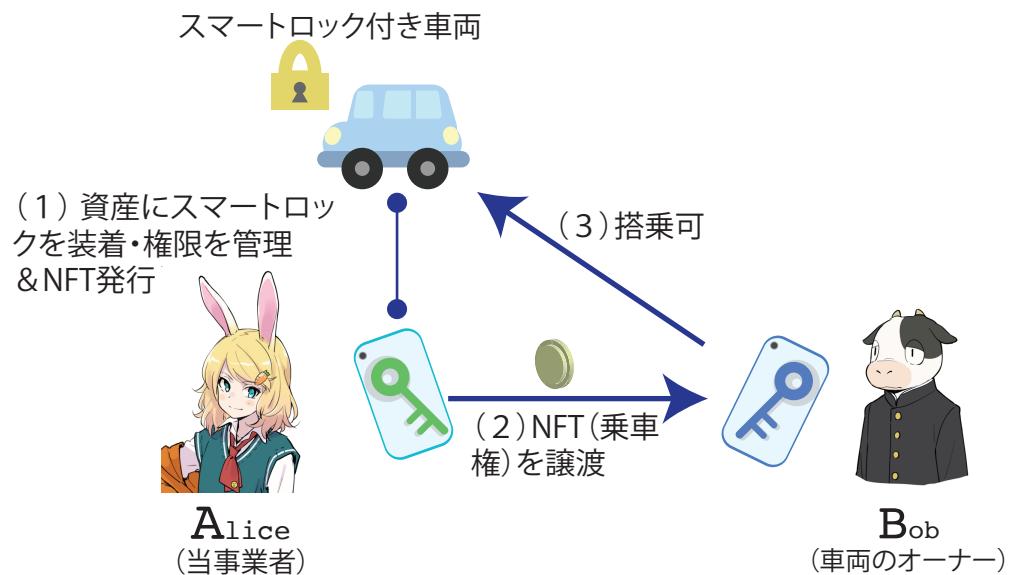
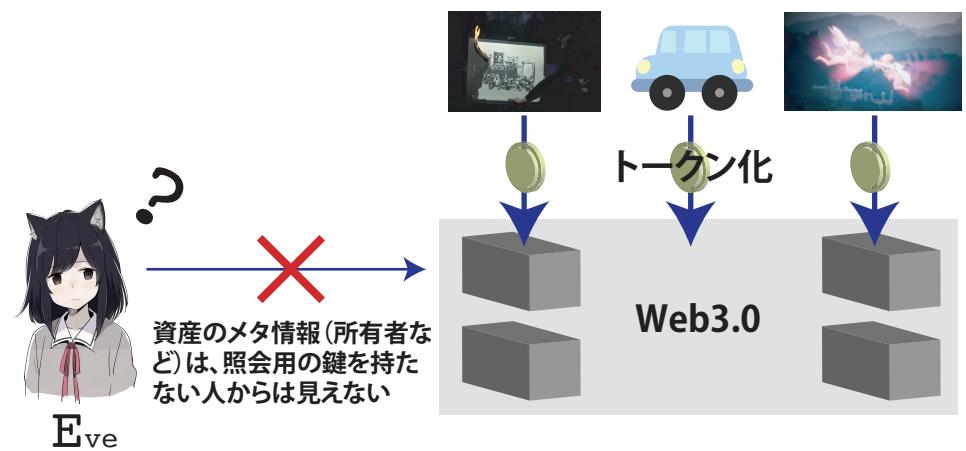


(1) バーチャルキー



(2) NFTs (Secret NFTs)



