Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies

PRITESH SHAH AND DANIEL FORESTER, DAVIS POLK & WARDWELL LLP, AND MATTHIAS BERBERICH AND CAROLIN RASPÉ, HENGELER MUELLER, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

A Practice Note discussing blockchain technology, recent trends in data privacy law, and the tensions between them. It explains blockchain technology's characteristics and describes issues and potential strategies for complying with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the California Consumer Privacy Act of 2018 (CCPA), including anonymity and pseudonymity, data controller and data processor identification, territorial and cross-border data transfer issues, legitimate bases for processing personal data, and individuals' rights.

Blockchain is one of the most hyped developments to arrive on the technology scene in recent years. However, blockchain technology and data privacy laws and regulations have largely developed independently. Heightened global data protection regimes with dramatically increased potential fines drive businesses to further reevaluate their privacy practices. Significant ambiguity and complexity currently exist for organizations in applying data privacy requirements to blockchain technology and associated services.

This Note:

- Explains blockchain technology, including core elements and design choices.
- Considers key tensions and issues between using blockchain technology and data privacy laws and regulations.
- Offers potential steps for mitigating compliance risks.

BLOCKCHAIN TECHNOLOGY CHARACTERISTICS

Blockchain gained notoriety and quickly became part of popular parlance during 2017's unprecedented cryptocurrency boom.

The technology builds on longstanding concepts and techniques in distributed transaction processing and encryption. Software developers initially brought these ideas together in a remarkably innovative manner to support Bitcoin's 2009 launch, giving rise to the first "blockchain" network. Cryptocurrencies, many of which use the concepts Bitcoin introduced, continue to proliferate.

Astute observers quickly recognized the underlying technology's potential beyond its original use to record trustless, peer-to-peer transfers of value. Blockchain applications have grown, with current use cases in:

- Smart contract development.
- Supply chain management, asset registers, and recordkeeping tools.
- Other innovations in varied industries, including:
  - fintech;
  - real estate;
  - health care; and
  - retail.

Blockchain implementations share several core elements, regardless of use case or application, including:

- Distributed ledger technology. This software infrastructure provides a synchronized and shared data structure that multiple participants can access and modify over a peer-to-peer network. The ledger chronologically links each new published data block to previous blocks of transactions using a cryptographic hashing process to form a chain. Participants or nodes generally store a complete copy of the ledger with previous transactions.
- **Consensus mechanisms.** These algorithms typically require a defined majority of participants to verify the legitimacy of and agree on each new ledger transaction request, taking the place of a traditional centralized administrator. Some consensus models include:
  - proof-of-work, which, mostly in public blockchains, induces participants to compete for the right to verify and settle blocks of transactions by solving computationally intensive puzzles;
  - proof-of-stake, which sets block publishing rights according to participants' known investment in the blockchain; and

  - proof-of-authority, which verifies a participant's identity and authorization level before granting block publishing rights, typically in private blockchains of known participants.
- **Selection of public versus private participation.** Public or permissionless blockchains, like those supporting most cryptocurrencies, allow anyone in any location to participate, subject to the implementation's consensus mechanisms. Private or permissioned blockchains restrict who may access and participate in the network and particular transactions either automatically or through identified gatekeepers. Many business or enterprise applications require access controls or other limitations, such as restricting data content or storage locations, that private blockchains can offer. These applications, often with more centralized networks and smaller participant groups, benefit from blockchain characteristics but also share many features and risks with traditional centrally administered databases.
- **Transaction immutability.** Widely touted as a blockchain benefit, transaction immutability follows from the way the distributed ledger technology cryptographically links each new block to the previous entry. Participants must however consider immutability strength through the lens of the particular blockchain's characteristics, including security levels and other potential risks. For example, a "51% attack" occurs when bad actors compromise a majority of participants, overwhelm the consensus mechanism, and alter the blockchain contents for their benefit. The guarantee of immutability is stronger in large robust networks where the resources required to gain majority control make these attacks cost-prohibitive.

For more on blockchain technology characteristics, including other cybersecurity risks and issues, see Practice Note, Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview (w-017-1916).

