IMPLEMENTATION OF AN IDENTITY VAULT SMART-CONTRACT

Authors:

Chan Yeong Hwang

Elina Jankovskaja

Messilva Mazari

Karima Sadykova

SORBONNE UNIVERSITÉ

Supervisor:

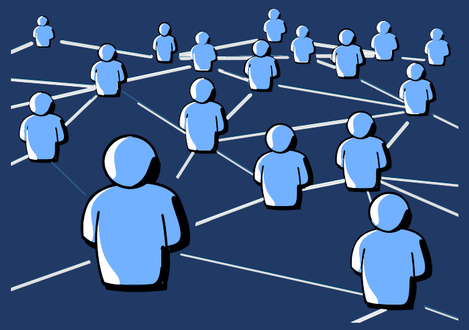
Nour El Madhoun

In collaboration with

Daniel Maldonado-Ruiz

SUMMARY

WHAT IS THE BLOCKCHAIN?



A TECHNOLOGY FOR STORING AND SHARING DATA, OPERATING WITHOUT CENTRAL CONTROL BODY

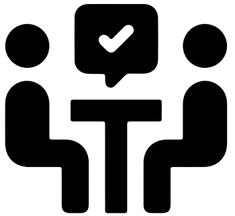
A KIND OF DISTRIBUTED DATABASE THAT CONTAINS THE HISTORY OF ALL EXCHANGES EXCHANGES BETWEEN ITS USERS SINCE ITS CREATION

CONCEPT OF THE BLOCKCHAIN

Distribution

Transparency

Security



Consensus

Immuability

OPERATION

ALICE

A USER A SUBMITS A TRANSACTION ON THE BLOCKCHAIN (TRANSFER OF MONEY, DOCUMENT, ETC.), TO A USER B.

TRANSACTIONS ARE GROUPED IN A BLOCK

THE BLOCK IS VALIDATED BY THE NETWORK NODES USING CRYPTOGRAPHIC TECHNIQUES

ONCE THE BLOCK IS VALIDATED, IT IS ADDED TO THE BLOCKCHAIN.

BOB

B RECEIVES THE TRANSACTION FROM A

SMART CONTRACTS

- CODE (COMPUTER LANGUAGE)
- STORED IN THE DISTRIBUTED DATABASE OF A BLOCKCHAIN NETWORK
- CALLED ALSO "DAPPS"
- CAN CHANGE ITS OWN STATE, E.G. CHANGE A VARIABLE, TRANSFER MONEY.
- WITHOUT HUMAN INTERVENTION - « CODE IS LAW »