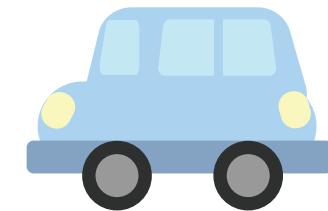
デジタルアート



絵画

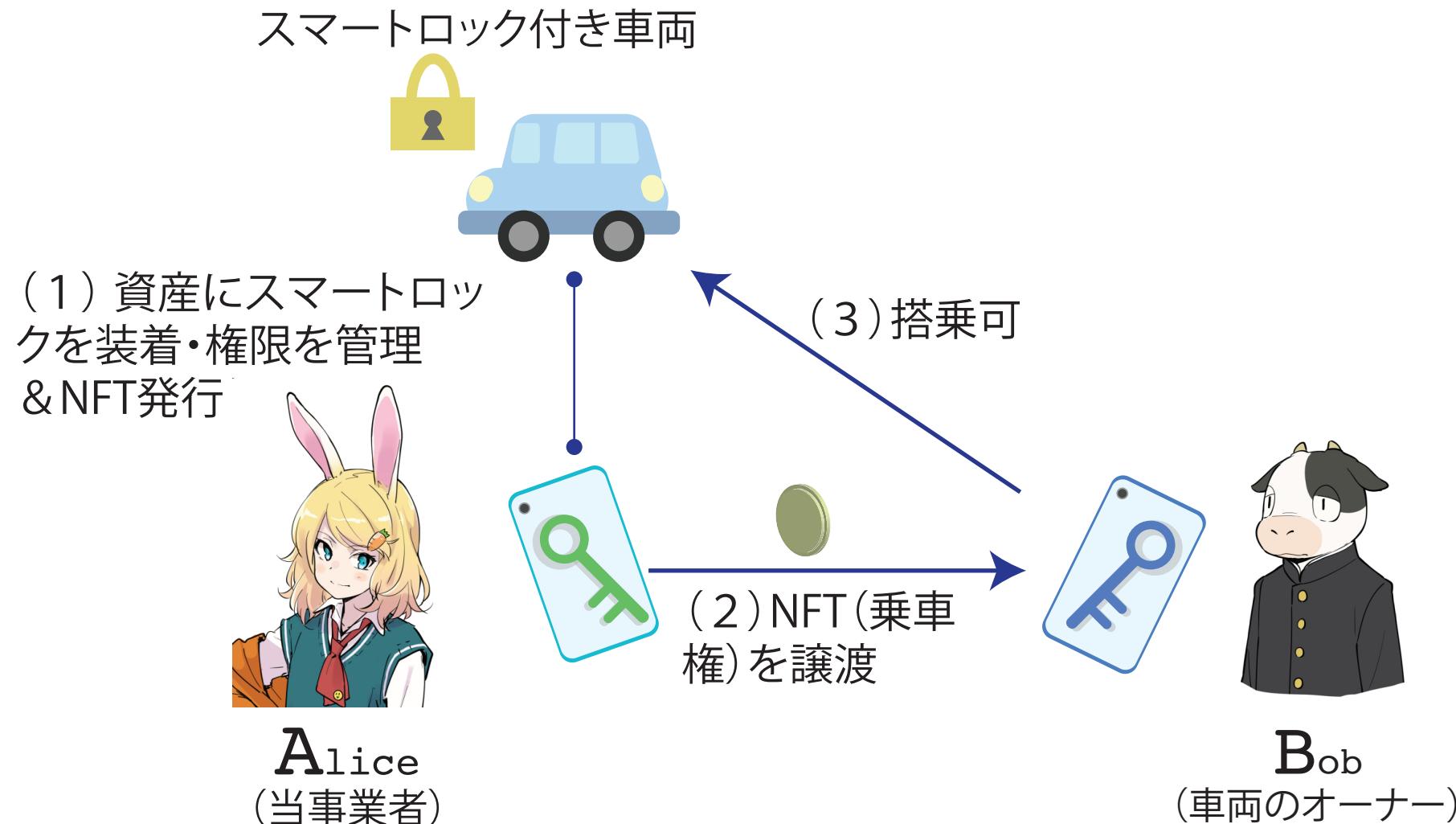


機能的資産
例:自動車