RECENT TRENDS IN DATA PRIVACY LAW

Paralleling blockchain technology's growth over the past decade, data privacy has seen a sharp uptick in global attention as a general policy and regulatory concern. Changes in the EU and US especially have the potential to affect blockchain technology users, although these jurisdictions have historically approached data privacy in different ways. Specifically:

- The EU takes an omnibus approach with its General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which entered into force on May 25, 2018. Its proposed EU E-Privacy Regulation further addresses electronic communications (see The EU's GDPR and Draft E-Privacy Regulation).
- The US conversely approaches data privacy in a patchwork, sector-specific fashion at the federal level. Some states have taken the lead by adopting broader legislation, for example, with the California Consumer Privacy Act of 2018 (CCPA) (see The CCPA and US Trends).

For a summary comparison of the GDPR and CCPA, see Practice Note, CCPA and GDPR Comparison Chart (w-016-7418).

These and other current regimes perpetuate a traditional data protection framework that challenges decentralized technologies like blockchain because they envision:

- Data controllers or businesses that determine the purposes for and means of processing, for instance, by collecting, using, and managing personal data at their discretion.
- Data processors or service providers that work on data controllers' behalf.

This longstanding notion of centralized entities that control both the data they collect and their service provider relationships contrasts with blockchain technology's distributed peer-to-peer network architecture.

THE EU'S GDPR AND DRAFT EU E-PRIVACY REGULATION

The GDPR sets out a high, harmonized personal data protection standard for the EU and the European Economic Area (EEA), although it allows member states to make some derogations.

The GDPR:

- Defines personal data broadly to include any information relating to an identified or identifiable individual (Article 4(1), GDPR).
- Takes an expansive extraterritorial view, protecting EU residents from less stringent data protection standards in other countries by applying to:
  - processing personal data of individuals in the EU when offering goods or services to those individuals in the EU; and
  - online behavioral monitoring of individuals in the EU.

Controllers and their optional processors must take various steps to document their programs and comply with the GDPR's principles and many obligations. Blockchain technology users may find several compliance requirements challenging, including:

- Ensuring the legality of personal data processing, for example, by:
  - obtaining individual data subjects' consent; or
  - meeting requirements for other legal bases like fulfillment of a contract or balancing of legitimate interests.

  (Article 6, GDPR.)
- Informing data subjects about and fulfilling various individuals' rights, such as:
  - notice;
  - data access, rectification, and portability;
  - opportunities to object to processing, including automated decision making; and
  - data removal, also known as "the right to be forgotten," under specified circumstances.

  (Articles 12 through 23, GDPR.)
- Maintaining risk-based data security standards (Article 32, GDPR).

The GDPR sets out high potential fines for noncompliance of up to the greater of EUR20 million or 4% of annual worldwide turnover (Article 83, GDPR). For more on the GDPR and its applicability, see Practice Notes, Overview of EU General Data Protection Regulation (w-007-9580) and Determining the Applicability of the GDPR (w-003-8899).

The current E-Privacy Directive (Directive 2002/58/EC), as amended by the EU Citizens' Rights Directive (Directive 2009/136/EC), further governs data protection for electronic communications. EU policymakers intend for the draft E-Privacy Regulation to

complement the GDPR. A final draft is expected in late 2019 at the earliest, making entry into force unlikely before 2020. Transitional periods may postpone its applicability.

The current draft E-Privacy Regulation indicates that it is likely to apply to:

- The processing of electronic communications data relating to the provision and use of electronic communications services.
- Information related to end users' terminal equipment.

The draft E-Privacy Regulation regulates data with a different scope than the GDPR, including only certain communications data like content and metadata regardless of whether it is personal data or not. Like the GDPR, data processing requires a legal basis by consent or law, such as processing that is technically necessary for providing communications services. Potential issues for blockchain technology users remain open. For example, as they are finalized, the draft E-Privacy Regulation provisions may further challenge online services using blockchain technology.

US TRENDS AND THE CCPA

The US has not yet implemented a comprehensive federal data protection framework, relying instead on sector-specific privacy and data security laws and regulations, such as:

- The Gramm-Leach-Bliley Act (GLBA) for financial institutions.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) for health care providers, health plans, and their service providers.

For more on current US privacy and data security laws, see Practice Note, US Privacy and Data Security Law: Overview (6-501-4555).

Many observers expect Congress to eventually enact a more comprehensive privacy and data security law that may at least partially preempt state laws. In the meantime, states have taken the lead. For example, California enacted the most comprehensive and stringent state-level data protection law in the US to date with the CCPA. The new protections for California residents begin January 1, 2020. Similar legislation is under consideration in several other states (see Practice Note, 2019-2020 Federal and State Privacy-Related Legislation Tracker (w-020-3899)).

