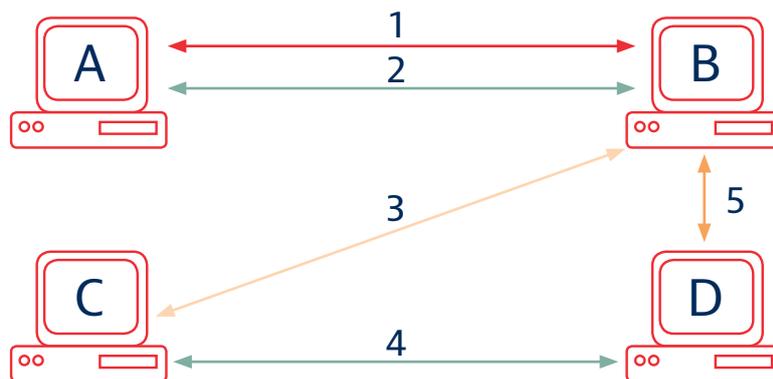
Bank D's Ledger

ID	Fact
1	Bank A pays bank B \$5.
2	Bank B purchases bond X from issuing bank A.
3	Bank C purchases bond X from bank B.
4	Bank C enters a credit default swap with bank D.
5	Bank D owes bank B \$10.

Shared Ledger

Bank A's Ledger	
ID	Fact
1	Bank A pays bank B \$5.
2	Bank B purchases bond X from issuing bank A.

Bank B's Ledger	
ID	Fact
1	Bank A pays bank B \$5.
2	Bank B purchases bond X from issuing bank A.
3	Bank C purchases bond X from bank B.
5	Bank D owes bank B \$10.



Bank C's Ledger	
ID	Fact
3	Bank C purchases bond X from bank B.
4	Bank C enters a credit default swap with bank D.

Bank D's Ledger	
ID	Fact
4	Bank C enters a credit default swap with bank D.
5	Bank D owes bank B \$10.

In reality, only certain participants need to see data that is being agreed upon. You don't want everyone seeing everything.

Physical data centers

The physical location of distributed ledger network participants drives legal complexities.

Network participants	Single jurisdiction	Multiple jurisdictions
Single organization	<ul style="list-style-type: none"> ■ An organization such as a local bank may have data centers replicating data within the borders of one country. ■ They may use a public or private cloud service provided by a third party. 	<ul style="list-style-type: none"> ■ An organization such as a multinational bank, with multiple legal entities, may have data centers in different countries. A distributed ledger may pass data across borders.
Multiple organizations	<ul style="list-style-type: none"> ■ This may be a group of banks in one country using one distributed ledger for a specific local asset. 	<ul style="list-style-type: none"> ■ A group of banks may communicate with each other across borders using a distributed ledger.

Based on the boundaries of the network, different legal questions emerge. However, broken down, the elements making up distributed ledgers are familiar:

- **Data at rest:** Data is stored on computers. The computers can be owned and managed by the entity who is responsible for the data, or it could be computers rented from another entity through cloud computing.
- **Data in motion:** Data is passed from one computer to another.
- **Regulated data:** Some of the data may contain personally identifiable information (PII) about individuals or businesses, or private data, or other data that is subject to different local regulations.
- **Encryption:** Some data may be encrypted either at rest or while in motion, or both.

Some contracts in practice

How does a distributed ledger work in practice? We describe three common examples of financial contracts — digital cash, a zero coupon bond, and an interest rate swap.

Cash

In this example, “cash” means a demand deposit from an institution, like a current account balance, ie, a liability of the institution and an asset of the customer.

For a “cash” contract transaction on a distributed ledger, the relevant data elements are:

- **Current owner** (this could be an individual or an entity, denominated by an account number).
- **Currency** (this is a three-letter code, eg USD).
- **Amount to be transferred** (this is a number, for example 123.45).
- **The issuer of the cash** (this is determined by whose balance sheet the liability resides on. It could be a central bank or a commercial bank).

