DATA PRIVACY

BECKY CHRISTMAN

PURPOSE OF TONIGHT'S TALK

- Explore the question, "What is data privacy?"
- Gain understanding of emerging technologies addressing data privacy which are being developed by the **Linux Foundation Hyperledger Indy** and **Aries** projects.
- Suggest aspects of data privacy that could be explored in a future session.

DATA PRIVACY INCURSIONS MAKE HEADLINE NEWS

- 2017 Equifax hack puts 145.5 million people at risk for identity theft.
- Facebook involvement in 2016 presidential election investigated by Congress.

WHEN YOU HEAR **DATA PRIVACY**,
WHAT COMES TO MIND?

"Every century or so, fundamental changes in the nature of consumption create new demand patterns that existing enterprises can't meet."

~ Shoshana Zuboff, author of

"The Age of Surveillance Capitalism"

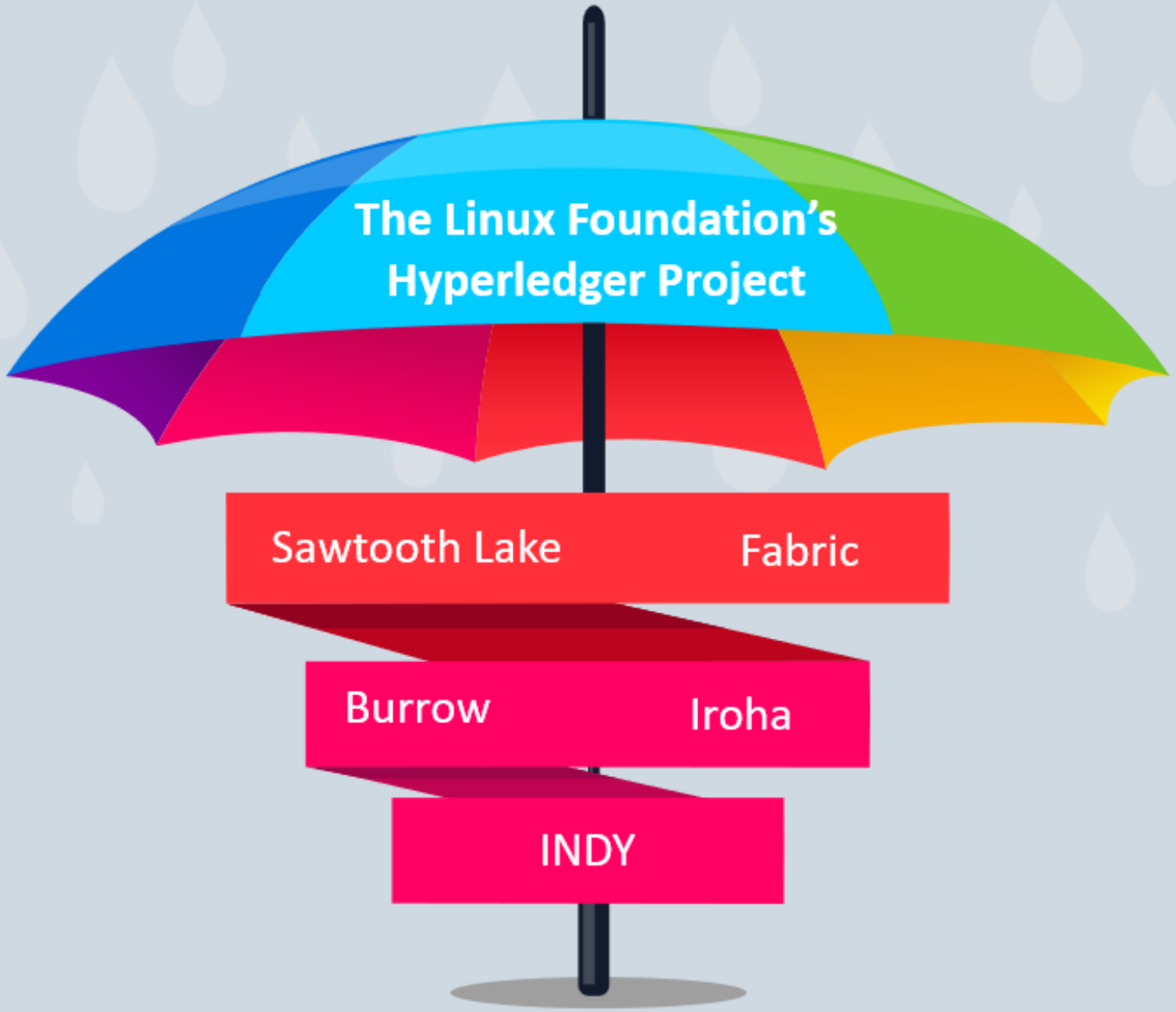
WE'RE IN A TIME OF FUNDAMENTAL CHANGE...