COMPARISON BETWEEN TRADITIONAL CONTRACT AND SMART CONTRACTS

LIMITATIONS OF TRADITIONAL CONTRACTS

PASSIVE

ASYMMETRIC INFORMATION

INEFFICIENT

EXPENSIVE

USER ERROR AND FRAUD

ADVANTAGES OF SMART CONTRACTS

ACTIVE EXECUTION

COMPLETE REGISTRATION AND AVAILABLE DATA

REDUCED FEES

EFFICIENT

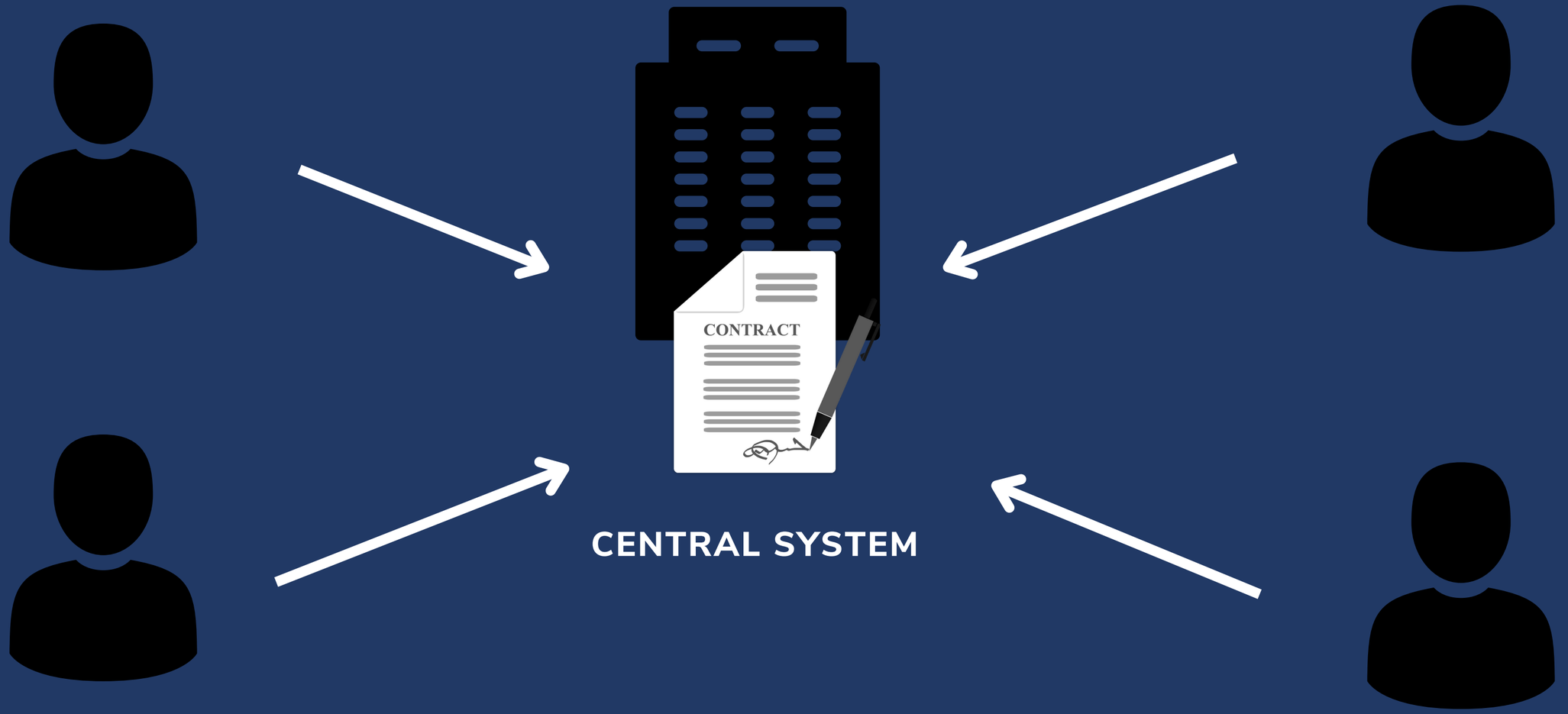
ELIMINATION OF USER ERRORS

OBJECT-ORIENTED LANGUAGE

ETHEREUM BLOCKCHAIN

INTRODUCTION TO THE PROBLEM

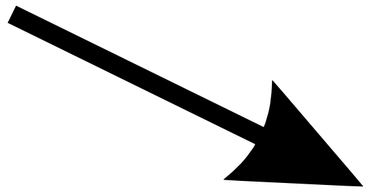
- PARTIES WHO WISH TO TRANSACT WITH EACH OTHER DO SO VIA THE CENTRAL SYSTEM

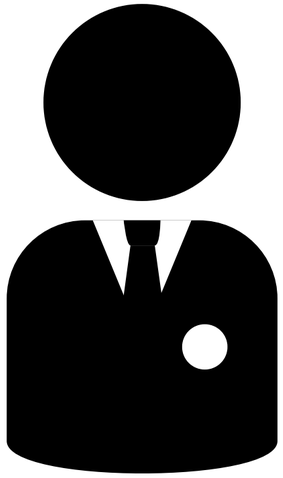


UNIVERSITY AND STUDENT CARDS

EMAIL, NAME, CVEC...

STUDENT

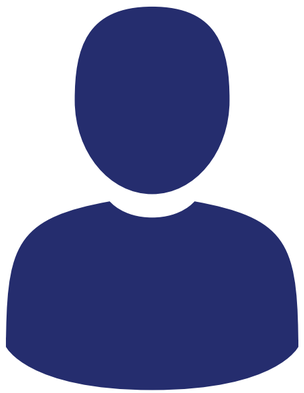




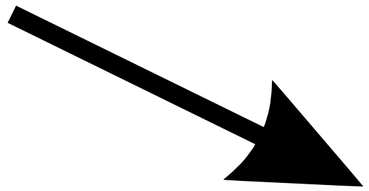
THE ADMINISTRATION

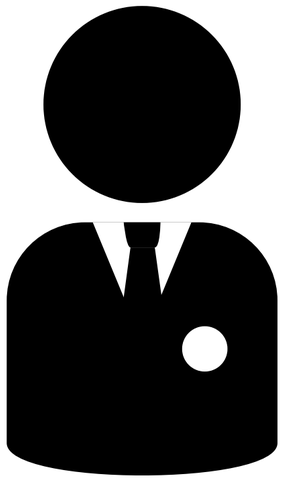
SCIENCES SORBONNE UNIVERSITÉ

UNIVERSITY AND STUDENT CARDS

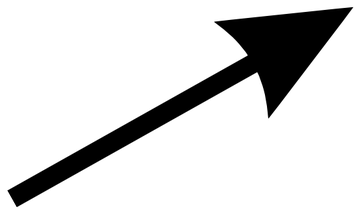


STUDENT





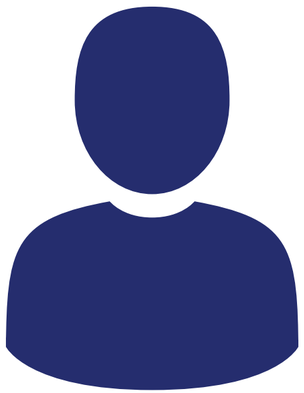
THE ADMINISTRATION



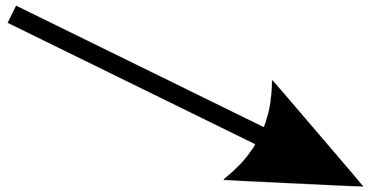
EMAIL, NAME, CVEC...

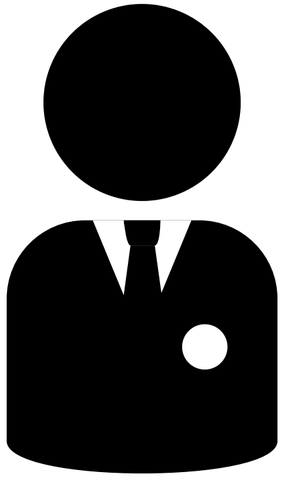
SCIENCES SORBONNE UNIVERSITÉ

UNIVERSITY AND STUDENT CARDS

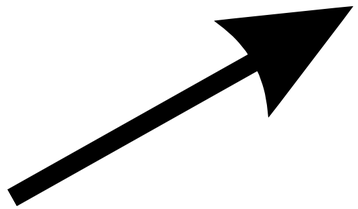


STUDENT





THE ADMINISTRATION



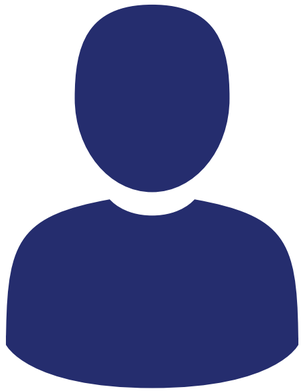
EMAIL, NAME, CVEC...