The CCPA:

- Defines personal information broadly to include any information that directly or indirectly identifies, describes, or can reasonably link to a particular California resident consumer or household (Cal Civ. Code § 1798.140(o)).
- With some exceptions, applies to businesses that collect and control consumers' personal information and meet at least one of the following thresholds:
  - annual gross revenue that exceeds $25 million (adjusted for inflation);
  - annually buys, receives, shares, or sells alone or in combination the personal information of more than 50,000 consumers, households, or devices for commercial purposes; or
  - derives 50% or more of annual revenues from selling consumers' personal information.

(Cal. Civ. Code § 1798.140(c)(1).)

Like the GDPR, the CCPA provides consumer protections and compliance obligations that may be challenging for blockchain technology users, including:

- Informing consumers about and fulfilling various individuals' rights, such as:
  - notice, access, and disclosure, including details regarding third-party disclosures or sales (Cal. Civ. Code §§ 1798.100, 1798.110, 1798.115, and 1798.130);
  - an opportunity to opt-out of sales of personal information without discrimination, or opt-in for minors (Cal. Civ. Code § 1798.120); and
  - the right to be forgotten, subject to certain limits (Cal. Civ. Code § 1798.105).
- Maintaining risk-based data security standards, enforced by a CCPA-granted private right of action regarding data breaches that result from a business's failure to maintain adequate data security standards (Cal. Civ. Code §§ 1798.81.5 and 1798.150).

The CCPA grants rulemaking and enforcement authority to the California Attorney General (CAG) with administrative penalties of up to $2,500 per violation and $7,500 per intentional violation that likely extend to each affected individual (Cal. Civ. Code § 1798.155(b)). It is not yet clear how the CAG intends to implement these fines.

For details on the CCPA and current amendment status, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) (w-017-4166) and CCPA Proposed Amendments and Other California Privacy-Related Legislation Tracker (w-020-3287).

TENSIONS BETWEEN BLOCKCHAIN TECHNOLOGY AND COMMON DATA PRIVACY REQUIREMENTS

Legislators do not appear to have focused on blockchain technology and its unique features when drafting recent data privacy laws and frameworks. Some blockchain technology features can help mitigate or cater to privacy concerns, such as using encryption and verifying data integrity. However, blockchain technology's distributed peer-to-peer network architecture often places it at odds with the GDPR's and CCPA's traditional notion of centralized controller-based data processing. This disconnect can make it difficult to reconcile current data protection laws with blockchain's other core elements, such as the lack of centralized control, immutability, and perpetual data storage. Regulatory guidance on reconciling this and other potential conflicts is currently limited.

Handling data privacy issues and properly applying laws, such as the GDPR and CCPA, increasingly contribute to a business venture's success or failure, including those that use blockchain technology. Circumstances may require or organizations may benefit from conducting a privacy impact assessment (PIA) or data protection impact assessment (DPIA) before implementation or release.

Some important tensions between blockchain technology and data privacy requirements to consider include:

- Different perspectives on anonymity and pseudonymity and how they affect the applicability of various data protection and privacy laws (see Anonymity, Pseudonymity, and Privacy Law Applicability).
- How to identify data controllers and data processors in various blockchain technology implementations (see Data Controller and Data Processor Identification).

- Territorial implications for distributed blockchain networks (see Territorial Considerations).
- When cross-border data transfers occur and potential restrictions on them (see Cross-Border Data Transfers).
- Applying criteria for legitimate reasons for processing personal data to blockchain use cases (see Legitimate Reasons for Processing Personal Data).
- Reconciling transaction immutability and data preservation in blockchain applications with individuals' rights (see Immutability and Individuals' Rights).

For more on PIAs, DPIAs, the commonality between them and a template, see Practice Note, Conducting Privacy Impact Assessments (w-012-5912) and Standard Document, Privacy Impact Assessment (w-012-5914).

