Cyber Security: Privacy & Blockchain Perspective

Shahid Sharif

Secunoid Systems Inc.
http://www.secunoid.com

Goni Sarakinov

Sarakinov Consulting Inc.
https://sarakinovconsulting.com

Disclaimer & License

Disclaimer

The views and opinions expressed in this presentation are those of the authors. They do not purport to reflect the policies, views, opinions or positions of any other agency, entity, organization, employer or company.

License

This presentation is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0).

You are free to:

- Share , copy and redistribute the material in any medium or format
- Adapt , remix, transform, and build upon the material for any purpose, even commercially
- Under the following terms of Attribution: You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

License details: https://creativecommons.org/licenses/by/4.0/legalcode

Topics

- Intro
- Privacy Overview
- What is Private Data?
- Privacy by jurisdiction (We will focus on Canada, the EU and the USA)
- Privacy Considerations
- Conclusion
- Q&A

BIO's

Shahid Sharif

CCSK, CISA, CISSP, CRISC, CSSP, PCIP, PMP

IT Security professional with over 20 years of experience in various industries in different roles. Some of the highlights include:

- Application Security Assessments
- Security Architecture advisory pertaining to Mobile Devices, Networks, Applications, & Systems
- Extensive experience in managing and supporting audits related to PCI-DSS, SSAE16. CSAE3416, 5025, SOC2, and SOX
- In-depth knowledge and experience on implementing Governance, Risk, & Compliance and supporting frameworks like COBIT 5, NIST, ISO, etc
- Extensive experience in creating procedures, policies and standards
- In-depth knowledge of Business Continuity Management which includes BCP, DRP, and Crisis Management.
- Private/Public Blockchain technologies

LinkedIn: https://www.linkedin.com/in/shahidsharif/

Goni Sarakinov

SCF, CISSP, CIPM, CIPT

CEO, Sarakinov Consulting Inc., Director of Information Security & Privacy at Libra Enterprises, Inc. is a SABSA Chartered Security Architect, Certified Information System Security Professional (CISSP), Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Technologist (CIPT). Over 20 years' experience on advising both public and private sector organizations on identifying, developing and deploying solutions to address privacy regulations in Canada, USA and EU, plan and roll-out successful programs encompassing information security and privacy capabilities.

LinkedIn: https://www.linkedin.com/in/gonisarakinov

Useful Links

- Slide deck
  - GitHub: https://github.com/secunoid/presentations
  - SlideShare: https://www.slideshare.net/ShahidSharif4
- Awareness training
  - https://sarakinovconsulting.com/wp/services-grid/training

Privacy Overview

From the International Association of Privacy Professionals (IAPP):

"**Privacy** is the right to be let alone, or freedom from interference or intrusion. **Information Privacy** is the right to have some control over how your personal information is collected and used.

In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA):

"Personal information includes **any factual or subjective information**, recorded or not, about an identifiable individual"

Jurisdictions

Jurisdiction in which you are doing business matters, for example:

- In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Recent update the Digital Privacy Act added new requirements particularly:
    - Reporting of breaches is mandatory starting November 1st, 2018
    - Businesses have to keep a record of ***ALL*** breaches (whether PII is leaked or not) for 2 years
    - Fines have been introduced, up to $100,000 per breach
  - Some provinces have privacy legislation that has been deemed similar, for example Quebec, Alberta, British Columbia
- The European Union General Data Protection Regulation (GDPR)
- The United States of America does not have comprehensive federal data protection legislation, instead:
  - Every business is subject to privacy legislation at the Federal and/or State level.
  - Some States are more active particularly California
    - California passed the California Consumer Privacy Act this summer (2018) to take effect in 2020
    - It provides protection for consumers data online and is similar to the EU GDPR

Some examples of Private Data

PIPEDA

- Age
- Name
- ID numbers
- Medical records
- Income
- Ethnic origin
- Opinions
- Evaluations
- Comments
- Social status, or disciplinary actions
- Employee files
- Financial records

GDPR

- Personal Data - Ability to identify an individual from the data
  - IP Address
  - Email address
  - Address
  - etc.
- Special categories of Personal Data
  - Date of birth
  - Religion
  - Gender
  - Personal lifestyle/affiliations
  - Genetic
  - Race
  - Ethnicity
  - Health, etc.

EU GDPR-1/2

GDPR stands for General Data Protection Regulation. It is a regulation in EU law on data protection and privacy of European Citizens residing in European Union. It has a global reach with tough sanctions for non conformance. It is all about providing assurances and rights to EU Citizens residing in EU, whose data is being collected by businesses to deliver a service or product.