- Behavioral data is a commodity to be mined, bought, and sold for the purpose of predicting and influencing future behavior of individual people.

- Previously assumed privacy boundaries no longer exist and we are being acclimated to the loss.

- Just as totalitarianism was something totally new in the 1920's, **surveillance capitalism** is something new and never before seen.

LET'S TALK TECHNOLOGY...



HYPERLEDGER UMBRELLA

BLOCKCHAIN-RELATED PROJECTS


HYPERLEDGER
INDY


HYPERLEDGER
ARIES


HYPERLEDGER
URSA

DATA PRIVACY: INTERTWINING TECHNOLOGY REALMS

- Identity Management
- Privacy by encryption
- Communications
- Data aggregation (avoidance thereof)

CURRENT SITUATION WITH CENTRALIZED IDENTITY MANAGEMENT

- Identity data is stored in centralized silos making prime targets for hackers.
- Username/password authentication is a huge hassle for users and easy to hack.
- Authentication (OAUTH) through Facebook, Google, Microsoft, etc. facilitates aggregation of personal data.

PRIVACY

REQUIRES ENCRYPTED DATA EXCHANGES OVER THE WIRE AND ENCRYPTED STORAGE AT THE ENDPOINTS

COMMUNICATIONS

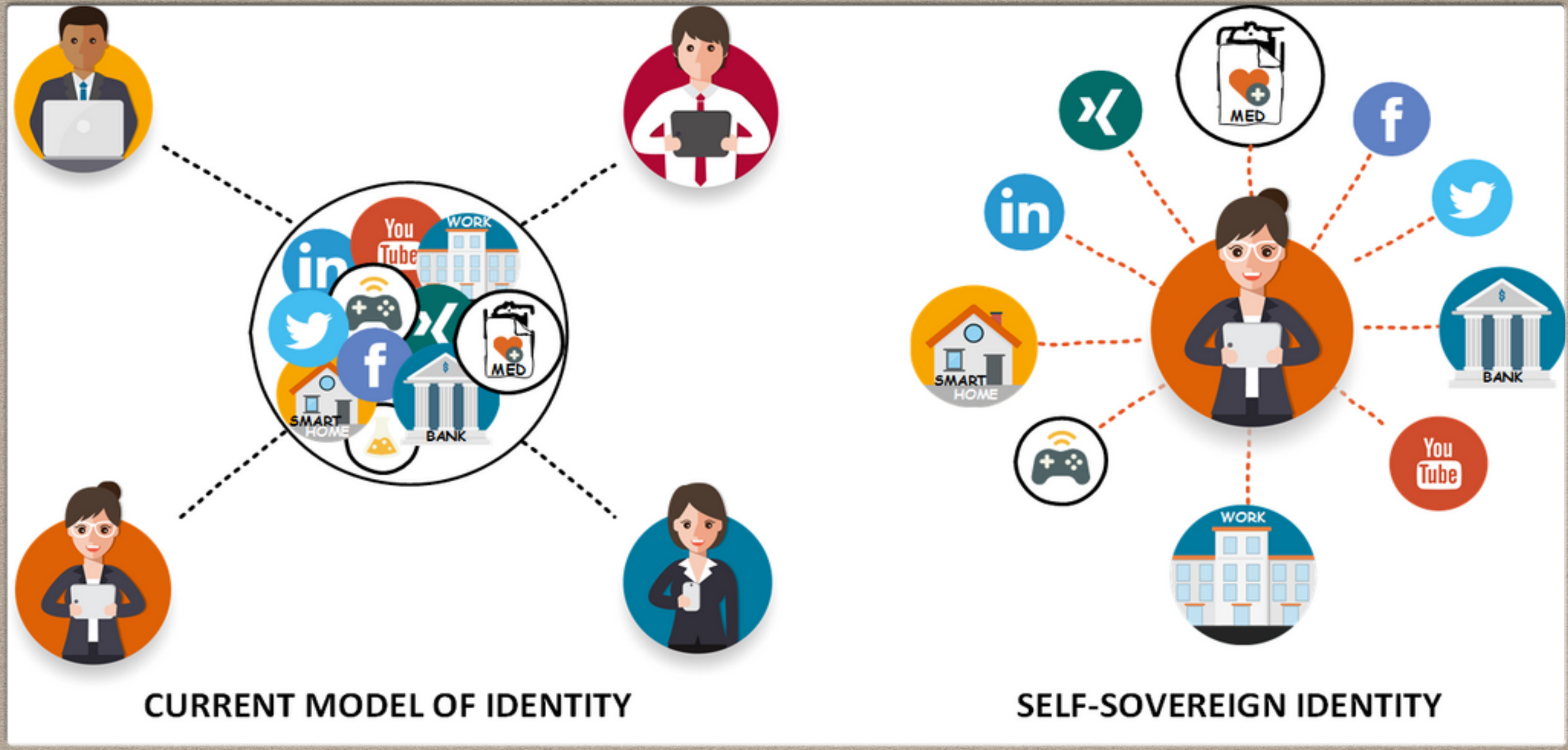
- Phone/text
- Email
- Search and web browsing
- **Messaging ← Hyperledger Aries addresses**