SCIENCES SORBONNE UNIVERSITÉ

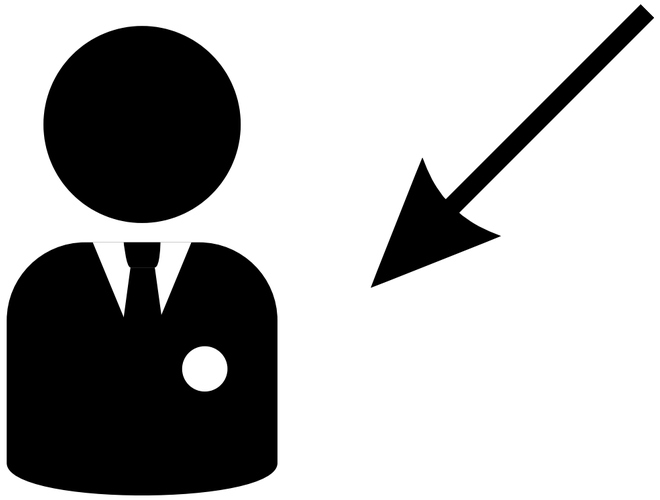
UNIVERSITY AND STUDENT CARDS

ID 28613456

SCIENCES SORBONNE UNIVERSITÉ

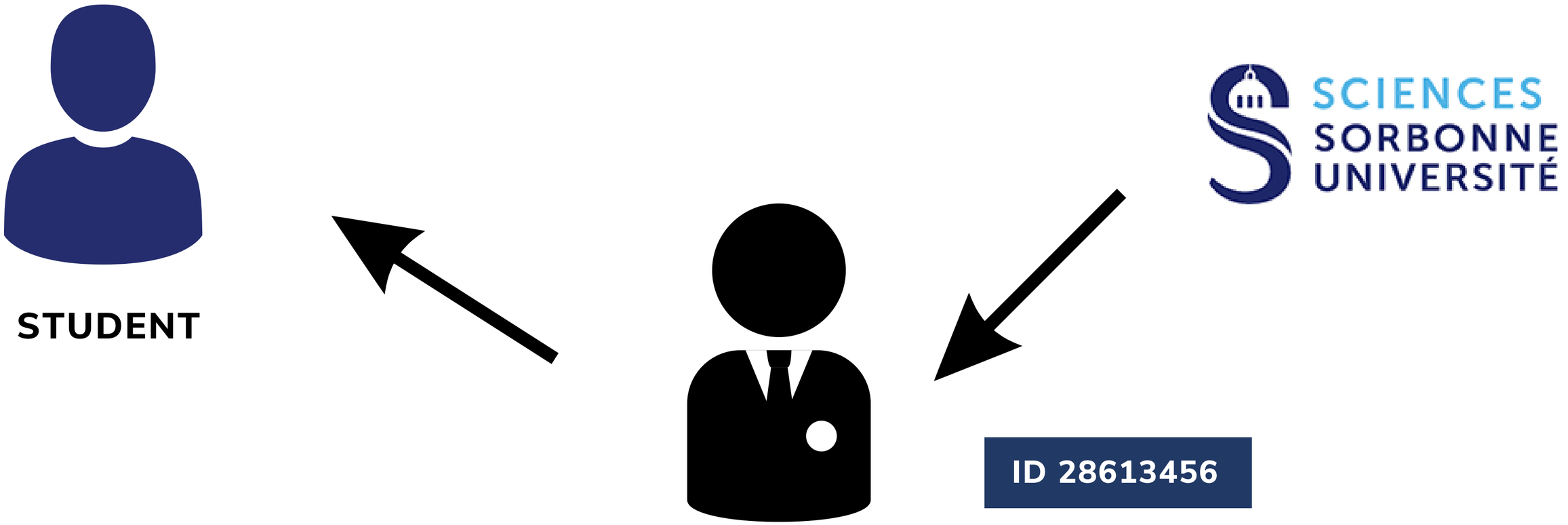


STUDENT

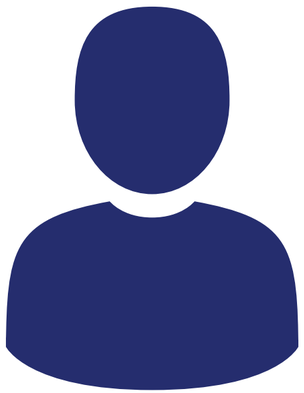


THE ADMINISTRATION

UNIVERSITY AND STUDENT CARDS



UNIVERSITY AND STUDENT CARDS



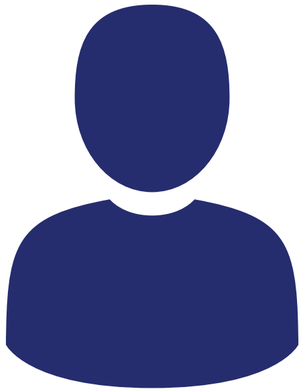
ID 28613456

STUDENT

THE ADMINISTRATION

SCIENCES SORBONNE UNIVERSITÉ

PROPOSAL FOR THE PROJECT CORE



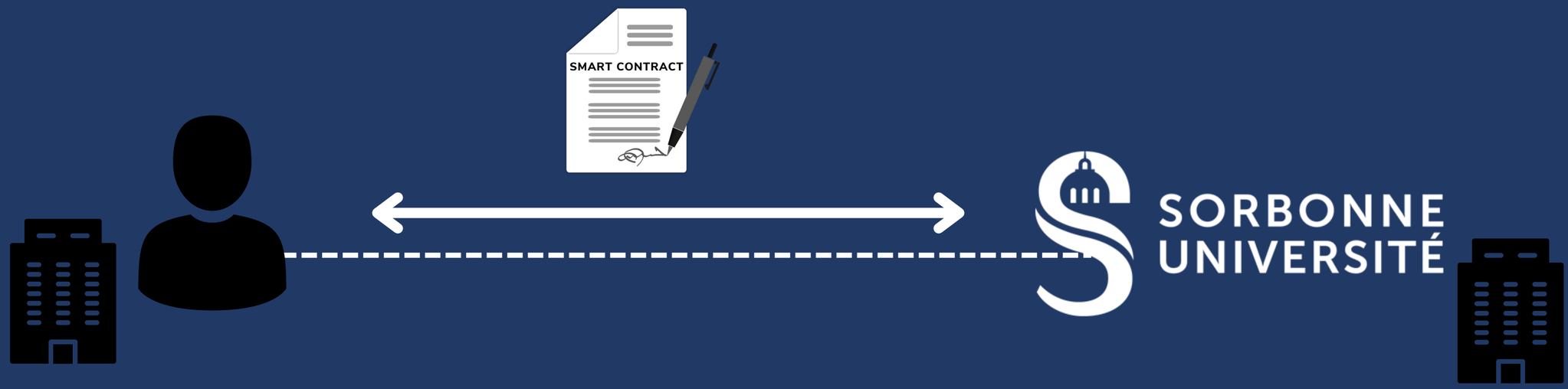
STUDENT

THE ADMINISTRATION

SCIENCES SORBONNE UNIVERSITÉ

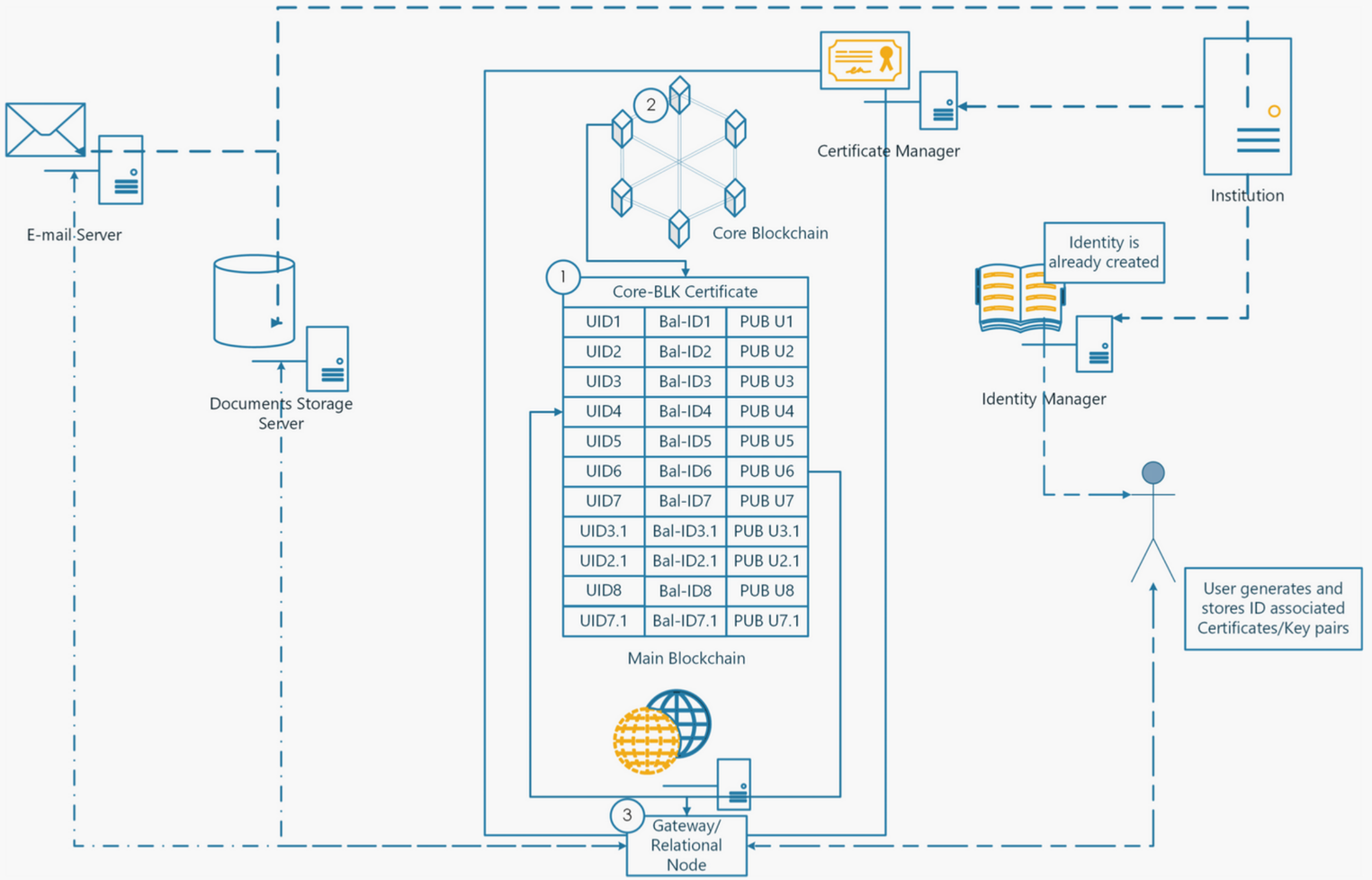
PROPOSAL FOR THE PROJECT CORE

- BLOCKCHAIN COUPLED WITH SMART CONTRACTS TECHNOLOGIES REMOVES THE RELIANCE ON CENTRAL SYSTEM BETWEEN TRANSACTING PARTIES



- UNTRUSTED PARTIES CAN COMMUNICATE DIRECTLY WITH EACH OTHER USING SMART CONTRACTS
- SMART CONTRACTS ARE STORED ON THE BLOCKCHAIN WHICH ALL PARTIES HAVE A COPY OF