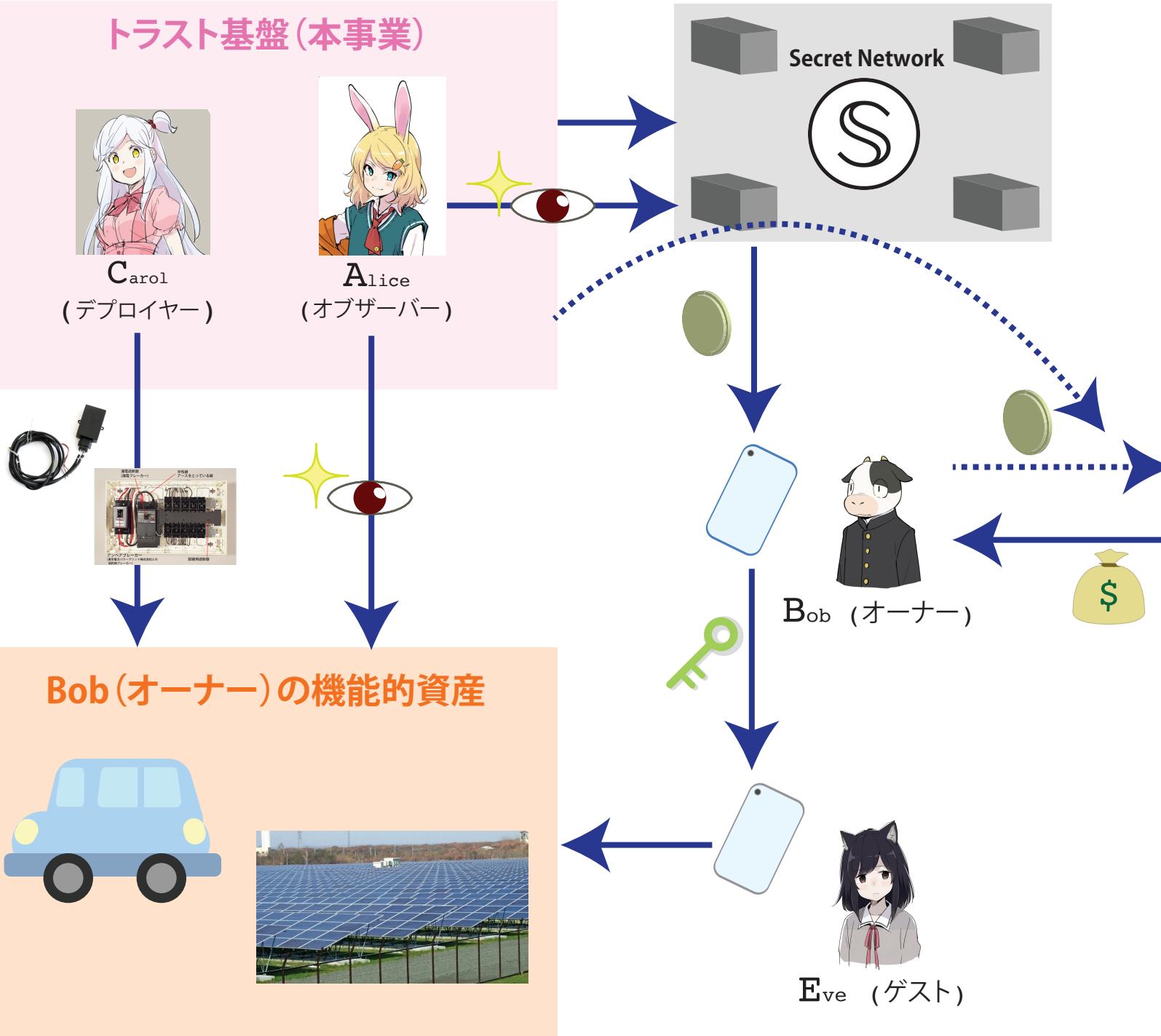


「NFTの所有権」と「乗車権」を1:1対応させて解決。

※ 例)「ウォレットの秘密鍵 = バーチャルキーの秘密鍵」として運用



トラスト基盤(本事業)



