Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

If applicable, insert your organization's disclaimer statement here, in black (or delete this line)

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PRV-R01**

The Privacy and Blockchain Paradox

Greg Schu, CPA, CISA, QSA

Partner, Cybersecurity – National PCI Compliance Lead
BDO Digital

Jim Amsler, FIP

Director, Governance, Risk & Compliance

BDO USA, LLP
@JimAmsler

Agenda

- Introduction to Blockchain Technology
- Privacy and Data Protection Obligations
- The Privacy Paradox
- Compliance Considerations for Companies using Blockchain

RSAConference2022

Introduction to Blockchain Technology

History and Implementation of Distributed Ledger Technologies

How did Blockchain Emerge?

ORIGIN	TRANSACTIONS	CONTRACTS	APPLICATIONS
1990s	*2000s*	*Early to mid-2010's*	*Late 2010's to 2021*

The Core - Distributed Ledger Technology

Enhanced security

Greater transparency

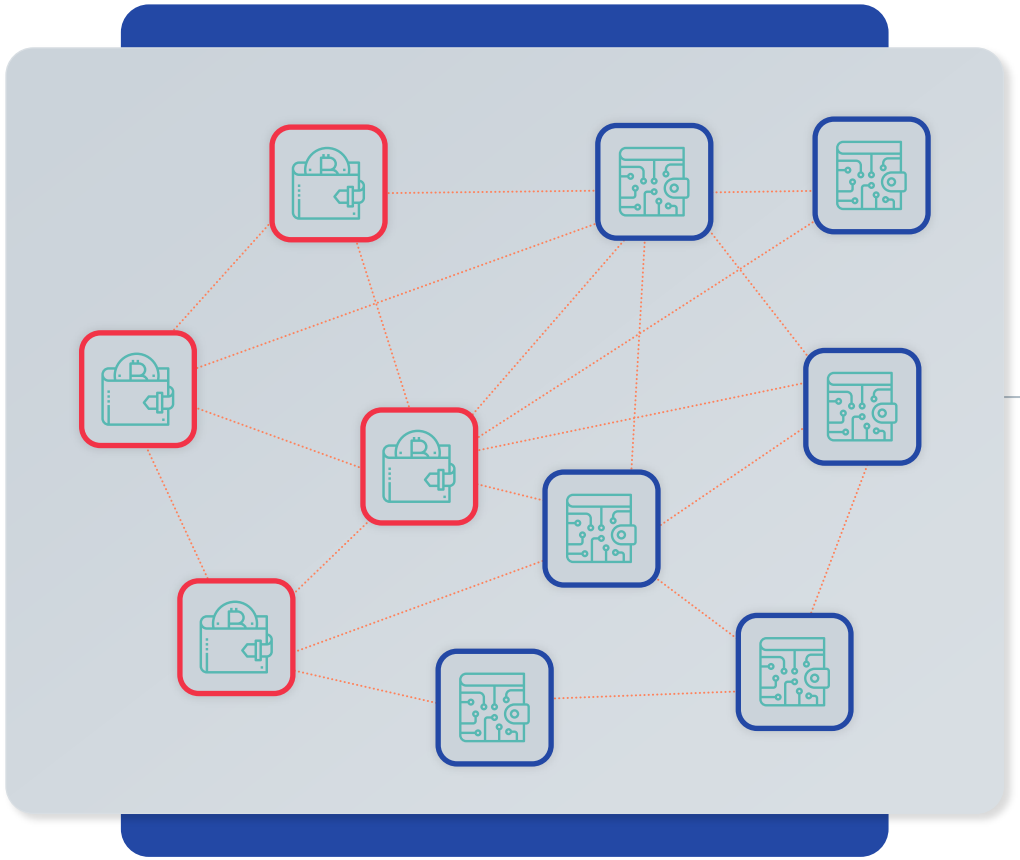
Instant traceability

Increased efficiency

Advanced automation

Source: Gartner — Blockchain Technology: What's Ahead? — [2019]; EU Science Hub — Blockchain Now and Tomorrow — [2019]; IBM — Top five blockchain benefits transforming your industry — [2018]; Blockchain Council website; Forbes website; Euromoney website

What is Blockchain?