SCHEMATICS OF AUTONOMOUS NETWORK PROPOSAL



STEPS TO BE TAKEN

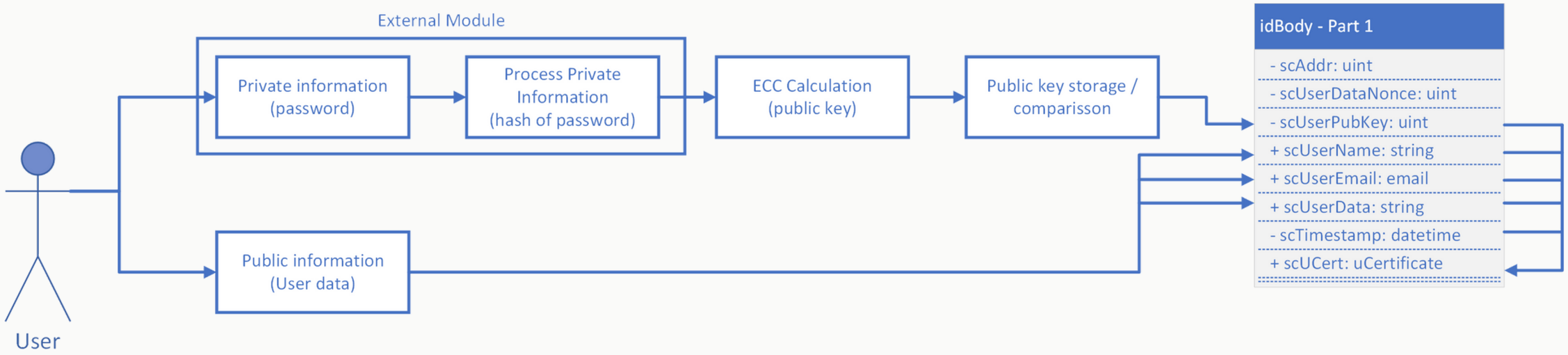
1. STORE USER INFORMATION

2. USE RSA ENCRYPTION TO GENERATE A PUBLIC AND PRIVATE KEY PAIR

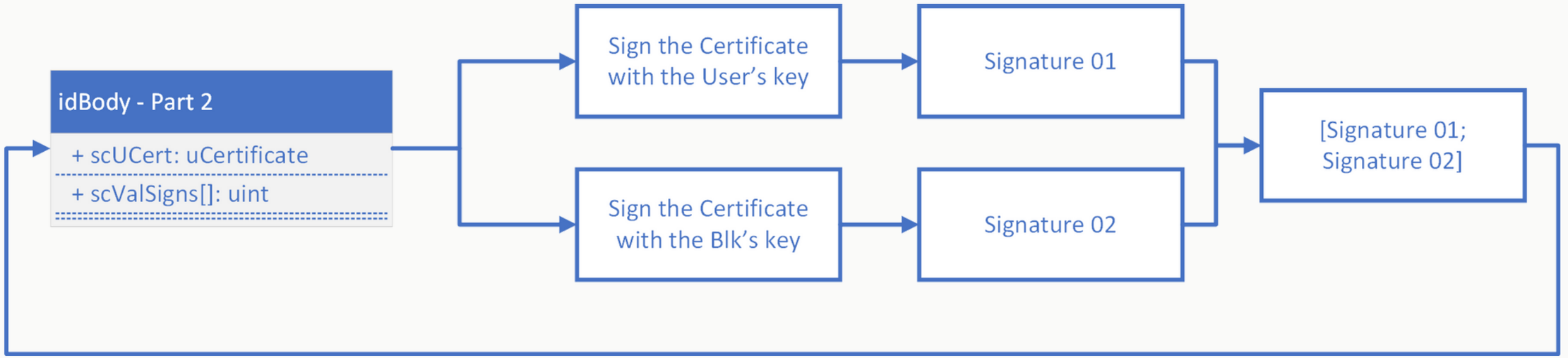
3. CREATE A DIGITAL SIGNATURE BOARD TO CERTIFY THE VALIDATION OF STORED INFORMATION

4. VERIFICATE THE VALIDITY AND EXPIRATION TIME OF STORED INFORMATION

THEORETICAL CONCEPTION



SIGNATURE VALIDATION



IDEA OF THE PROJECT

STUDENT

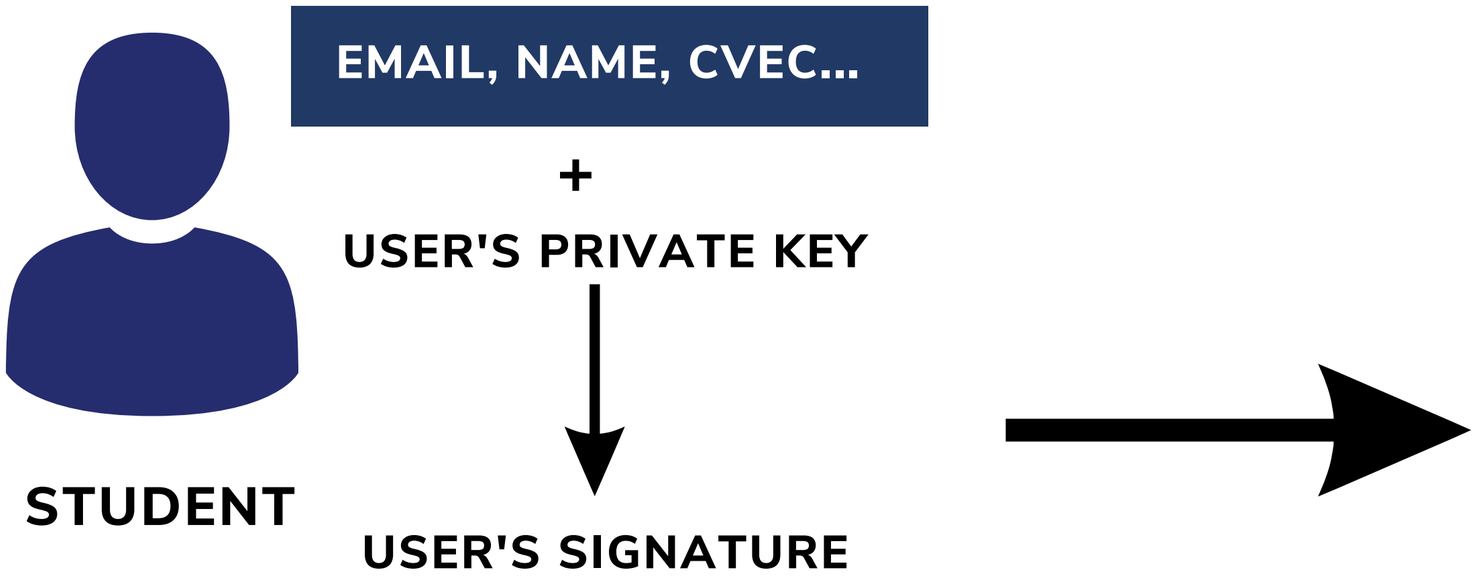
EMAIL, NAME, CVEC...