AGGREGATION OF PERSONAL DATA:
YOUR DIGITAL FOOTPRINT

- Social Media
- Email
- Searches
- Location services
- Purchases
- All digital interactions…

PRIVACY TECHNOLOGIES ADDRESSED BY HYPERLEDGER INDY, ARIES, URSA

INDY	Self-sovereign identity & verified credentials on a distributed ledger
Aries	Wallet and ledger-agnostic agents
Ursa	Cryptography library



CENTRALIZED VERSUS DECENTRALIZED

WITH SELF-SOVEREIGN IDENTITY (SSI), YOU OWN AND CONTROL YOUR CREDENTIALS.

THE SOLUTION: SELF-SOVEREIGN IDENTITY (SSI)

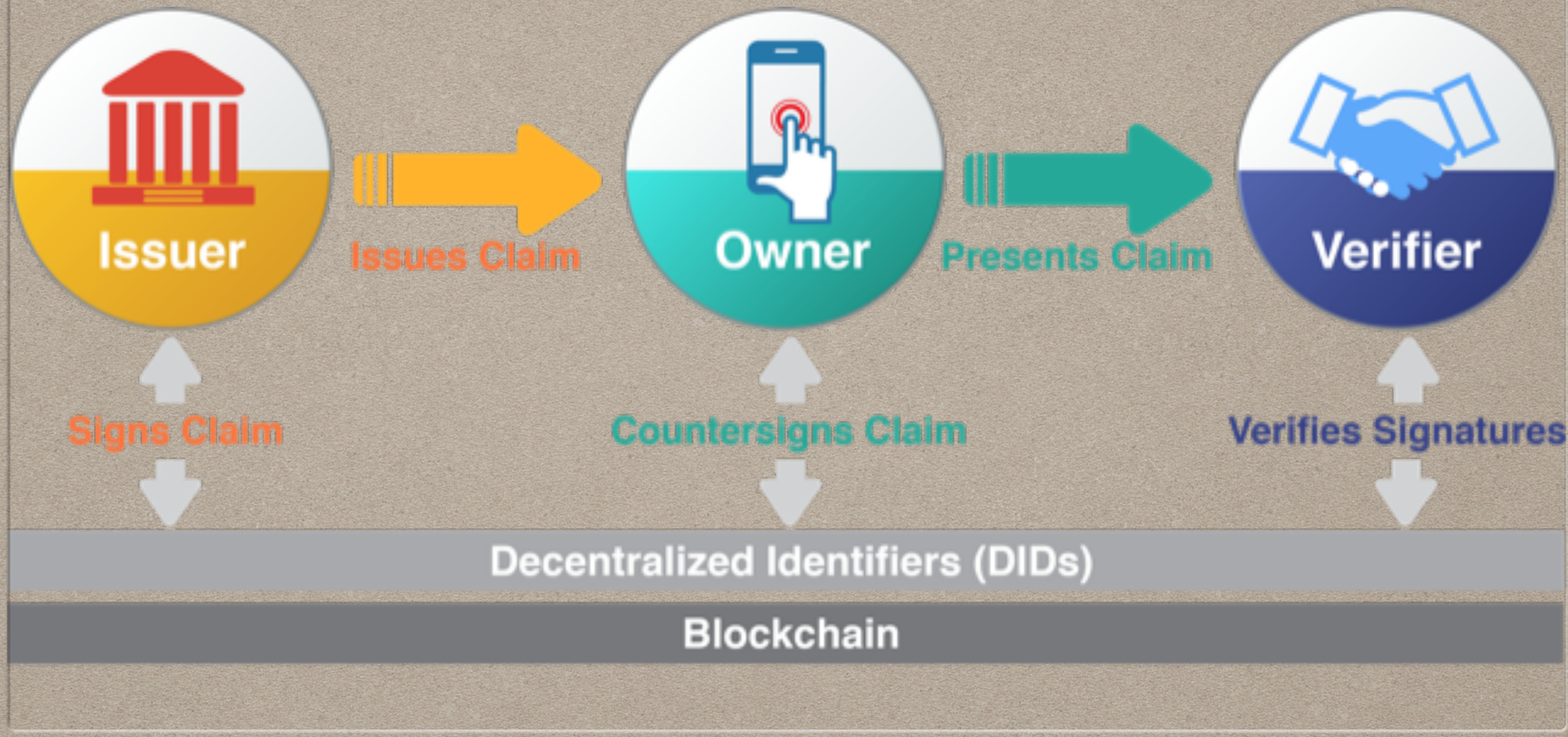
- A person owns his/her own identity credentials in a digital wallet. No identity silo to hack!
- Exchanges of credentials are encrypted with keys specific to the relationship for privacy.
- Communications are not correlatable to a legal identity. This stops data aggregation.