ANONYMITY, PSEUDONYMITY, AND PRIVACY LAW APPLICABILITY

The applicability of most data privacy laws, including the GDPR and the CCPA, depends first on whether the activities in question involve the processing of personal data. Blockchain implementations that expressly record personal data on the blockchain are clearly subject to laws regarding personal data. However, whether the data some blockchains record, process, or use to manage transactions qualifies as personal data varies. For example:

- Blockchains may expressly include personal data as "payload" if they aim to create a record of ownership or other assigned rights that require sufficient identifying information.
- Blockchains, including many public blockchains that support popular cryptocurrencies, tout anonymity or at least some level of privacy by using public-private key pair encryption. These asymmetric encryption systems:
  - leverage the mathematical relationship between the public and private keys in a particular pair;
  - record public keys on the blockchain implementation;
  - do not typically record public key owner data or other similar personal information; and
  - leave users to retain and protect their own private keys.

Some blockchain enthusiasts claim that using public-private key encryption preserves anonymity and privacy. This is a relatively simplistic view of personal information that may not hold up under GDPR or CCPA definitions because:

- Methods exist for linking individuals to public keys by analyzing blockchain transactions and other publicly available data. Some businesses offer services to identify individuals using their public keys, blockchain transactions, and other available data.
- The GDPR defines personal data broadly (see The EU's GDPR and Draft E-Privacy Regulation). The threshold for identification is low, recognizing any means "reasonably likely to be used," considering all objective factors, such as costs and time, and available and anticipated technology (Recital 26, GDPR). The GDPR also includes online identifiers, which the European Court of Justice (ECJ) previously addressed in its *Breyer v. Germany* decision (Case 582/14), holding that dynamic IP addresses are personal data (see Practice Note, Overview of EU General Data Protection Regulation: Online identifiers (w-007-9580)).
- The CCPA takes a similarly broad view of personal information that includes:
  - "online identifiers," without specific definition; and
  - unique identifiers that encompass "persistent or probabilistic identifiers that can be used to identify a particular consumer or device" (Cal. Civ. Code § 1798.140(x)).

See Practice Note, Understanding the California Consumer Privacy Act (CCPA) : Personal Information Under the CCPA (w-017-4166).

Better practice treats public keys as tokenizations of personal information from a privacy perspective instead of anonymized data, because:

- They correspond to an individual.
- Reidentification becomes possible in some circumstances.

Blockchain technologists also sometimes claim that their implementations are anonymous because they record transaction data that:

- Only references a public blockchain address and not the underlying owner's name or other directly identifiable personal information.
- Often do not display unencrypted public blockchain addresses.

This usage again contrasts with data privacy laws that only consider personal information anonymized or deidentified if it cannot be reasonably linked to an identifiable individual. Applying pseudonymization techniques lowers risk but does not remove regulatory obligations. For more on these techniques under the GDPR, see Practice Note, Anonymization and Pseudonymization Under the GDPR (w-007-4624).

Reidentification risks and related concerns have led some blockchains, including privacy-focused cryptocurrencies, to try to reduce the risk of identifying individual participants by:

- Implementing various mitigation strategies to protect transaction and other data.
- Introducing alternative cryptographic approaches.

Organizations should consider the applicability of the GDPR, the CCPA, and other data privacy laws to proposed blockchain use cases by:

- Carefully assessing specific blockchain implementation details.
- Reviewing potential reidentification methods and risks.
- Monitoring emerging guidance.

DATA CONTROLLER AND DATA PROCESSOR IDENTIFICATION

Blockchain implementations that process personal information are at odds with the clear distinction that data privacy laws and frameworks, like the GDPR and CCPA, make between:

- Controllers and their processors.
- Individual data subjects.

The distributed peer-to-peer network architecture means that it is often unclear which party determines the purposes and means of processing.

Private blockchains present a simpler case. Here a central operator or consortium likely qualifies as a controller or joint controllers if they:

- Have control over the blockchain system, like a traditional system architecture.
- Determine the purposes and means for any personal data processing.

Other actors that help operate the blockchain specifically for the central operator, such as nodes or miners, can take the processor role. The private blockchain operator or consortium must implement appropriate data processing agreements or other contracts to hold these service providers accountable and meet regulatory obligations. Alternatively, private blockchains where the central operator performs all technical support activities may not have data processors or service providers by default.

