

La blockchain pour la sécurisation des communications V2C



Eliott Blondin

Tanguy Fraboni

Simon LeVen

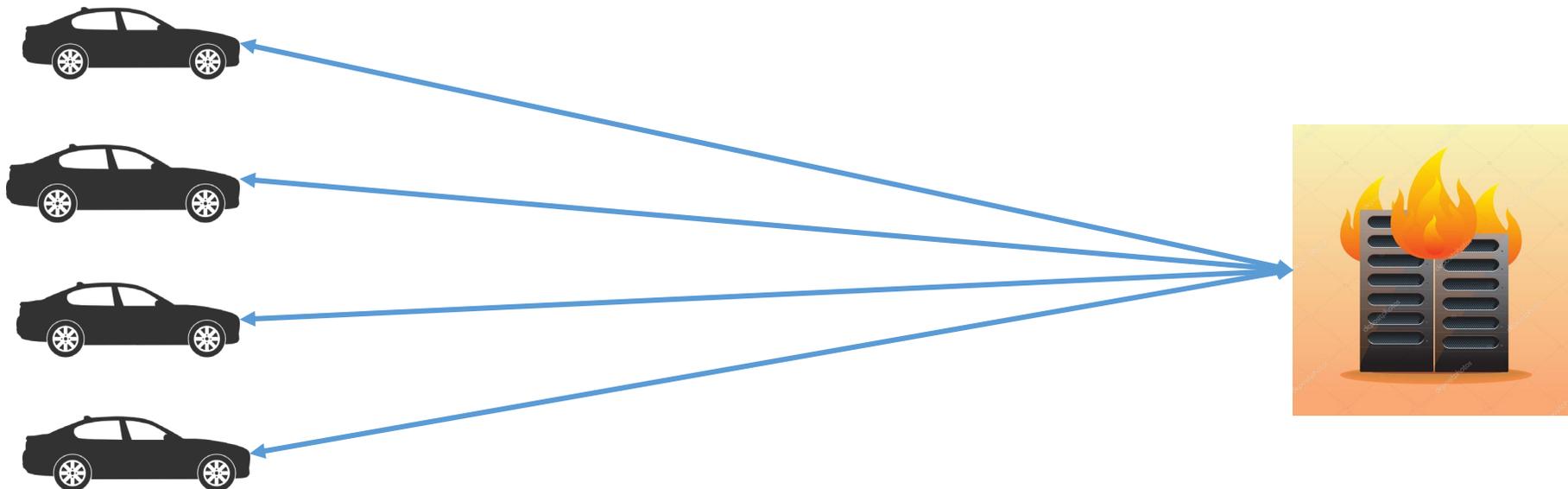
Arthur Piquée-Audrain

Grégoire Torchet-Bianchi

Mariam Traore

Problématique

- Charge envoyée au cloud pour le changement des clés

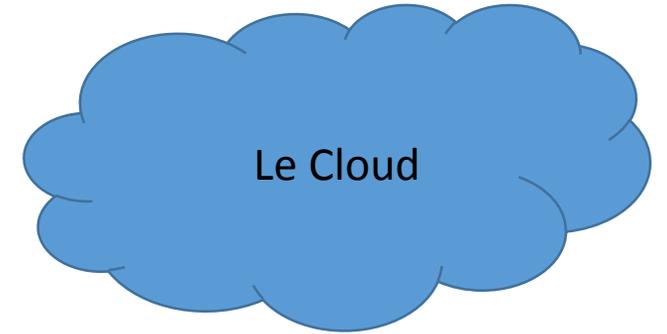


Problématique

- Connexion sécurisée pour l'échange des clés



Notre Solution :