Let's take an example: Anne was issued USD 100 by Retail Bank and wants to transfer USD 80 to Beth.

A simple view of the ledger follows:

Ledger Before	Currency	Amount	Owner	Issuer	ID
	USD	100	Anne	Retail Bank	499602D2

Transaction

The transaction itself is a digitally signed message from Anne, assigning ownership of USD 80 of the USD 100 to Beth. The message contains the ID (499602D2), the currency (USD), the amount (80), the new owner (Beth) and Anne's digital signature. Note that the issuer doesn't need to be explicitly named

— it can be anonymized or obfuscated in the message details.

This transaction message is broadcast in clear text to those who need to know and approve that this has happened — this is likely to be Anne's bank, Beth's bank, and perhaps Retail Bank as the issuer of the cash.

Ledger After	Currency	Amount	Owner	Issuer	ID
	USD	100	Anne	Retail Bank	499602D2-SPENT-
	USD	20	Anne	Retail Bank	496318FF (from 499602D2)
	USD	80	Beth	Retail Bank	24CB016EA (from 499602D2)

The relevant ledgers are updated to reflect the evolved owner of the USD 100.

Note that in the case of a broadcast blockchain, all participants who are running the blockchain database would need the transaction message, whether they are party to the transaction or not, whereas in the case of a private distributed ledger, only relevant ledgers need to be updated on a need-to-know basis.

A zero coupon bond

A bond builds on the cash model. For a zero coupon bond with limited lifecycle events, key data elements are: bond issuer, owner, face value, currency issuer, maturity date. Of these, when a bond changes hands or matures, the message would contain the new

owner and face value. The bond issuer and currency issuer can be obfuscated.

An interest rate swap

An interest rate swap differs from a bond in that future payment obligations are initially unknown, and only crystallize on specified dates. In the simplest example of a single currency fixed-to-floating rate swap, parties make a commitment to pay each other based on prevailing rates on specified future dates.

Here, key data elements are: an ID for tracking the interest rate swap, the owner, interest rate swap terms, payment schedule, and

details of the fixed and floating legs. These are all propagated as messages to the appropriate parties during lifecycle events including payments and termination, resulting in data being stored in their respective databases.

Generalized obligations

Digital financial assets can be reduced to contracts between parties. A generalized obligation would have elements of cash, bond, and new future obligations based on events in the “real world.”

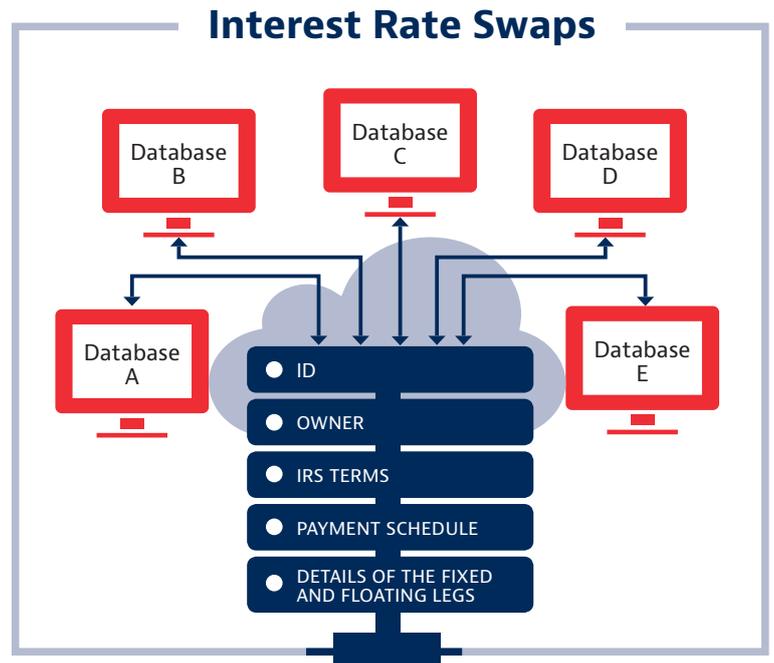
Some of the future obligations can be quantified at the outset, such as the payment of the face value of a zero coupon bond on a particular maturity date. Other future obligations are understood but not yet calculable, such as a payment on an interest rate swap. Perhaps obligations crystallize when external events happen, such as the payout of a binary option (party A pays party B a million dollars if the price of oil breaks USD 200 before 31 December).