WHAT IS A CREDENTIAL?

- Drivers license
- Passport
- Diploma
- Proof of employment
- Proof of something like age ≧ 20
- Etc.

DIGITAL WALLET

HOLDS VERIFIED CREDENTIALS AND MORE...

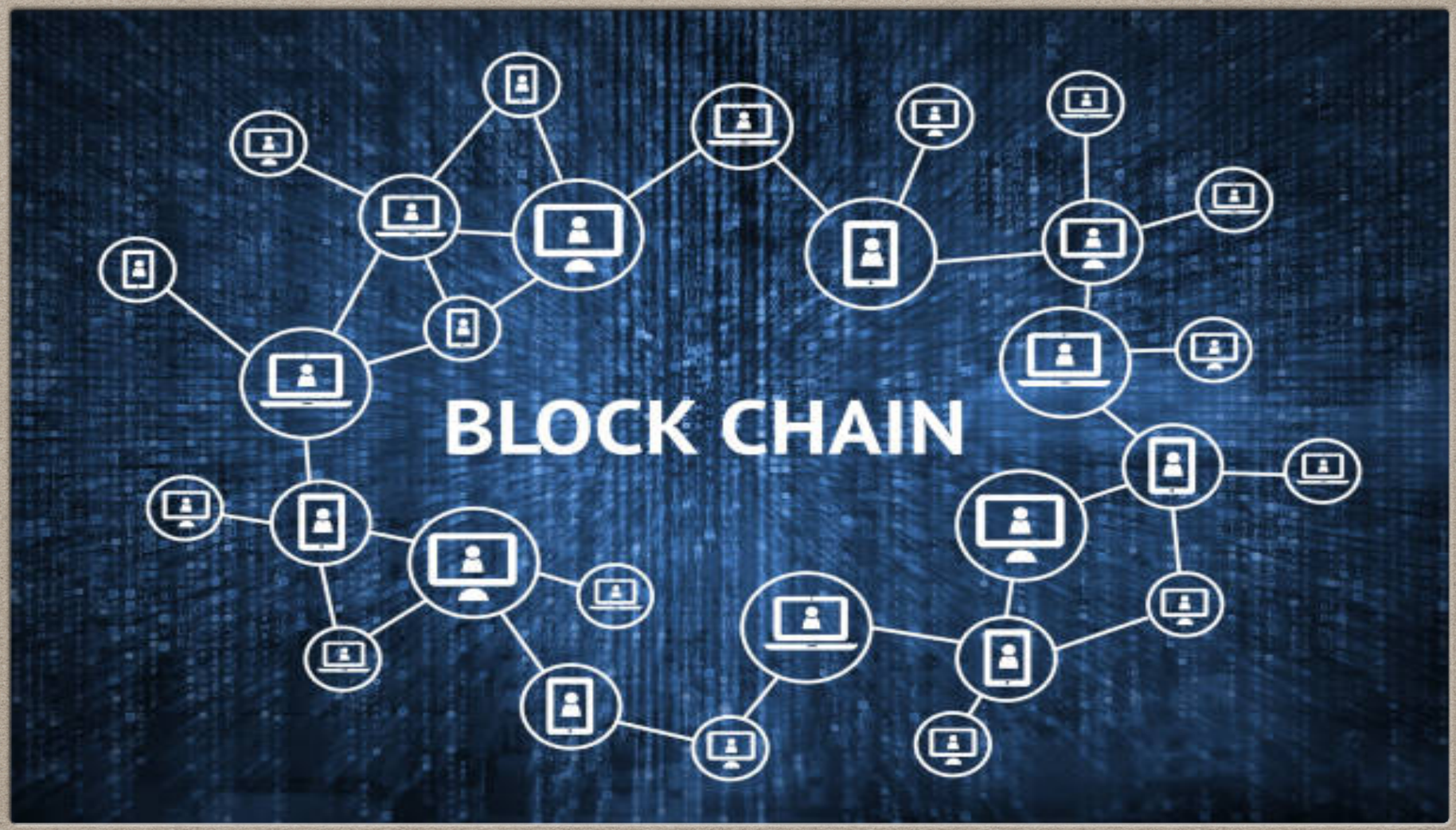


VERIFIED CREDENTIALS

- Credential owner reveals only the information needed by the verifier.
- Issuers can revoke credentials.