Public blockchains typically lack a central operator, making it difficult to assign traditional controller and processor accountability. For example:

- Each public blockchain node independently processes the same transaction data set, at least during the block verification process. This might lead to classification of each blockchain node as a joint controller under the GDPR, but authorities and commentators alike are reluctant to draw this conclusion for all nodes (Articles 4(7) and 26, GDPR; see CNIL Guidance).
- Conversely, if no entity has clear control over the data, then participants may try to argue that there is no controller and hence there can be no processors. However, this argument may not be compatible with the GDPR, because the GDPR emphasizes a "clear allocation of responsibilities" for personal data processing (Recital 79, GDPR).

Data protection authorities and other regulators have been slow to address blockchain technology, except for the French data protection authority (*Commission Nationale de l'informatique et des Libertés* (CNIL)) (see CNIL Guidance).

Businesses that use blockchain technology when collecting or managing personal data should carefully analyze their accountability under applicable regulations, including the roles any service providers they engage play.

CNIL Guidance

The CNIL has issued initial cautious guidance on applying the GDPR to some blockchain technology use cases. The CNIL guidance focuses on various blockchain actors, distinguishing among:

- Participants that have full writing rights to enter transactions on the blockchain and to send the data for validation to miners.
- Accessors that may retain full copies of a blockchain but have read-only rights.
- Miners that validate transactions and create new blocks according to the implementation's governance model.

Participants under these distinctions are controllers regarding personal data they enter on a blockchain, because in doing so, they determine the purposes and means for processing. Mere accessors and miners normally do not make these determinations and so are not controllers. The CNIL guidance also notes that individuals entering personal data on a blockchain for strictly personal purposes are not controllers under the GDPR's household exception (Article 2, GDPR).

However, when third parties act on a participant's behalf, they may become processors and then should enter into data processing agreements.

Regarding miners, the CNIL guidance notes that:

- Miners that are only validating transactions and are not involved in the object of those transactions, for instance, miners just building new blocks according to the technical protocol, are not controllers in the CNIL's view.
- In some cases, miners may be data processors in the CNIL's view, if they follow a data controller's instructions, for example, in a private blockchain of insurance companies that mine transactions on behalf of customers.

Although this may suggest that in certain circumstances miners may be neither a data controller nor a data processor, the CNIL guidance is not clear.

TERRITORIAL CONSIDERATIONS

Data privacy laws often apply according to either or both:

- The individual's location.
- The personal data processing location.

For example:

- The CCPA is indifferent to a business's processing location if it involves the personal information of California residents.
- The GDPR applies:
  - to personal data processing activities by either controllers or processors established in the EU or the broader EEA; and
  - regardless of location, if the personal data processing involves offering individuals goods or services in the EU or online behavioral monitoring of individuals in the EU.

(See The EU's GDPR and Draft E-Privacy Regulation.)

Evaluating jurisdictionality and applying regulations to decentralized blockchain implementations is not a straightforward exercise compared to traditional centralized systems.

More cautious blockchain projects that handle personal data may try to limit participants by jurisdiction, although reliably confirming online locations can be difficult. Private blockchains more often set restrictions in their governance models and agreements to limit regulatory scope. Public blockchains that process personal data may assume applicability for various regulatory regimes as a best practice, but:

- Managing the diverse set of regulations can incur significant overhead costs.
- Using common public-private key pairing for encryption may bring them in many regimes' scope (see Anonymity, Pseudonymity, and Privacy Law Applicability).

CROSS-BORDER DATA TRANSFERS

The distributed nature of blockchain technology not only poses a challenge regarding the applicability of various jurisdictions' laws, but it also raises tensions with those that restrict cross-border data transfers. Most notably, the GDPR:

- Permits personal data transfers to countries outside the EEA only under specific circumstances.

- Requires specific safeguards in the recipient jurisdiction to ensure the same or an adequate level of protection.

Controllers must implement additional safeguards unless the European Commission issues an adequacy decision for the recipient location. Safeguards may take the form of standard contractual clauses, binding corporate rules, codes of conduct, or certification mechanisms. For more on cross-border data transfers under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Cross-border data transfers (w-007-9580).

These safeguards:

- Normally require some centralized compliance program to implement them.
- Are especially difficult to consider implementing in public blockchains with their undefined participant groups.

Other jurisdictions are increasingly seeking to limit cross-border data transfers and may call for similar protective mechanisms.