As the financial instruments get more complicated, additional data is passed between entities — but notice that this data is exactly the same data that would be passed between them during the normal course of business today without a distributed ledger.

So what's new?

The value of the distributed ledger is the shared control over the data and the calculations governing the data, so that each party knows that what they see in the database they control is the same as what their counterparts see in the databases that the counterparts control. In that respect, it is business as usual, and the same regulations apply to the data based on what the data is, and whether it's at rest or in motion.

With broadcast blockchains, all data including commercially sensitive data (eg, prices) and



data the dissemination of which is restricted by regulation (eg, personally identifying) is passed to all participants in whichever jurisdiction their servers are held. This has legal implications: How can a system that broadly distributes personal information comply with laws prohibiting dissemination of personal information? Who is liable if your server suddenly has data on it that is prohibited by regulation from being there, sent by someone else?

Private distributed ledgers run by known participants will be subject to contractual agreements such as service level agreements and limitations of liability, so the existing legal framework can be referred to when there are issues.

What's new? Shared control over bilateral facts and their evolution.

GLOBAL DATA PROTECTION LAW

When thinking about the application of data protection laws to distributed ledger technologies, the first point to understand is that there is no such thing as global data protection law. Although overarching principles such as Article 12 of the Universal Declaration of Human Rights and the OECD Privacy Principles developed in the 1980s provide a common source for many data protection regimes, there is significant variation around the world.

Mapping such varied and sometimes even conflicting regimes onto global distributed ledger implementations poses obvious difficulties, particularly where logical relationships between nodes bear no necessary connection to the physical jurisdictions in which they are located. However, this is not a new issue for global networks — the question of which law or laws apply to distributed digital activity has been a central concern for the application of laws online for the last 20 years, if not longer.

What this does mean, however, is that compliance with data protection laws in the context of distributed ledgers is a matter of some significant complexity, and requires consideration of each of the laws where legal entities, headquarters, nodes, and, ultimately, consumers are located. The days of arguing that communications or interactions that cross borders can somehow escape regulation are gone.

Key data protection concerns

Despite this complexity, there are some key themes that are likely to arise in most if not all jurisdictions when it comes to compliance with privacy and data protection requirements in the context of blockchain and distributed ledger implementations.

1 Is the data regulated by privacy laws at all?

A threshold question is whether the particular data sets are regulated at all — for example, whether the data is considered “personal data” in Europe or “personally identifiable information” in the US. Data can, for example, be confidential without being personal to an individual — sensitive corporate data might well fall into that category.

In most jurisdictions, if data does not relate to a particular individual in some way, then privacy and data protection regimes will not apply.

Of course, other important legal rules might apply to impose restrictions on the way data might be able to be used and shared. This would include, for example, the confidentiality and secrecy obligations a bank has to its corporate and private wealth customers in respect of certain data sets.

2 Can data sharing occur anonymously?

The treatment of anonymous or pseudonymous data is an even more difficult question under many data protection regimes. In many cases, data that relates to an individual who is not identified will not be within the scope of data protection laws.

However, many jurisdictions contemplate that anonymous or pseudonymous data that can be subjected to re-identification processes, or can be combined with other data sets to identify the individual in question, must be treated as personal data.

3 Are all participants equally responsible for compliance?

Some jurisdictions, particularly in the EU, make a clear distinction between data "controllers" (generally, the primary collectors of personal data from end users) and data "processors" (generally, secondary holders of personal data who act on behalf of data controllers, including, for example,

outsourced service providers). However, many other countries do not make such a distinction in their data protection laws, but rather treat each collector of personal data as a primary actor, requiring full compliance in each case.