Distributed Ledger

Replicated Across Network Nodes

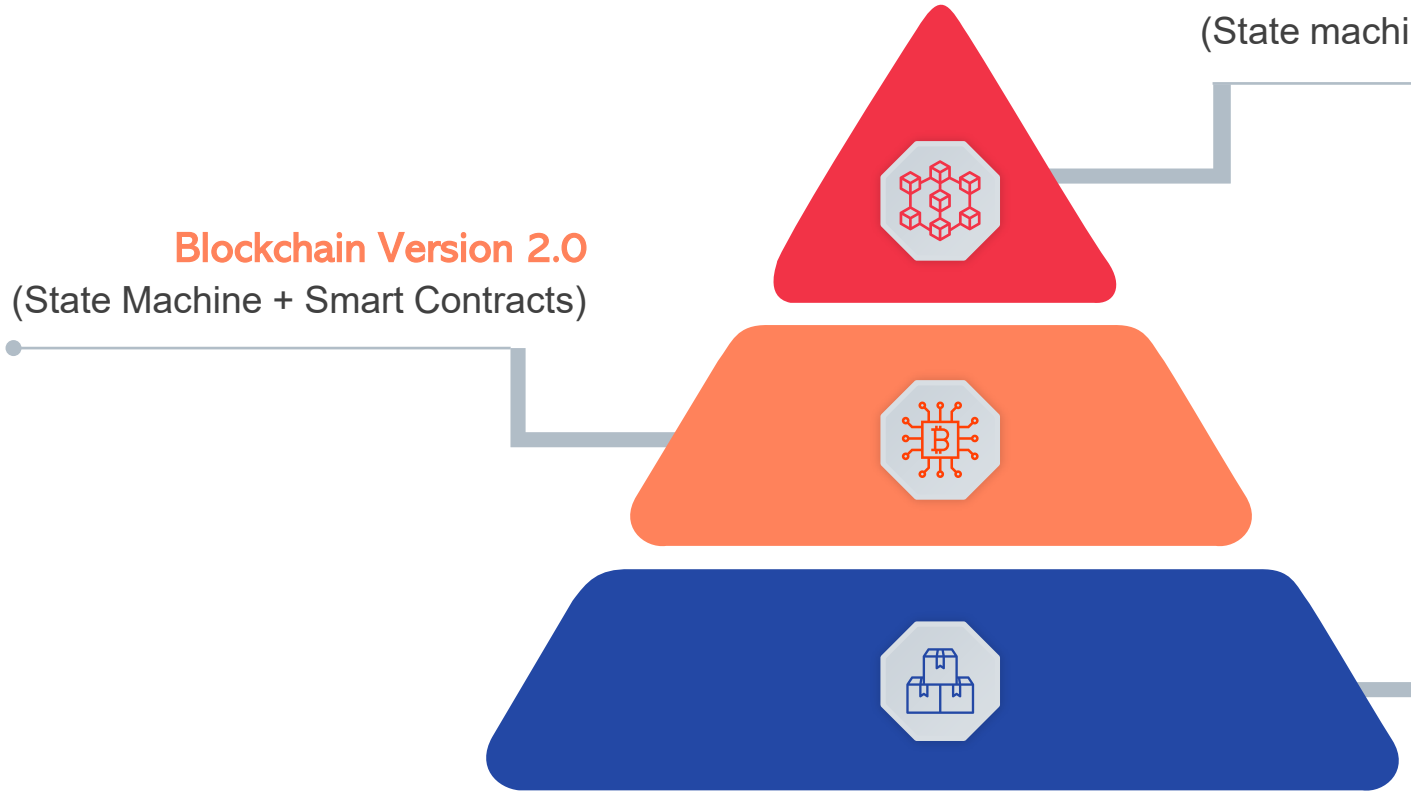
Extensible

Generations of Blockchain Technologies

Block Chain Version 3.0
(State machine + Smart Contracts + Cryptlets)

Blockchain Version 2.0
(State Machine + Smart Contracts)

Block Chain Version 1.0
(Simple State Machine)