クレジット基盤

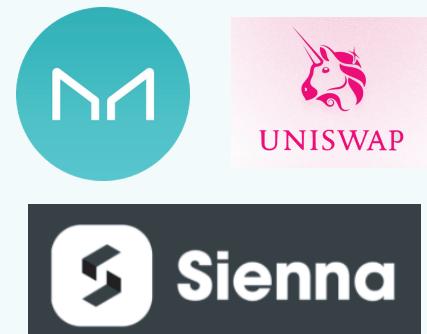
銀行A



銀行B



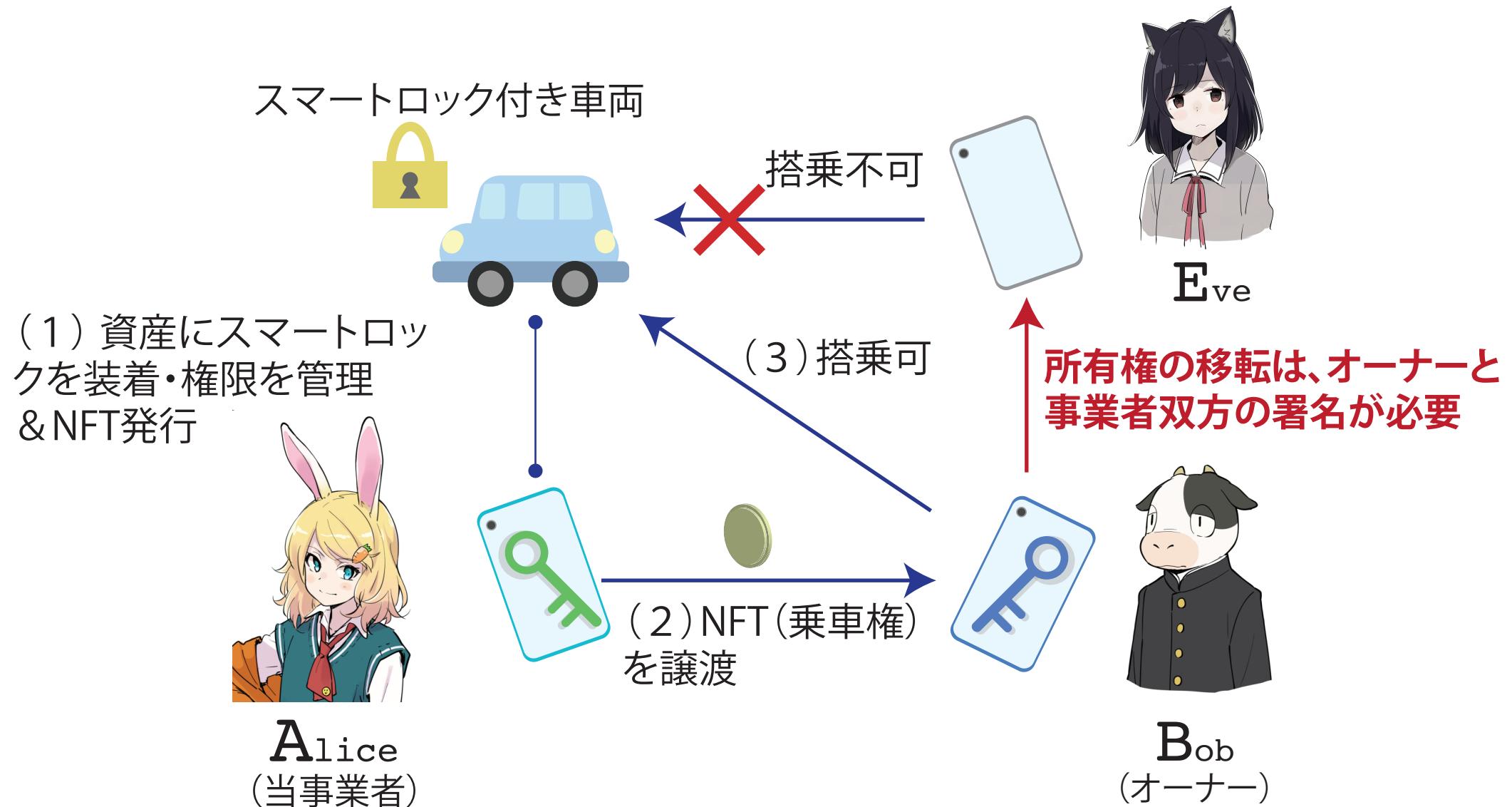
DeFi



NFTの所有権の譲渡(Transferコントラクト)は、オーナーと当事業者の双方の署名を要求する実装とする(マルチシグ)。

すなわち、**抵当権の付与された資産が、不正に移されることを防ぐことができる**。

※あるいは、NFTのメタデータとして、抵当権付与の有無を保存することでも解決可能だが、上記の方が

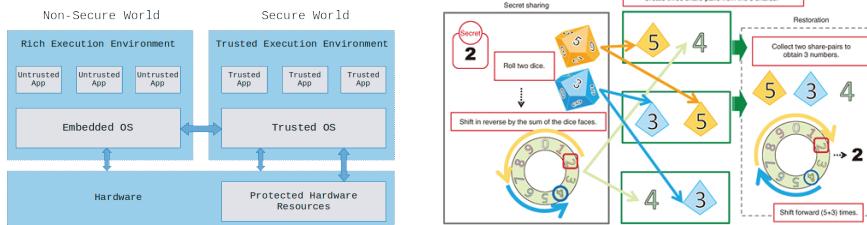


NFTの弱点は、メタデータがパブリックになってしまう点。
所有者のプライバシーを守るには、**Secret NFT**が効果的。

※Secret NFTは、秘匿計算により、メタデータを非公開にできる技術である。閲覧用の鍵を持つ者だけが、非公開情報にアクセス可能となる。SNIP721として標準化されている。

秘匿計算・秘密計算