LEGITIMATE REASONS FOR PROCESSING PERSONAL DATA

Some data protection and data privacy laws limit the permitted uses of or require legitimate reasons for processing personal data. For example:

- Federal sector-specific laws in the US, like the GLBA and HIPAA, and various state laws limit certain personal data use without individuals' consent. Various exceptions may apply, such as HIPAA's permitted uses for treatment, payment, and health care operations (45 C.F.R. § 164.506).
- The GDPR only allows controllers to process personal data based on one or more lawful purposes, including data subjects' consent or processing to the extent necessary for:
  - entering or performing a contract with the data subject;
  - complying with the controller's legal obligations;
  - protecting vital interests of the data subject or another natural person;
  - performing public interest or official tasks; or
  - pursuing the controller's or a third party's legitimate interests unless the data subject's interests or fundamental rights and freedoms override them;

  (Article 6, GDPR.) For more on the GDPR's legal processing grounds, see Practice Note, Overview of EU General Data Protection Regulation: Lawfulness of processing (w-007-9580).

It is unclear whether these options encompass perpetual distributed blockchain storage. Blockchain participants may request consent from their users or data subjects, as applicable. However:

- In some instances, it may be preferable for controllers under the GDPR to depend on a basis other than consent because it must be:
  - freely given;
  - specific;
  - informed; and
  - unambiguous.

  (Article 4(11), GDPR.)
- Even if consent mechanisms meet GDPR or other relevant standards:
  - individuals can withdraw consent at any time without reason; and
  - blockchains may store personal data in a way that is extremely difficult to remove making later processing unlawful.

Organizations must carefully consider scenarios like consent withdrawal when determining what data they store in blockchain applications and how they record it.

IMMUTABILITY AND INDIVIDUALS' RIGHTS

Data privacy laws increasingly grant individuals with rights, aiming to:

- Help individuals regain a measure of control over their personal data.
- Allow individuals to choose to protect their personal data from monetization or exploitation without their consent or other justification.

For more on data subject rights under the GDPR and CCPA, see Recent Trends in Data Privacy Law.

Rights of data correction and data erasure, also known as the right to be forgotten, present the most apparent conflict with blockchain technology's transaction immutability characteristics. Blockchains, in particular implementations that provide ownership, supply chain, and other recordkeeping tools, including smart contracts, can likely address data updates by recording additional transactions. However, these later transactions do not technically delete data previously stored on the blockchain. The same approach supports updating various process steps and status values.

Whether blockchain technology fundamentally conflicts with the right to be forgotten depends on how strictly authorities interpret "erasure." A strict technical erasure of blockchain data, in a current standard blockchain architecture, requires both:

- A backward deconstruction of the blockchain up to and including the targeted record.
- A reconstruction of the blockchain from the point of the deleted data forward.

This kind of operation:

- Conflicts with basic blockchain design principles.
- Consumes significant processing resources from participants.
- Requires consent from the necessary threshold of participants or according to other rules in the blockchain's governance model (see Blockchain Technology Characteristics).
- Would therefore be feasible only as an extreme exception in operation, comparable in its efforts to a "hard fork" in public blockchain communities, where a group decides to split the code of a particular blockchain and run a modified, parallel implementation.

These strict technical data deletion measures:

- Are very difficult to implement every time individuals seek to exercise their rights.
- May be more feasible in private blockchain governance models with a central operator.

POTENTIAL MITIGATING STEPS

Some have called for legislative updates or at least guidance from relevant authorities to reconcile data privacy laws with emerging decentralized technologies like blockchain. For now, organizations should follow several risk management strategies when considering blockchain technology by:

- Carefully evaluating whether using blockchain technology is a good fit for current business and processing objectives, as even early commenting regulators like the CNIL have emphasized (see CNIL Guidance).
- Preferring private or permissioned blockchains to enforce stricter usage rules (see Use Permissioned Blockchains to Support Governance Models).
- Using data structure and design techniques to limit the personal data they actually store on blockchains (see Avoid or Limit Personal Data Stored on Blockchains).
- Adopting alternative data encryption and destruction techniques to protect personal data (see Use Alternative Data Encryption and Destruction Approaches).

USE PERMISSIONED BLOCKCHAINS TO SUPPORT GOVERNANCE MODELS

Public permissionless blockchains reflect the technology's original notions and benefits of permitting any individual to access, view, and submit transactions with minimal data governance. Organizations must balance these benefits with their needs to follow consistent data privacy practices and comply with applicable laws and regulations.