BDO

Blockchain Variants

Public Blockchain

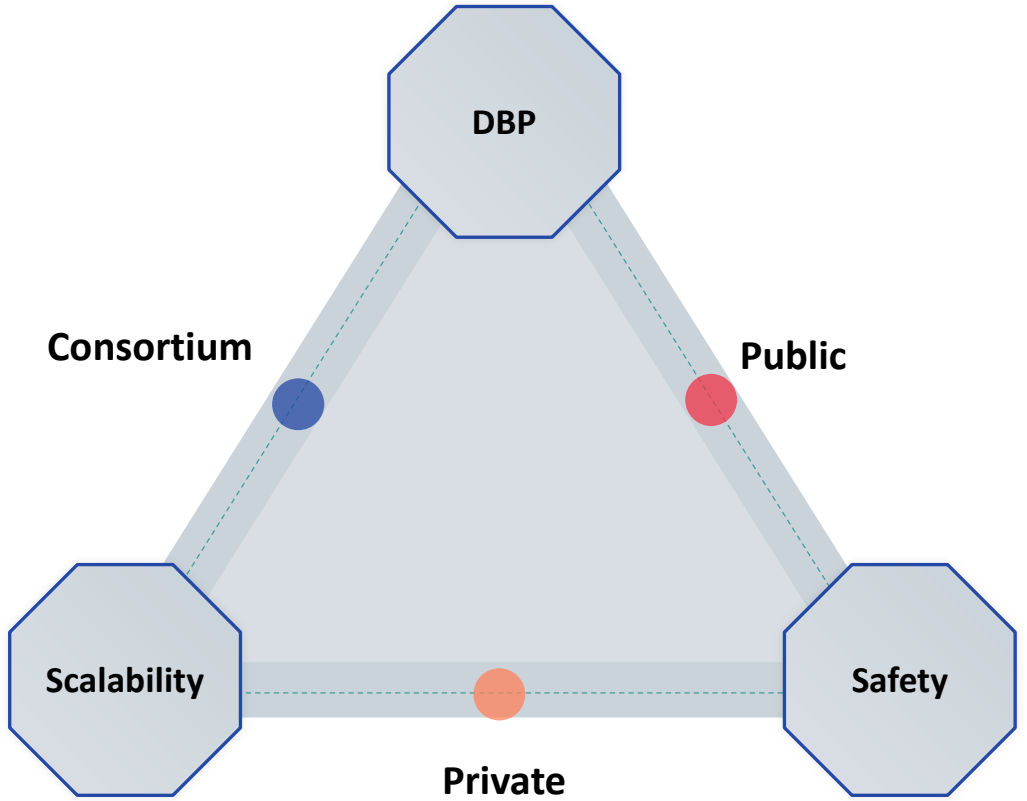
In public blockchains, distributed ledgers are visible to each user on the network. It permits public users to verify and submit new blocks of transactions recorded within the blockchain. Example: cryptocurrencies such as Bitcoin, Ethereum, Dash, etc.

Private Blockchain

Private blockchains are usually incorporated within single organizations and only permit invited users to engage in and verify transactions with permissions. Example: Multichain and Blockstack.

Consortium Blockchain

An association of multiple organizations share responsibility for governing and operating the blockchain for a shared purpose (e.g., banks participating in a payment messaging network). Examples: Ripple, R3, and Hyperledger 1.0.



Smart Contracts

User-Defined Contracts solving Privacy Challenges

Self-executing contract with terms of the agreement between buyer and seller being written directly into lines of code

Decentralized Autonomous Organizations

What is a Decentralized Autonomous Organization (DAO), and how do DAO's positively impact privacy?