- It has evolved from Data Protection Directive, which came out in 1995
- Adopted in April 2016 with a two year grace period, which came into effect in mid 2018
- Addresses modern use of data
- Respect the individual's right to their personal data

GDPR-2/2

The French Data Protection Supervisory Authority (the CNIL) is one of the first to publish initial thoughts on blockchain and GDPR compatibility. They covered 4 topics:

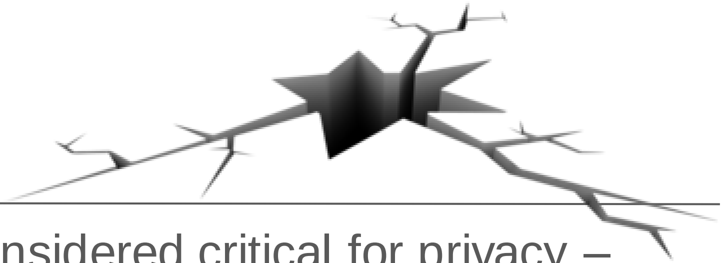
1. What solutions for a responsible use of Blockchain involving personal data?
2. How to minimize risk for data subjects when the processing of their data relies on a blockchain?
3. How to ensure the effective exercise of the data subjects' rights?
4. What are the security requirements?

Considerations
Architecture
Vulnera
Priva
Alt Coins
Cryptocurrency
Block
Ether
Hype
Tezos
IOTA
Neo
Mobile Payments
Proof of Work
Secure Code Analysis
Cryptoeconomics
Distributed Ledger Technology
IT Security
Compliance
Data Classification
Data Retention
Risk Management

Blockchain Strengths

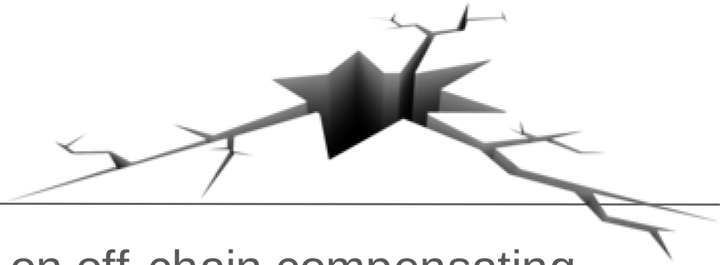
- Note that not all data on a blockchain is encrypted, however data encryption can be made a default easier.
- Another advantage is that data can be processed without the use of a key.
- Because data on the blockchain is encrypted and split up, getting access is more complex – the malicious actor need to decrypt all the blocks that the data is spread over which use a different algorithms for their security.
- Blockchain also has stronger verification controls than traditional models.
- Blockchain use for authenticating identity is particularly high.
- Allows for higher quality of data that is complete, consistent and accurate (for example, PIPEDA calls for maintaining the accuracy of records)

Blockchain Weaknesses



- Where Blockchain fails is in areas that are considered critical for privacy – access controls and data destruction
- Access is either all or nothing – i.e. access is public for public blockchains or permissions are given to select groups of entities on permissioned blockchains
- Even on permissioned blockchains it not possible to limit access to a part of the blockchain, they would have access to the whole blockchain
- Once data is on the blockchain it is not possible to destroy it
- It is also not possible for users who interact with the data to remain anonymous – once data is on the blockchain it’s there forever

Private & Public Blockchains



- Consortiums (Private Blockchains) could rely on off-chain compensating controls to address Confidentiality issues, as part of Consortium Governance.
- Public blockchains currently lack the controls required to provide forward looking Confidentiality requirements, and any data stored in a public blockchain could be considered to be at risk and potentially exposed in the future.
- A review of use cases, either in public or consortium domains, would reveal that Database technology is not challenged by blockchain technology when considering confidentiality and data retention requirements.

Data Classification

- Consideration should be placed on the classification of the data (all of the data that the business will be handling), specifically around the inclusion of data elements that require High Confidentiality. For example, this can be Personal Identifiable Information (PII) or business sensitive:
    - Customer information
    - Employee information
    - Intellectual Property
- Public and Consortium Blockchains may not suitable for sharing data across parties, when the data needs to remain confidential to those parties.

Data Protection-1/2

- Storing or managing data requires that you pay attention to data security requirements. Not doing so could lead to a mis-application of blockchain technology.
- Use of blockchain technology for storing PII is strongly not recommended, as it is not likely to comply with evolving privacy legislation:
  - Once the data is shared, it can not be unshared
  - Data encryption, as a confidentiality control, is exposed to technology obsolesce
  - Data that has been shared, and protected with current encryption standards, could be exposed in the future
  - Current technologies don’t address data retention requirements
  - Data stored in a blockchain is immutable and cant be updated as per new encryption standards

Data Protection-2/2

- Depending on the jurisdiction where you will be deploying or using blockchain technology, they may have privacy requirements and/or recommendations as they relate to the use of blockchain technology.

Conclusion

- Requirements, Requirements, Requirements
- Know the laws of the Jurisdictions you will be targeting
- Know what data you are collecting
- Know why you are collecting the data
- Know how long you can keep the data
- Document the design

Hint: Consult with qualified Privacy & Security SMEs if you need help.

Q
&
A
Architecture
Vulnerability
Compliance
Privacy
Alt Coins
Cryptocurrency
Distributed Ledger Technology
IT Security
Risk Management
Hacking
Ransomware
Mobile Payments
Proof of Work
Secure Code Analysis
Cryptoeconomics
Hyperledger
Tezos
IOTA
Neo
Compliance
Data Classification
Data Retention

Thank You!