+

USER'S PRIVATE KEY

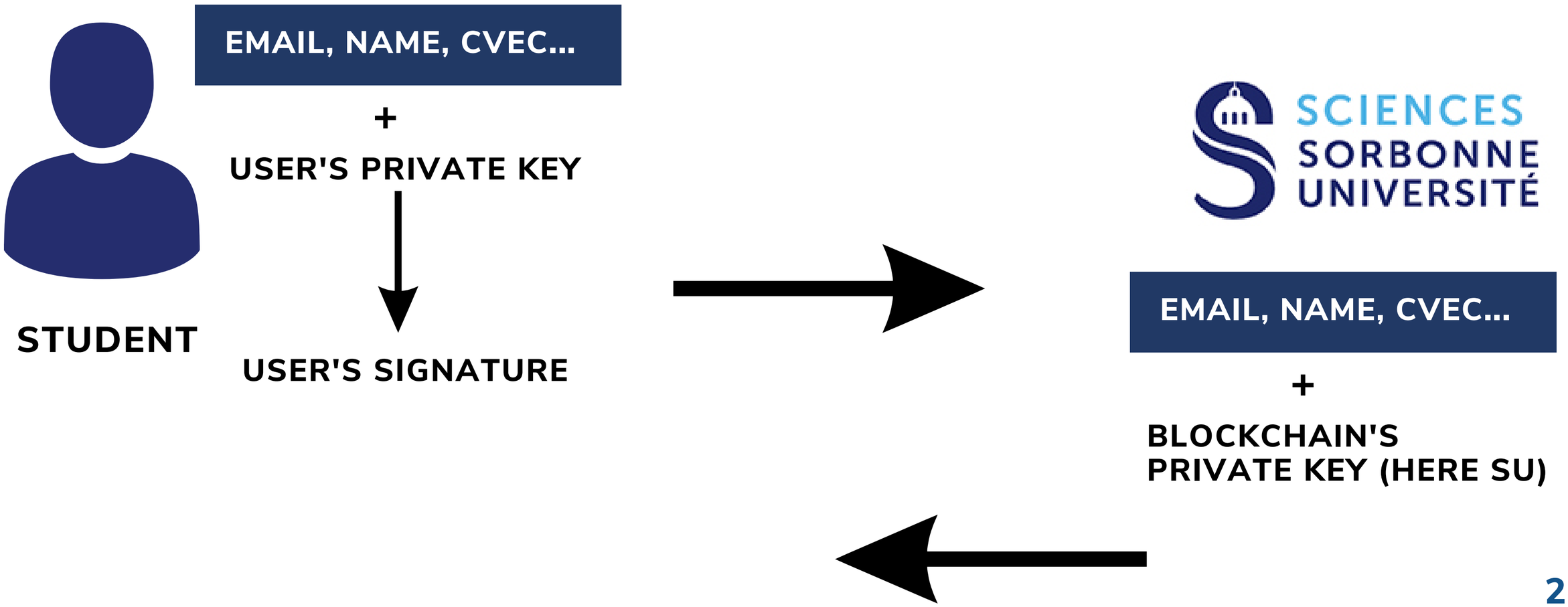
SCIENCES SORBONNE UNIVERSITÉ

IDEA OF THE PROJECT



SCIENCES SORBONNE UNIVERSITÉ

IDEA OF THE PROJECT



IDEA OF THE PROJECT

- USER GENERATE IDENTITY(STUDENT CARD) HIMSELF WITHOUT THIRD PARTY
- SMART CONTRACT IS IN RELATION WITH ALL STUDENTS AND SORBONNE UNIVERSITY

STUDENT

EMAIL, NAME, CVEC...

+

USER'S PRIVATE KEY

USER'S SIGNATURE

SCIENCES SORBONNE UNIVERSITÉ

EMAIL, NAME, CVEC...

+

BLOCKCHAIN'S PRIVATE KEY (HERE SU)

NETWORK'S SIGNATURE + ID 28613456

IMPLEMENTATION

SOLIDITY

1 Smart-Contract

- idBody.sol

2 Interfaces

- Index.js (User)
- Network.js (network)