The implications of these distinctions will vary depending on the nature of the DLT implementation and the level of autonomy of each participant. However, one feature of most public blockchains is that each node deals with the data it receives as a fully autonomous operator rather than on a shared basis with any other node, meaning that each participant is likely to be required to comply as an independent controller of the personal data it receives.

4 How are end users made aware of their rights?

One important effect of the controller/processor distinction relates to how collectors of personal data need to interface with the end users (in EU data protection law, the "data subjects").



Most data protection regimes focus on the relationship between collector and data subject as a key point in the compliance cycle. Typically, such compliance involves the provision of various notifications to the data subject (in documents such as privacy policies, collection notices or other disclosures) and the collection of certain consents from the data subject. The key to compliance here is that the collector of the personal data clearly sets out for the data subject how the collector proposes to treat data subject's personal data, including what personal data will be collected, how it will be used, to whom it will be transferred and how it will be secured.

A clear challenge in DLT implementations is how these compliance requirements can be achieved by each participant, given that although each (or at least many) of them may end up holding personal data, in many instances only one of them will have the opportunity to directly interface with the data subject. This is likely to be a far more thorny issue in a public blockchain implementation, where there is no necessary relationship between each of the nodes, as it is in a private implementation,

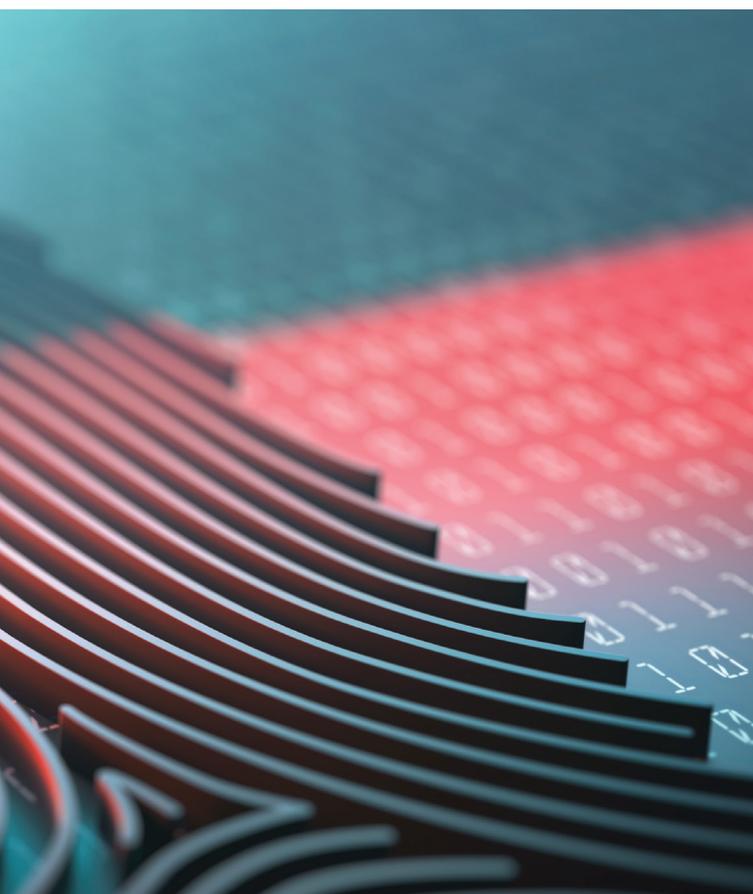
where contractual arrangements between participants can facilitate data protection compliance across the board. In a point-to-point DLT implementation where there is no global data broadcast, this issue is an entirely familiar one: the data being shared between nodes in such a context is effectively the same data that is shared in traditional confirmations between banks today.

5 How are cross-border transfers of data to be treated?

In addition to the difficulties caused by the multiplicity of privacy regimes that may apply in a DLT context, many data protection regimes also regulate the circumstances in which personal data collected from data subjects can be transferred outside the jurisdiction. Typically, data protection regimes will seek to restrict the transfer of personal data to countries where the strength of data protection that will apply in that country is not "adequate" (ie, not up to the standards imposed in-country).