$$\text{Dec}(\text{Enc}(a) \cdot \text{Enc}(b)) == a \cdot b$$

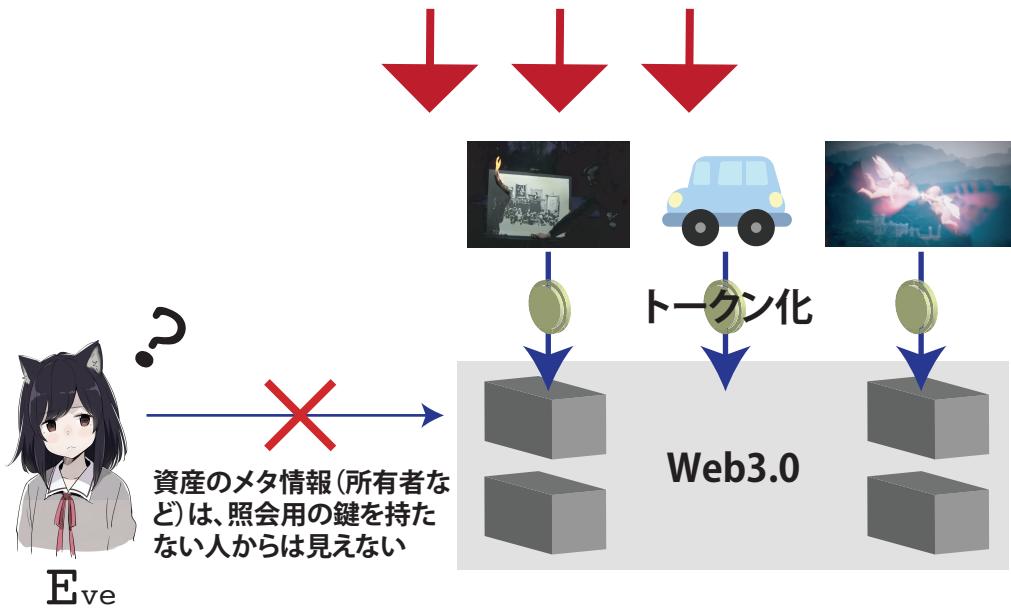


出所) <https://embeddedbits.org/introduction-to-trusted-execution-environment-tee-arm-trustzone/>
<https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201903fa3.html>

Secret NFTは、通常のNFTと異なり、
暗号化された情報がブロックチェーン
に刻まれる。これらの情報の更新は、**秘
匿計算 / 秘密計算**で行われる。

そのため、NFTに紐づく情報を閲覧
可能な人を絞り込むことが可能となる。

結果、資産所有者のプライバシーを
保護することが可能になる。



実装方式はSNIP721として標準化が行われている。
<https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-721.md>