One commonly proposed way to foster consistent participant practices and regulatory compliance encourages organizations to:

- View the differences between public permissionless and private permissioned blockchain implementations as a spectrum rather than a binary decision.
- Implement a blockchain architecture that lies closer to the private permissioned end of the spectrum.

These increasingly adopted implementations can employ various governance structures and processes to:

- Authorize a select number of vetted and approved participants.
- Ensure that the authorized participants follow strict consensus practices for data privacy.
- Take technical measures to further reduce and regulate the amount of personal data that participants process.

Using blockchain technology for business applications with lower numbers of authorized participants has pros and cons. For example, a lower number of participants:

- Theoretically makes it easier for one participant to overwhelm the blockchain's consensus mechanism depending on its characteristics (see Blockchain Technology Characteristics).
- Conversely may heighten security because:
  - participants can contractually bind each other regarding their usage; and
  - misbehavior is not anonymous and is easy to link to identifiable participants.

More centralized control over the blockchain implementation may also permit more traditional contractual approaches to:

- Allocating data processing responsibility and accountability.
- Managing cross-border data transfers.
- Responding to individuals' and authorities' requests.
- Deploying data processing agreements between those playing controller and processor roles.

AVOID OR LIMIT PERSONAL DATA STORED ON BLOCKCHAINS

One way to address laws and regulations that hinge on personal data is to avoid putting any personal data on a blockchain. However, the broad definitions for personal data across various regimes make it challenging to fully avoid falling in their scope, especially in blockchains that use public-private key encryption to manage transactions among individuals (see Anonymity, Pseudonymity, and Privacy Law Applicability).

Use cases particularly suited to avoiding data capable of directly or indirectly identifying an individual include:

- Financial settlement systems that do not involve natural persons.
- Supply chain management.
- Managing distributed internet of things (IoT) non-personal sensor data.
- Other applications that do not handle information on natural persons.

For use cases that involve personal data, organizations should consider using more privacy-friendly blockchain techniques, such as those that:

- Combine on-chain and off-chain storage to:
  - avoid storing personal data as a payload on the blockchain; and
  - allow blockchain transactions to serve as mere pointers or other access control mechanisms to more readily managed storage solutions.

Future technologies may further strengthen privacy for blockchains that handle personal data by making individual user identification harder. For example:

- Some have suggested adding noise to blockchain data, mixing up transactions, or using groups of encryption keys to avoid reidentification.
- Others, including the emerging MimbleWimble protocol and the privacy-friendly cryptocurrency Grin, leverage encryption techniques that allow participants to:
  - prove that they know something without revealing the nature and identity of the information; and
  - use one-time addresses that do not require archiving.

These privacy-friendly techniques may run into additional regulatory concerns, especially for cryptocurrencies or other financial transactions, including know your customer, anti-money laundering, and anti-terrorism laws and regulations.

USE ALTERNATIVE DATA ENCRYPTION AND DESTRUCTION APPROACHES

Alternative data encryption and destruction approaches may help address compliance concerns regarding personal data on blockchains and address individuals' rights by using:

- Hashing or other irreversible data transformations.
- Destruction of separately stored hashing or encryption keys.
- Revocation of access rights.
- Other similar technical mechanisms.

Whether these mechanisms can meet regulators' demands for erasure remains to be seen, although the CNIL's guidance considers some of them as moving closer to the effect of data erasure (see CNIL Guidance). These techniques are typically easier to implement in private, permissioned blockchain systems, encouraging organizations to combine risk mitigation techniques.

THE FUTURE OF BLOCKCHAIN PRIVACY MANAGEMENT

Many current blockchain technology applications appear at least ambiguous from a privacy compliance perspective. Processing personal data directly on a public blockchain may, in the absence of clear regulatory guidance, involve significant business risks.

Looking forward, some technologists suggest that blockchain technology, with its data transparency and integrity features, offers unique possibilities to improve privacy by:

- Verifying and managing consent.
- Providing individuals with clear notifications and records of personal data usage across distributed systems.
- Minimizing data sharing between data controllers and their processors.

Taking this one step further, some researchers envision a future when self-governing blockchain-enabled identity and data management solutions provide the preferred way to maintain and demonstrate data privacy. For now, policymakers can support innovation by recognizing decentralized data storage models and better tailoring data privacy laws, regulations, and guidance for blockchain use cases.

10-19