Blockchain Is Not…

RSAConference2022

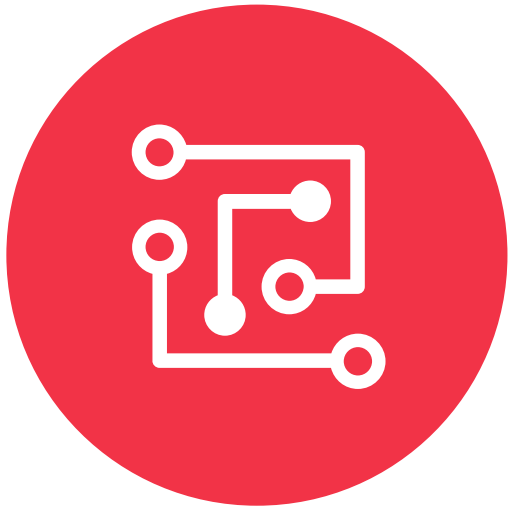
Privacy and Data Protection Obligations

Privacy and Data Protection

Privacy

Respect for…

- Private Life
- Family Life
- Home
- Communications



Data Protection

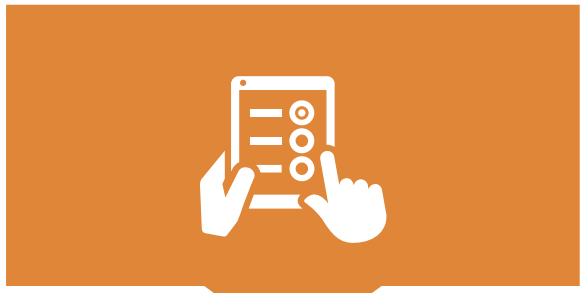
Protection of personal data

- Fair processing
- Specified purposes
- Consent or lawful grounds
- Access and rectification

Personal Data

ANY INFORMATION

When does information relate to a person?



RELATING TO

What qualifies as information?

AN IDENTIFIED OR IDENTIFIABLE

What is identity?

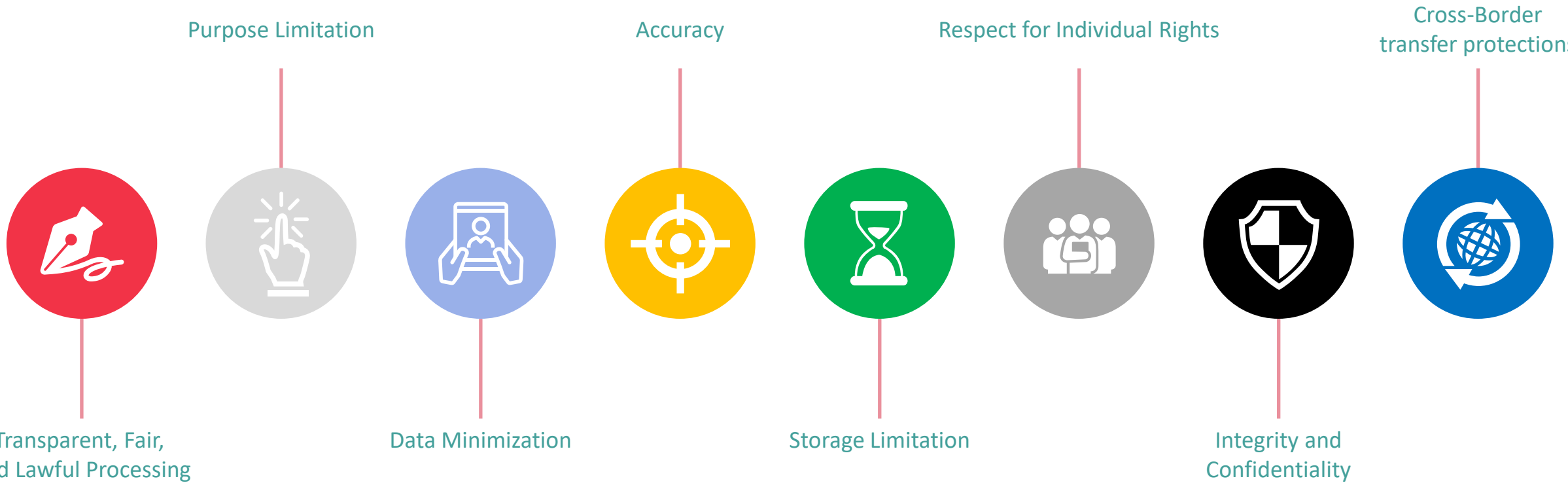
When is someone identifiable?

NATURAL PERSON

What is a natural person?

Privacy and Data Protection Domains

Privacy and Data Protection Regulations and Frameworks dictate protections and controls corresponding to these principles.