Clé	Valeurs

Stream Client

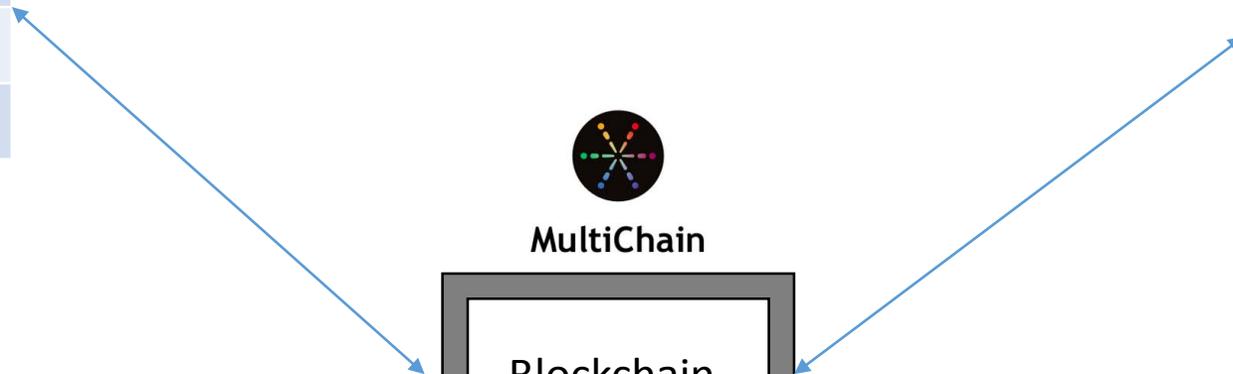


MultiChain

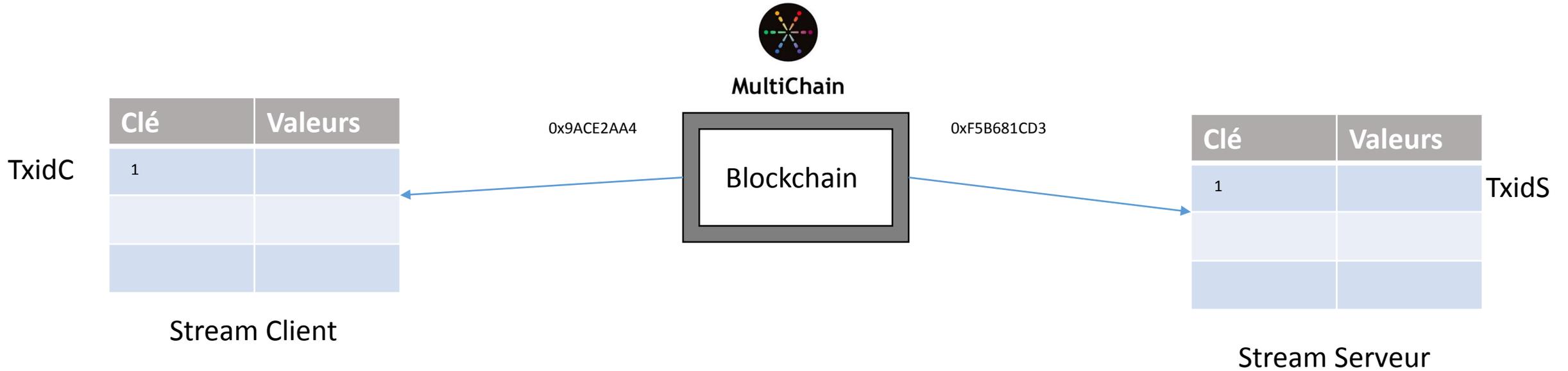


Clé	Valeurs

Stream Serveur



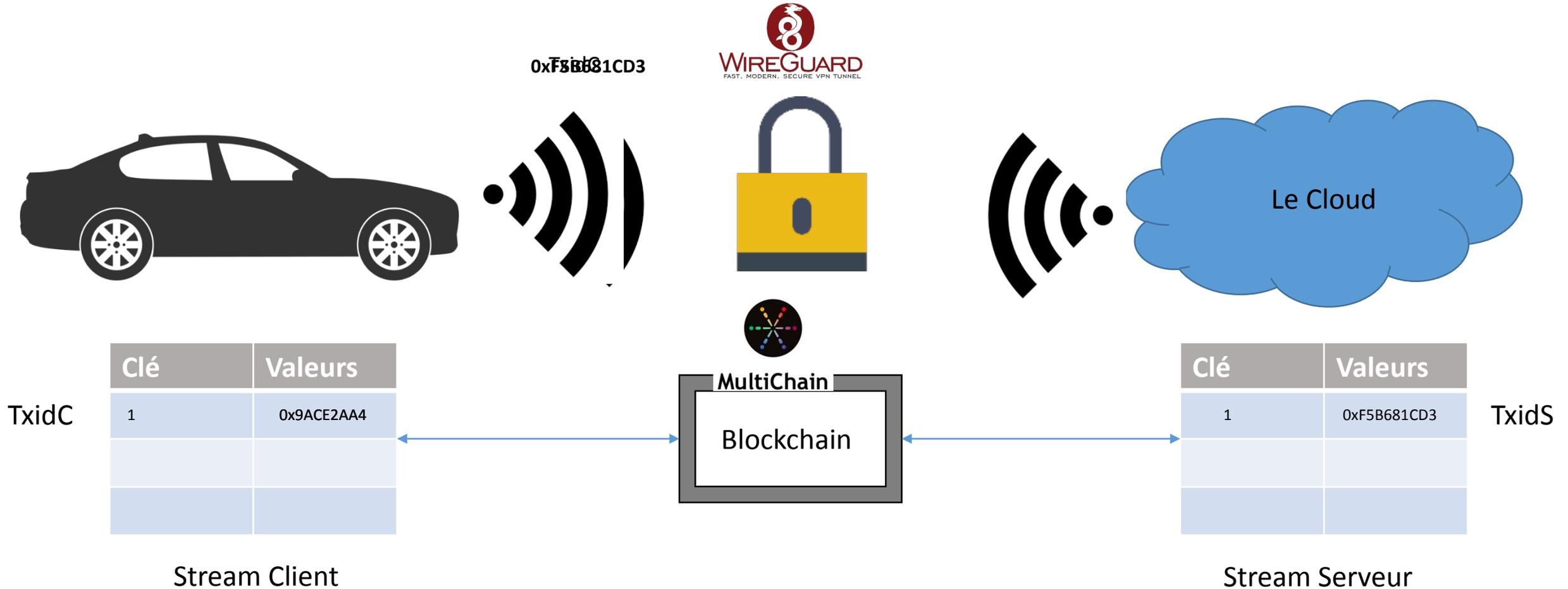
Notre Solution :



ETAPE 1 : Initialisation de la blockchain

- On génère 2 paires de clés RSA
- On écrit chaque clé publique sur la blockchain
- On peut les identifier grâce au Transaction ID généré lors de leur écriture

Notre Solution :



ETAPE 2: La Communication

- Le client chiffre son Txid avec la clé publique du serveur et l'envoi au serveur
- Le Serveur déchiffre le txid avec sa clé privée et obtient la clé publique du client
- Un Tunnel VPN peut être mis en place

The background features a repeating pattern of 3D cubes rendered in a dark blue color. The cubes are arranged in a staggered grid, with some appearing as solid outlines and others as fainter, semi-transparent versions. The overall aesthetic is clean and modern.

Merci de votre attention !