This has been the context for a very high-profile battle between the EU and the US on privacy matters. Essentially, the EU views the underlying US privacy laws as not meeting EU adequacy requirements, and has expressed concerns relating to the transfer of personal data from EU data subjects to the US. Various attempts have been made to deal with this issue to facilitate data flows from the EU to the US (originally, the "safe harbor" for qualifying US entities, and now the new "privacy shield").

However, this issue is not limited to the EU. It will be important for any DLT implementation to consider the transnational data flows that will be generated, and to establish processes to enable compliance with all relevant cross-border transfer requirements. Again, this is likely to be more problematic in a public blockchain implementation than in a private DLT, given the ability in the latter to establish clear contractual obligations and rules between each of the participants.



BLOCKCHAINS VERSUS DISTRIBUTED LEDGERS

The table below sets out some key distinctions between public blockchains and private distributed ledger implementations in terms of the likely application of data protection laws.

ISSUE	PUBLIC BLOCKCHAIN	DISTRIBUTED LEDGER
Data privacy	All data including commercially sensitive data (eg, prices) and data subject to regulation (eg, personally identifying) is passed to all participants. As such, every participant has to comply with data protection laws in the jurisdiction they are in, including in respect of subsequent cross-border transfers of that data.	Some private distributed ledgers pass data only to those who are party to a deal. Private distributed ledgers on which all participants are known will have in place contractual agreements such as service level agreements between the ledger operator and the participants, which would establish liability, including limitations of liability, so the existing legal framework can be referred to.
Responsibility for compliance	Each node deals with the data it receives as a fully autonomous operator, meaning that each participant is likely to be required to comply as an independent controller of the personal data it receives.	Each node receives only the data that is relevant to it. Some jurisdictions, particularly in the EU, make a clear distinction between data "controllers" and data "processors," and apply different compliance standards. Many other jurisdictions, however, do not make this distinction.

ISSUE	PUBLIC BLOCKCHAIN	DISTRIBUTED LEDGER
Rights of end users	<p>There is no necessary relationship between each node. Therefore, there are no contractual arrangements between participants that can facilitate data protection compliance across the board.</p>	<p>The data being shared between nodes is effectively the same data that is shared in traditional confirmations between banks today. Thus, there are contractual agreements in place between the participants that can ensure data protection compliance.</p>
Cross-border transfer of data	<p>Since data is broadcast to every node on the network and there is no permissioning to control who is on the network, it is not possible to control the flow of sensitive data cross-border. Public blockchains will not be able to meet the relevant cross-border transfer requirements.</p>	<p>Clear contractual obligations and rules can be established between identified participants to limit the flow of sensitive data. Processes can be established to meet the relevant cross-border transfer requirements.</p>

DATA PROTECTION LAWS IN VARIOUS JURISDICTIONS

While there is a level of alignment across data protection regimes in many major centers, this is still an area of law with important distinctions between jurisdictions.

Some key issues and differences include:

Europe and the UK: The right to be forgotten

The right to be forgotten, now embedded in EU law under Article 17 of the new General Data Protection Regulation, presents a particular challenge for open blockchain technologies. Article 17 confers a “right of erasure” of personal data, subject to certain conditions and limitations.

Where a data controller (eg, a node in a public blockchain) has made personal data public, exercise of the right will also place an obligation upon a node to take reasonable steps, including technical measures, to inform other controllers of the erasure request. In complying with this obligation, controllers must take into account the available technology and the cost of implementation.

However, because permissioned DLT systems involve known and trusted parties, historical entries can be amended provided the required number of parties agrees to an erasure. For example, a similar process has been carried out by participants of the Ethereum network to reinstate the funds lost in the infamous “DAO hack.” Accordingly, DLT systems may be designed to allow personal data to be deleted if a sufficient majority of parties to the system (or an authority appointed by the parties for the purpose) agree.