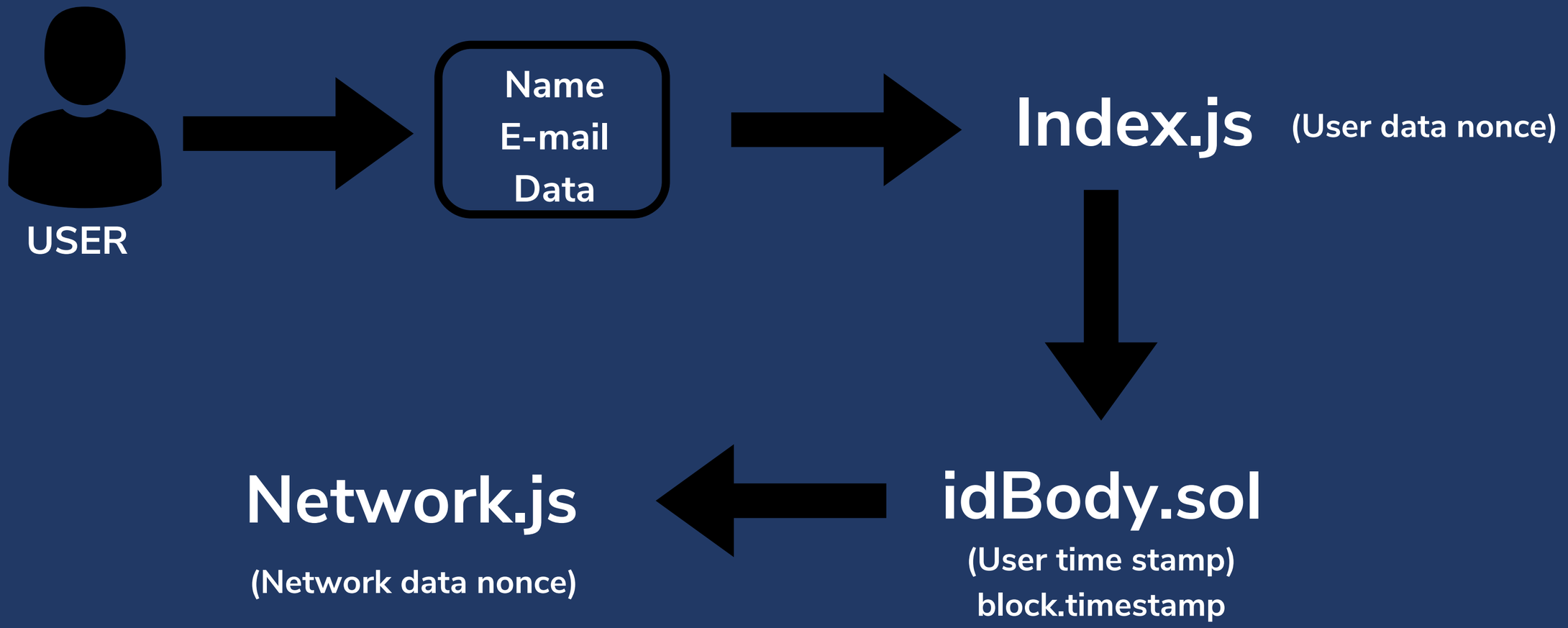
RSA ENCRYPTION

ASSYMETRIC ENCRYPTION → PAIR OF KEYS

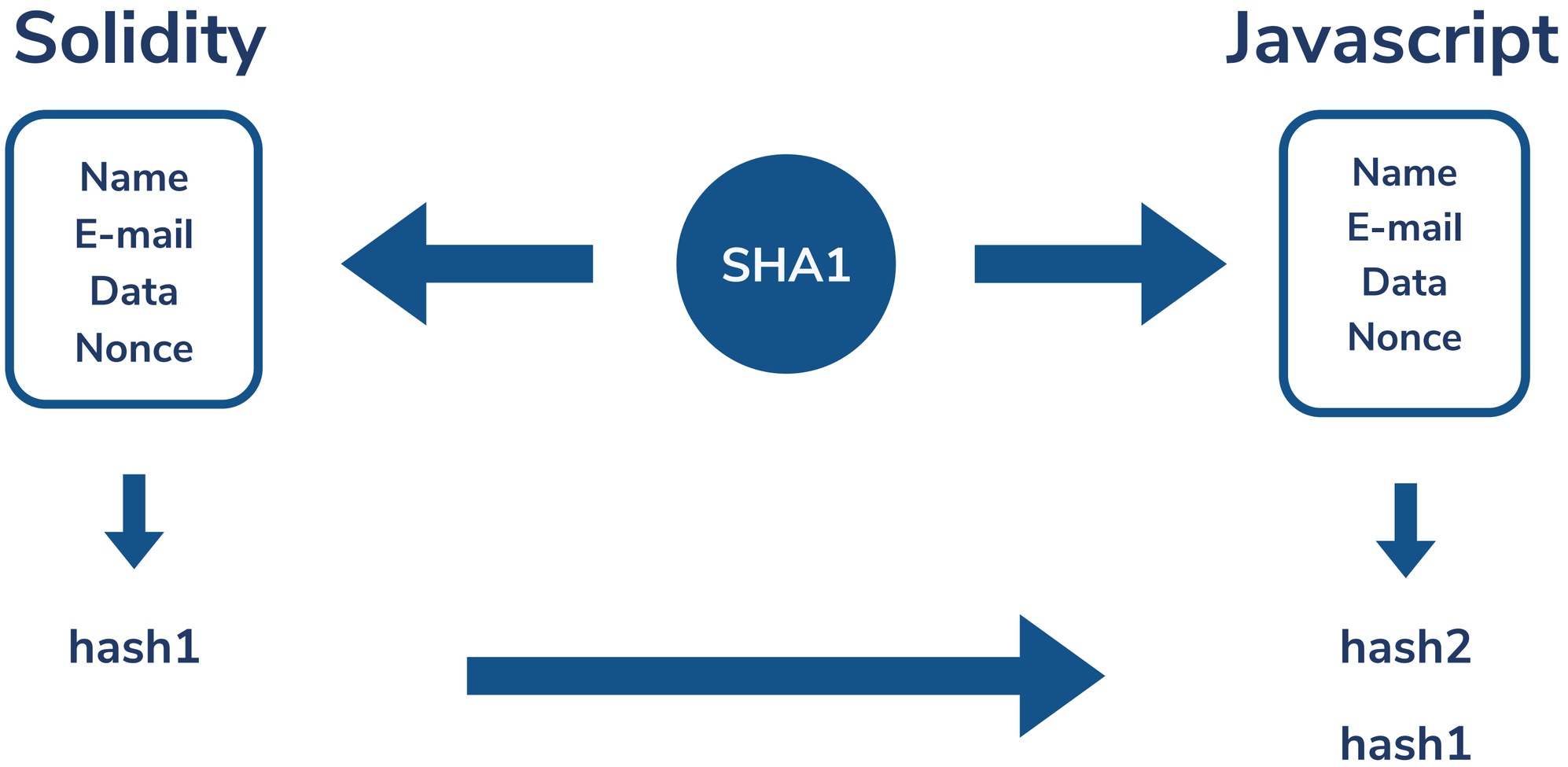
- Private key
- Decryption
- Secret

- Public key
- Encryption
- Visible to all users

SIGNATURES


USER
Name
E-mail
Data
Index.js
(User data nonce)
idBody.sol