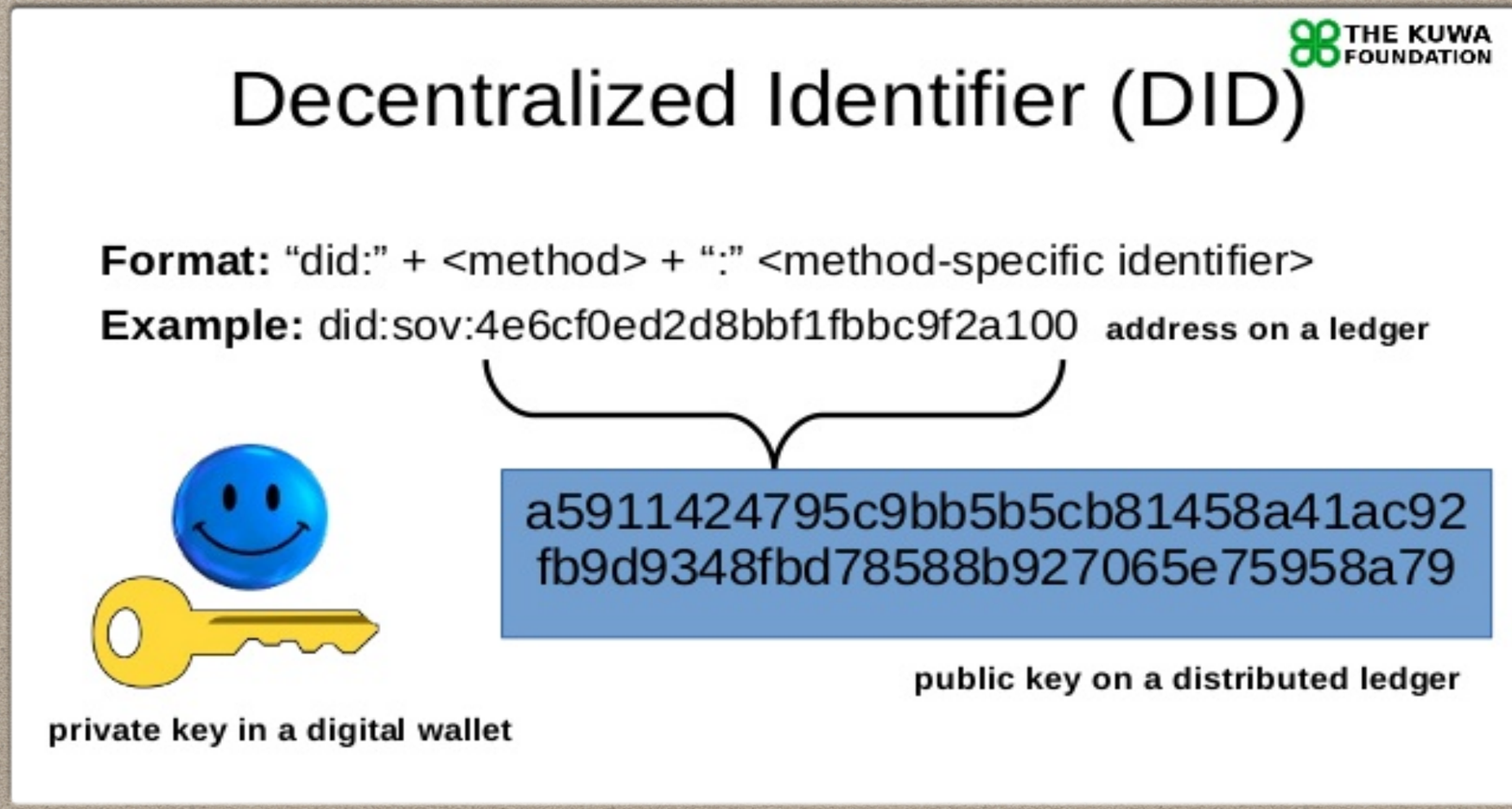
BLOCKCHAIN

A DISTRIBUTED LEDGER
EXAMPLE IS BITCOIN



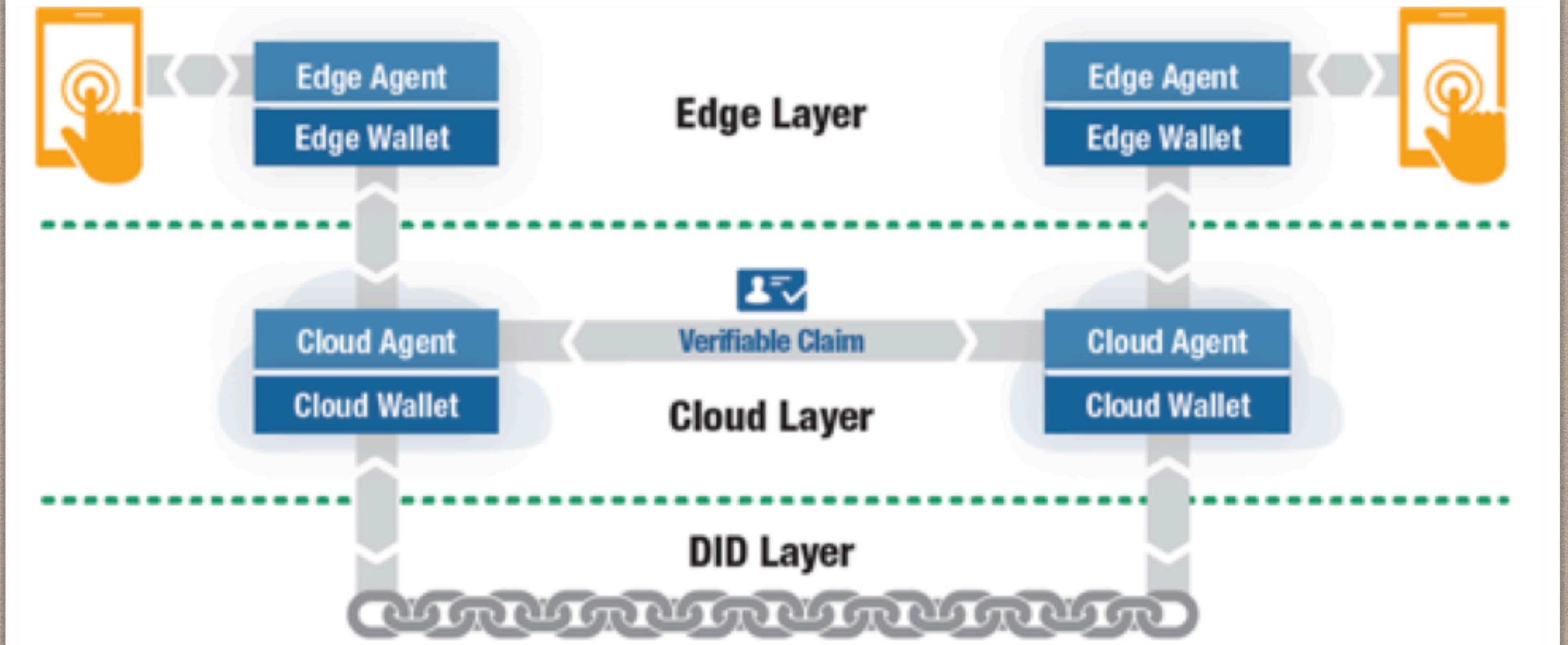
DISTRIBUTED IDENTIFIER (DID)

A globally unique **identifier** registered with a **distributed** ledger technology.



ARIES WALLET DIGITAL WALLET HOLDS:

- Verified Credentials
- Pairwise DID credentials for logins
- Relationship pairwise DID credentials for private communications
- May be expanded in the future



AGENT-TO-AGENT COMMUNICATIONS

ENCRYPTION KEYS BELONG TO ONLY ONE RELATIONSHIP

RECAP

- Self-sovereign identity is distributed identity management where each person stores his/her digital identities in a digital wallet.
- Verified credentials replace paper-based credentials such as diplomas, drivers license, passport, etc.
- PairwiseDID communications provide secure communications with encryption keys unique to the relationship.

LOOKING BACK TO OUR EARLIER BRAINSTORMING:

WHICH OF THE **DATA PRIVACY** CONCERNS ARE ADDRESSED BY THE HYPERLEDGER INDY, ARIES, URSA PROJECTS?