EU-Specific Rights

Data portability

Erasure and right to be forgotten

Restriction of processing

Right to object

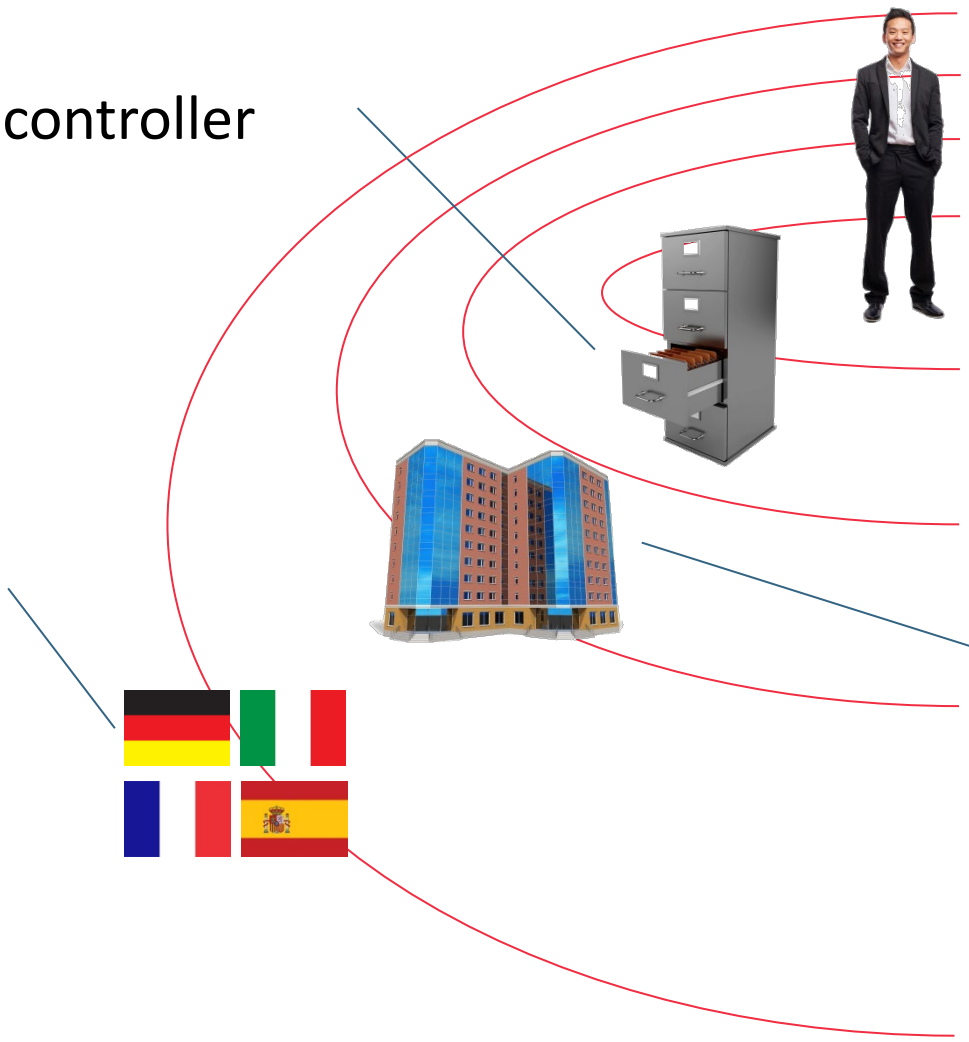
Right “not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects ... or similarly significant effects” (Article 22)

Controllers and Processors

Data controller

Data subject

Data protection authority (DPA)
Supervisory authority (SA)