(User time stamp)
block.timestamp
Network.js
(Network data nonce)

USER'S SIGNATURE



If hash1 == hash2

Solidity

Javascript

hash1 + user private key

web3.eth.accounts.sign(hash1, privateKey);

Signature1

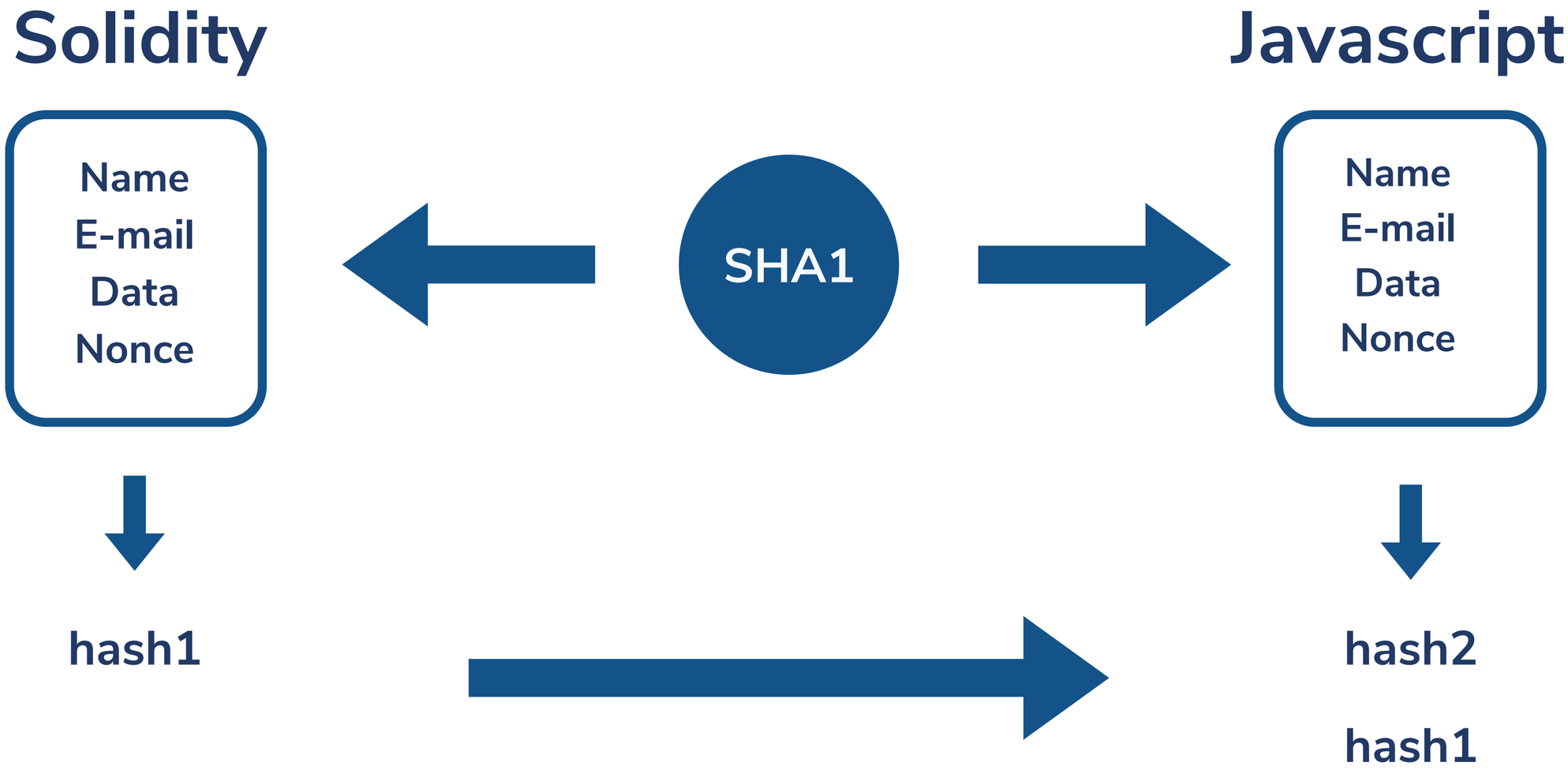
(Network time stamp)

new Date().getTime()