WHICH CONCERNS HAVE NOT BEEN ADDRESSED?

FOR MORE INFORMATION:

- The Sovrin Foundation at https://sovrin.org/
- The Linux Foundation Hyperledger Indy Project at https://www.hyperledger.org/projects/hyperledger-indy
- The Linux Foundation Hyperledger Aries Project at https://www.hyperledger.org/projects/aries
- “The Age of Surveillance Capitalism: the Fight for the Future at the New Frontier of Power”, Shoshana Zuboff

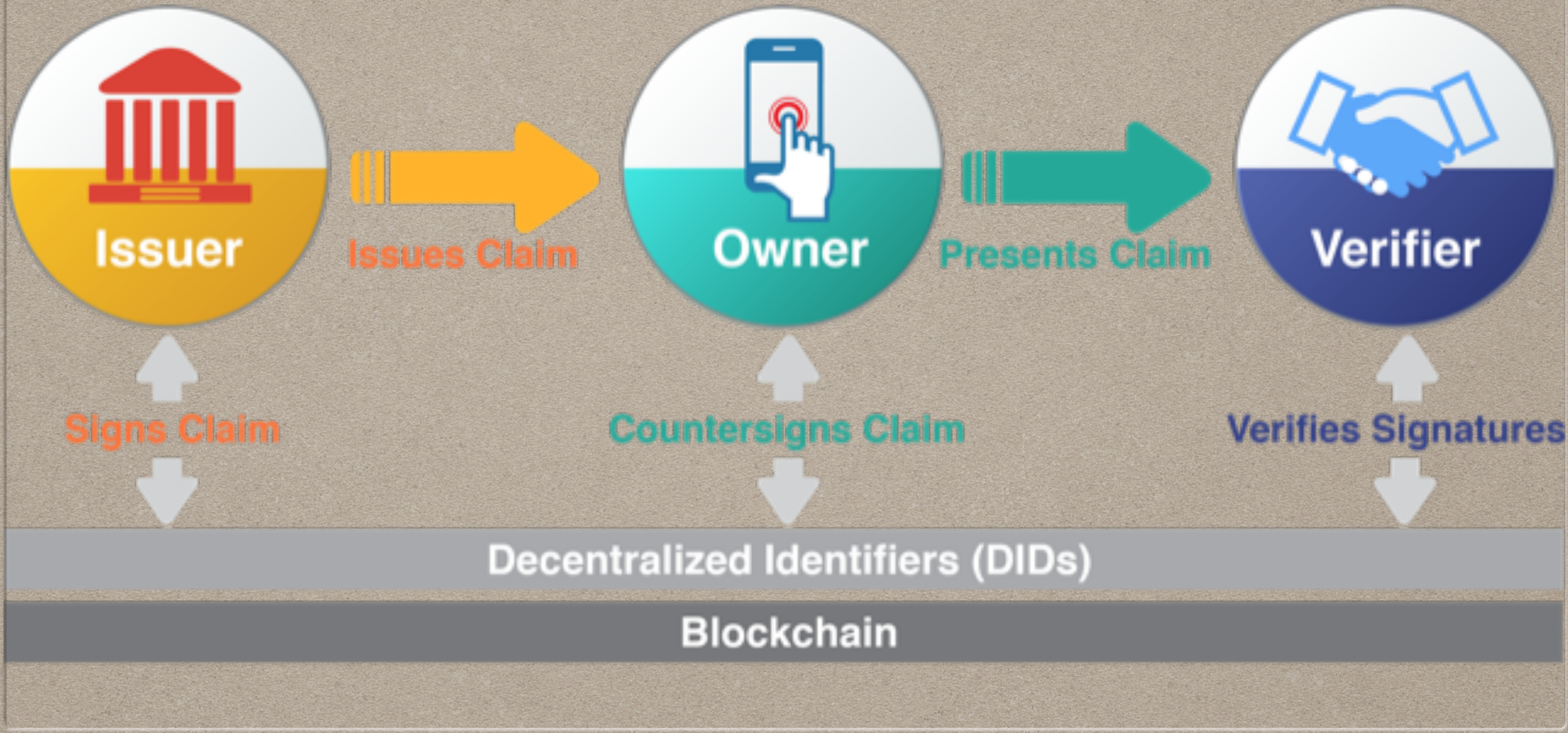
CONCLUSION

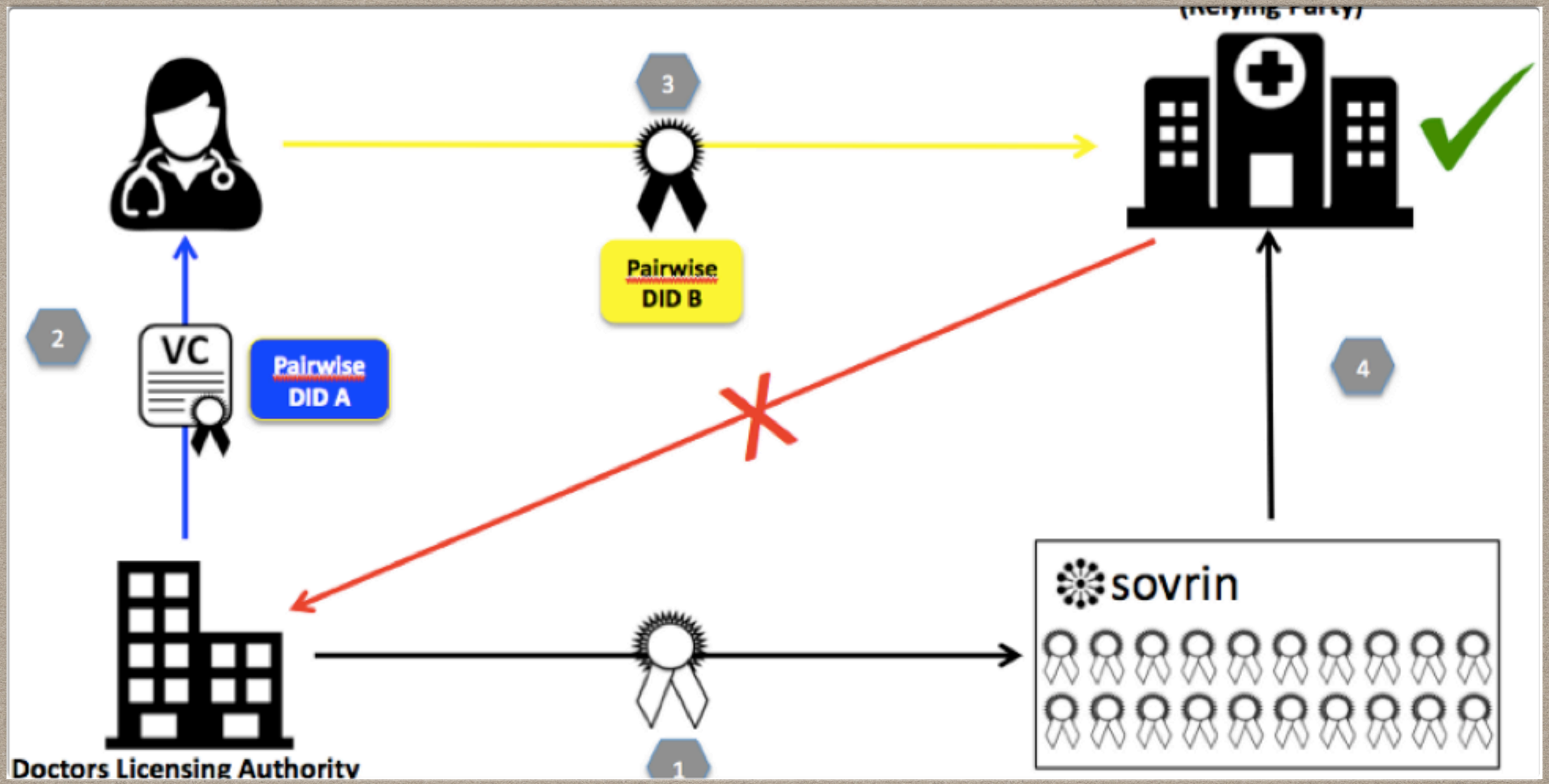
Decentralized self-sovereign identity management will solve the problems we're having with:

- Existing centralized identity management
- Privacy
- Aggregation of personal data

FOR MORE INFORMATION:

- The Sovrin Foundation at https://sovrin.org/
- Evernym at https://www.evernym.com/
- The Linux Foundation Hyperledger Indy Project at https://www.hyperledger.org/projects/hyperledger-indy
- The Linux Foundation Hyperledger Aries Project at https://www.hyperledger.org/projects/aries


Issuer
Issues Claim
Owner
Presents Claim
Verifier
Signs Claim
Countersigns Claim
Verifies Signatures
Decentralized Identifiers (DIDs)
Blockchain



EXCHANGE OF VERIFIED CREDENTIALS

USING WALLETS AND PAIRWISE DID


Issuer
Wallet
(Web-based)
Ledger
(Blockchain)
Verifier