Data processor

California Specific Rights

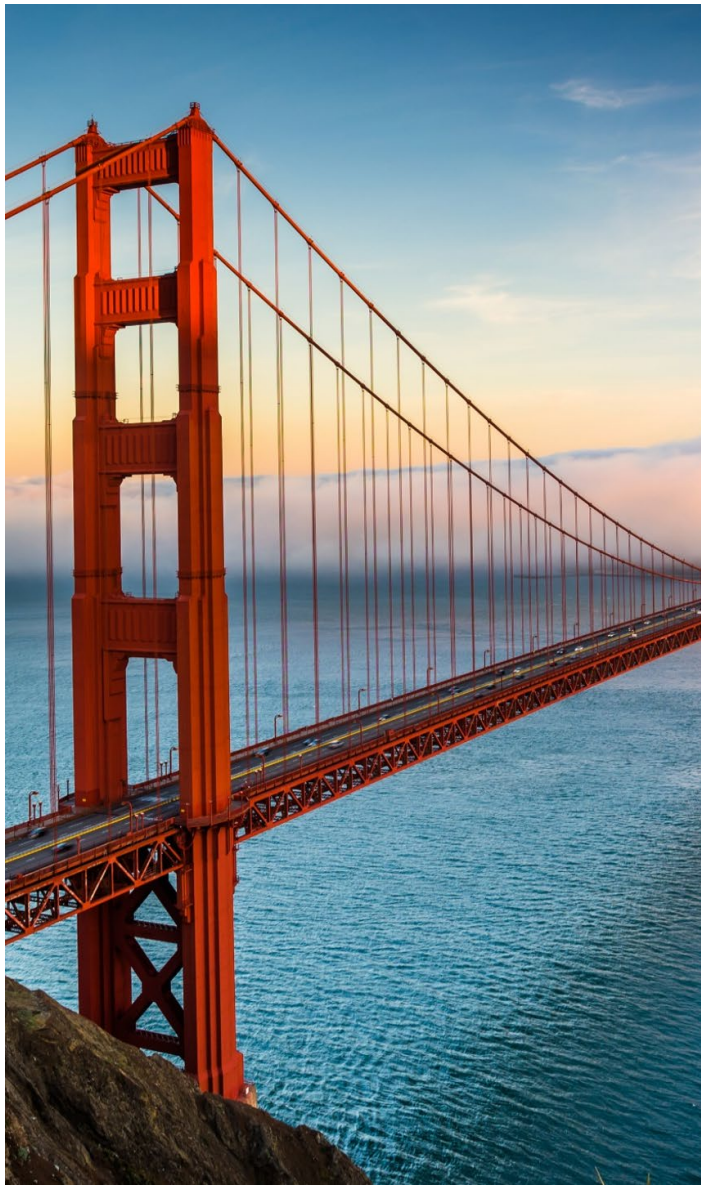
Right to request records

Right to erasure

Right to opt out of selling

Businesses must implement one or more designated means for submitting requests, including a (at a minimum) a toll-free number.

Consumers may not be discriminated against for exercising their rights.



“Do Not Sell My Personal Information”

CCPA Section 1798.135 defines specific requirements related to businesses who “sell” personal information to third parties.

The definition of a “sale” of personal information is broadly defined, and ostensibly includes almost any sharing of personal data with third parties. Businesses must:

- Provide a “clear and conspicuous” link on the corporate homepage, titled “Do Not Sell My Personal Information”
- NOT require the creation of an account in order to register this request
- Include a description of consumer’s rights and a separate link to the “Do Not Sell My Personal Information” page in the online Privacy Notice and any other description of California-specific privacy rights

RSAConference2022

The Privacy Paradox

Privacy and Blockchain

PRO'S

Immutable records

Instant traceability

Decentralized (public)

Asymmetric cryptography

Self-sovereign identity

Off-chain data storage

CON'S

Data control

Centralized (private)

Deletion

Privacy compliance

Error correction

Individual Rights

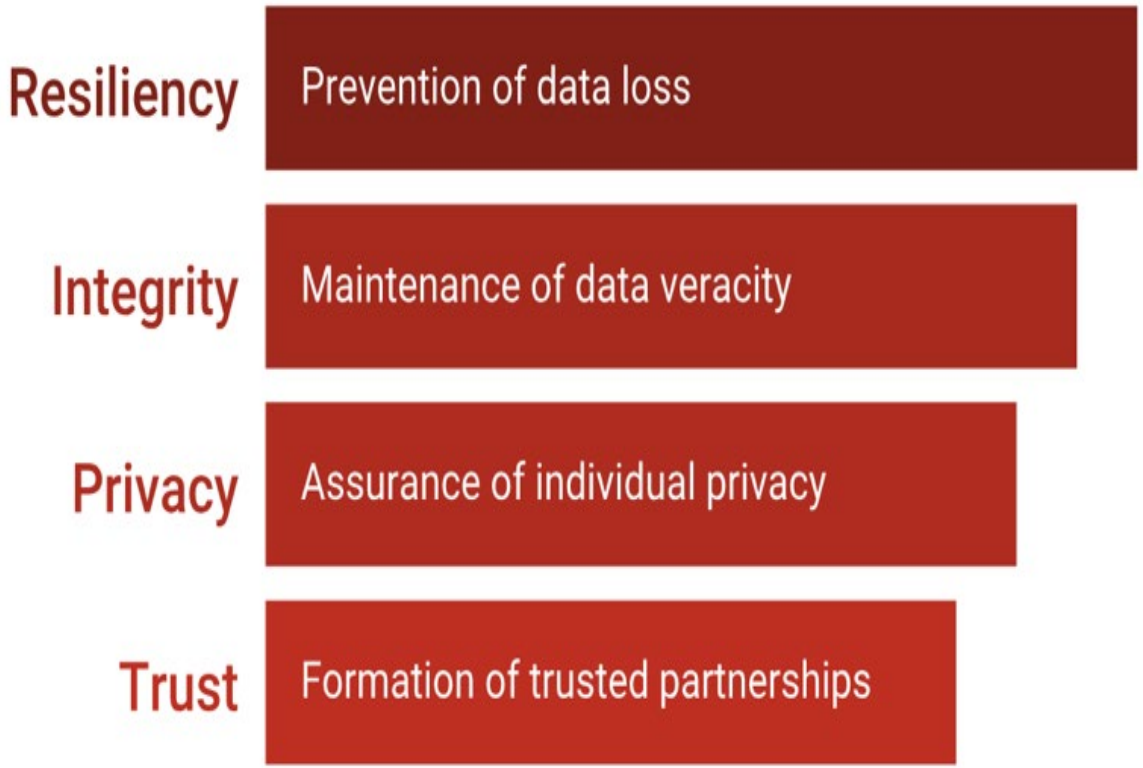
- Transparency
- Rights to Rectification, Deletion, Portability, and Limitations on Processing
- Controller / Co-Controller / Processor Relationships
- Blockchain Immutability
- Technology Leads – Regulatory Guidance Follows