Singapore: An evolving law

Rather than containing any specific areas of particular difficulty, a key feature of privacy law in Singapore is its nascence. The Personal Data Protection Act was only implemented in 2013, meaning that Singapore does not yet have as much history or precedent of data protection law as do some other jurisdictions such as those in Europe.

In the context of new and evolving technologies such as blockchain and DLT implementations, this means that difficult questions, such as the treatment of anonymous and pseudonymous data, and



questions around the de-identification and re-identification of data, may be uncertain. Of course, these types of concerns are not limited to Singapore, with much of the law of data protection in the rest of the Asia Pacific region also having undergone rapid development in the last 5 to 10 years.

Australia: Responsibility for offshored data

A key feature of Australian privacy law since a major round of legislative updates in 2014 is the increased focus on cross-border transfer of personal information.

The current law, under the Australian Privacy Act, provides a path for the offshoring of data, but requires the transferring entity to ensure that the recipient of the data holds it in accordance with the principles of Australian privacy law. This is commonly achieved through contracts that require recipients to maintain such standards, but this is unlikely to be possible in a public blockchain context. An important consequence under Australian law is that the entity transferring the data out of Australia remains responsible for any breaches by or on behalf of the recipient entity or

entities, meaning significant potential liability for any Australian node in a public blockchain under current rules.

US: Fragmentation and multiple sources of rules

Perhaps the defining feature of US privacy and data protection law is its fragmentation. There is, in effect, no overarching law regulating data protection; instead, collectors must contend with a range of state and federal laws, many of which cover specific data sets in particular industry sectors. In addition to healthcare, the financial services industry is one of the most highly regulated in the US, meaning that public blockchains with US nodes will need to consider and meet the requirements of a broad spectrum of regulation.

A key example of multiplicity of laws in the US is the state-by-state regulation of data breach notification: each state has its own rules governing the circumstances in which entities must notify regulators and individuals of actual or potential data breaches, and the processes for such notifications.

CONCLUSION

Regulated financial institutions who see the benefits of DLT continue to drive towards commercialization at pace. R3's Corda is tailored for use by financial institutions and, as such, has many design aspects that are different from public blockchains, one of which is the limited data sharing that allows flexibility in meeting multiple jurisdictional data privacy requirements.

As technology evolves, the law evolves. Every new piece of technology added to an institution's IT program needs to be fully understood, not just in the context of existing regulations, but for compatibility with future regulations.

Privacy and data protection laws, in their various iterations around the world, represent a real and current compliance challenge for public and private distributed ledger technology implementations. In general, such compliance cannot be "backfilled" into an ecosystem: "privacy by design," which is a mantra for privacy regulators around the world, should truly be a key consideration of any new implementation.

AUTHORS

Baker McKenzie

Adrian Lawrence

Partner, Sydney
adrian.lawrence@bakermckenzie.com

Harry Small

Partner, London
harry.small@bakermckenzie.com

Ken Chia

Partner, Singapore
ken.chia@bakermckenzie.com

Michael Schmidl

Partner, Munich
michael.schmidl@bakermckenzie.com

Brian Hengesbaugh

Partner, Chicago
brian.hengesbaugh@bakermckenzie.com

R3

Antony Lewis

Director of Research
Singapore
antony.lewis@r3.com

Isabelle Corbett

Director of Regulatory Affairs & Senior Counsel
New York & Washington DC
isabelle.corbett@r3.com

J. Ross Nicoll

Senior Developer
London
ross.nicoll@r3.com

Martin Sim

Research Associate
Singapore
martin.sim@r3.com



Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

About R3

R3 is an enterprise software company revolutionizing business ecosystems with a new peer-to-peer platform, Corda. Corda is a distributed ledger platform that is the outcome of over two years of intense research and development by R3 and 80 of the world's largest financial institutions. Corda is applicable to any commercial scenario, while meeting the highest standards of the banking industry.

www.r3.com
www.corda.net

www.bakermckenzie.com

©2017 Baker & McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.