Trong blockchain, mọi state variable đều có thể access được kể cả private vì blockchain public hoàn toàn. Vc ta dùng private chỉ là để bình thường k truy cập được chứ với những người có kiến thức họ vẫn vô như thg.

=> K lưu sensitive data trên blockchain

Cơ chế EVM lưu state variables:

EVM lưu state var dưới dạng 1 array với kích thước 2^256 phần tử, mỗi phần tử kích thước 32 bytes



VD đây là 7 slots đầu tiên. Ta xếp var vào:



Foo và bar có kích thước 32 bytes sẽ chiếm chọn slot 0 và 1

Num là uint tức uint256 tức 32 bytes(mỗi byte 8 bit lưu từ 0 đến 2^256-1) khi lưu nó sẽ chuyển sang hex và kích thước như v là nó chiếm chọn slot 2 rồi

Address chỉ chiếm có 20 bytes nên k chiếm hết slot 4. Nó xếp từ phải qua trái trong 1 slot tức là vẫn còn 12 bytes trống bên trái => EVM lưu var theo thứ tự khai báo nên nếu tiếp theo variable có kích thước vừa có thể fit vào 12 bytes còn lại

Bool chỉ có 1 byte nên chiếm vào bytes bên trái và slot 4 chỉ còn thừa 11 bytes

Do đó kể cả biến là private, nó chỉ ngăn các contract khác truy cập vào private variables trực tiếp mà thôi, chứ nếu ta cứ lấy byte của contract đọc ra ngược lại cơ chế trên thì có thể truy cập vào bất cứ state var nào ta muốn

Trong web3 có hàm getStorageAt giúp ta lấy ra giá trị tại vị trí nào