Benefits of Blockchain solutions

Due to its ability to provide transparency, immutability, and decentralized storage of data, applications using blockchain for data security can soon replace existing technologies that provide centralized storage.

Benefits of blockchain for data security

- Trust
- Privacy
- Integrity
- Resiliency



Jurisdiction-Specific Considerations

Cross-Border Transfers

Anonymization / Pseudonymization Differences

Encryption Standards

RSAConference2022

Compliance Considerations

Implementing Blockchain Technologies

“Apply” Slide

- Privacy Impact Assessments
- Pilot and Implement against Targeted Use Cases
- Engage Your Regulators (DPIA)
- Be Mindful of Cross-Border Transfers
- Individual Rights
- “Permissioned” Blockchains can support governance obligations

Five considerations for blockchain applied to data privacy and GDPR

When looking at blockchain as a solution to privacy challenges, here are five things to consider which could help us all feel more at ease.

- **A technology and a regulation** – Privacy in a digital world isn't something that can be solved with technology only. On the technology side, blockchain is making tremendous progress with networks that provide value in areas as varied as food trust, shipping containers, trade finance and international payments. Respecting the privacy of data and transactions is a core tenant for these projects.

- **Opposite starting points but same underlying principles -** Blockchain and GDPR share common principles of data privacy. Both want to oversee our own digital private data transactions and payments in the case of Bitcoin, or personal data that needs to be shared with others in the case of GDPR.

- **Privacy in public networks -** Privacy doesn't necessarily mean you need a private blockchain network approach, one that requires an invitation or is membership-based. These are privacy-enabling features like those of GDPR.

- **Right to Erasure -** One of the GDPR requirements is the right to erasure when an individual asks an organization that has their personal data to completely remove that data. To comply with GDPR, no personal data should be put on the blockchain directly. Techniques exist to deal with this, which consist of putting a cryptographic hash on the chain or the "evidence" instead of the actual data.

Achieving data protection compliance in blockchain projects

Hyperledger Fabric: A permissioned blockchain solution for superior data privacy

Permissioned blockchains like Hyperledger Fabric have ensured compliance with core GDPR (General Data Protection Regulation) principles concerning privacy, confidentiality and integrity of data and features such as ‘right to be forgotten’. Here’s how:

- **Consent on data collection and processing -** The number of stake holders required for user consent for data processing is more in the permissioned blockchain setting and hence, the level of complexity to ensure compliance has increased.
- **Privacy, confidentiality and integrity -** Permissioned blockchains rely on encryption and pseudonymous identities to adhere to GDPR properties such as the unlikability of transactions, anonymity of users, and confidentiality of transactions.
- **Data minimization and purpose limitation -** Privacy by Design mandates only and necessary data transaction, which is vital in ensuring data privacy across applications. Permissioned blockchains like Hyperledger Fabric have features that enable ‘right to be forgotten’.

The developers of blockchain projects should therefore carefully analyze the kind of data intended to be stored in the blockchain and weigh up the advantages and disadvantages of the type of blockchain to be used.