Store Signature1 in an array

scUserValSign[signature1]

NETWORK'S SIGNATURE



If hash1 == hash2

Solidity

Javascript

hash1 + network private key

web3.eth.accounts.sign(hash1, privateKey);

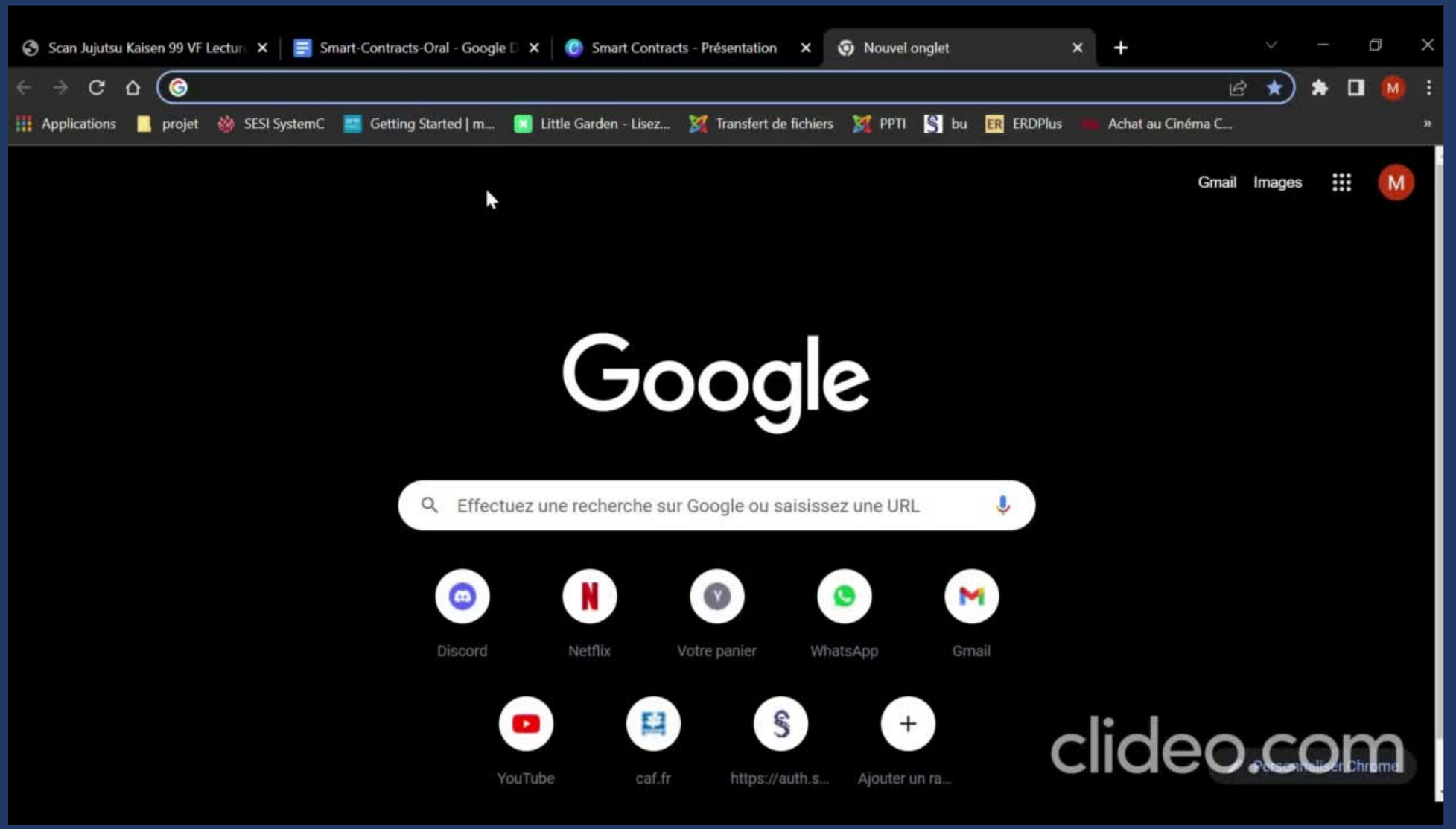
Signature2

Store Signature2 in an array
scUserValSign[signature1, signature2]

DECENTRALIZED AUTO-GENERATED CERTIFICATE

```
Validated authentication !
Display the user's certificate :
Smart Contract address : 0x8b6aa801ABA55D11053c35aF294e9E89B940964f
User public key : 448715257549991519252097319744396344793500692536102264592898537348553827543 04
User name : Tom
User E-mail : tom.olivier@gmail.com
User data : Ceci sont des données personnelles de Tom.
Network Time Stamp : 1652942038
User Time Stamp : 1652942006
Network data nounce : 20261
User data nounce : 12739708188
Network signature : 0xa1432233b30f5743b4789f3b5b8719f09ee0ccfd4bff845d798b19c880
User signature : 0xad75292458c0bf9e6523ff7cf965204a74079b82a8b882c1f581343b09
```

SIMULATION


Scan Jujutsu Kaisen 99 VF Lectur
Smart-Contracts-Oral - Google D
Smart Contracts - Présentation
Nouvel onglet
Applications
projet
SESI SystemC
Getting Started | m...
Little Garden - Lisez...
Transfert de fichiers
PPTI
bu
ERDPlus
Achat au Cinéma C...
Gmail
Images
Google
Effectuez une recherche sur Google ou saisissez une URL
Discord
Netflix
Votre panier
WhatsApp
Gmail
YouTube
caf.fr
https://auth.s...
Ajouter un ra...
clideo.com

CONCLUSION

Resultats

Qu'est-ce que ce projet nous a apporté?

Difficultés rencontrées

Ameliorations

REFERENCES

[1] Les Smarts Contract : ce qu’il faut savoir
https://arnaudtouati.com/smart-contract/
[2] Comprendre : les smart contracts (blockchain et contrats intelligents) - (itsocial.fr)
https://itsocial.fr/enjeux-it/enjeux-innovation/blockchain/comprendre-smart-contracts-blockchain-contrats-intelligents/
[3] Qu’est-ce que la blockchain ? | Ledger
https://www.ledger.com/fr/academy/quest-ce-que-la-blockchain

THANK YOU

Do you have any questions for us?