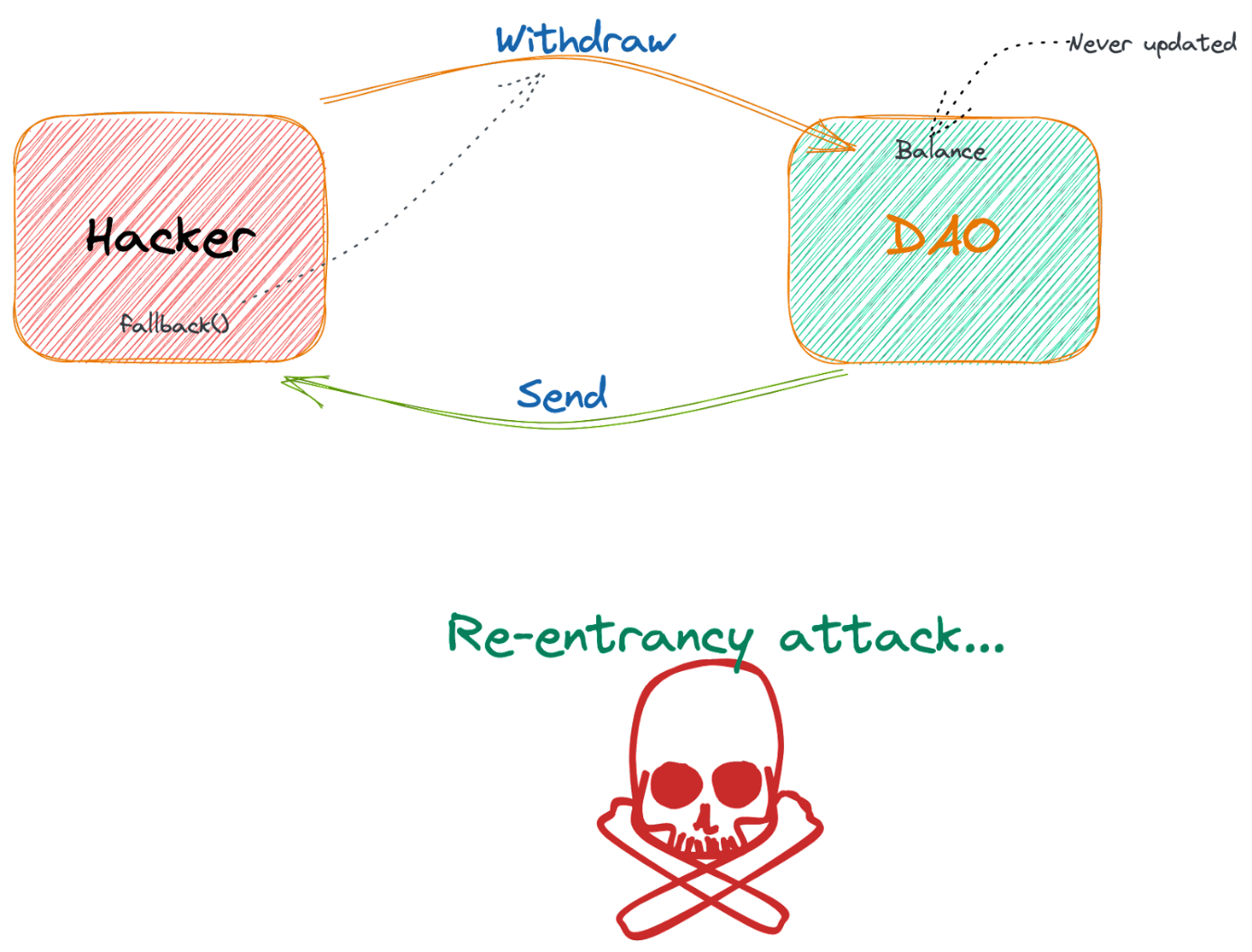
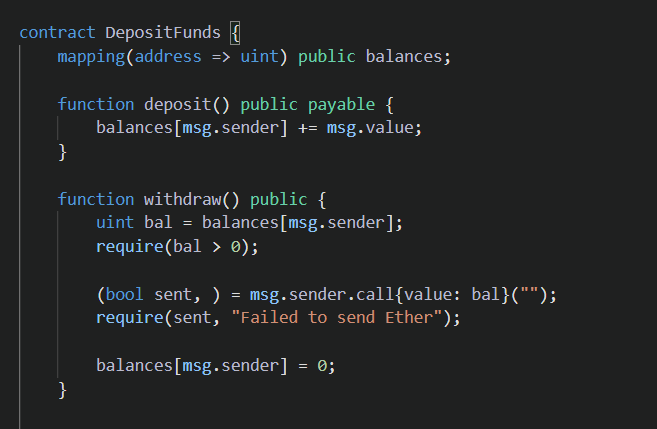
**Reentrancy Nedir?**

Reentrancy saldırısı, akıllı sözleşme güvenliği alanındaki en ünlü saldırılardan biridir. Reentrancy saldırısı, bir fonksiyon başka bir güvenilmeyen sözleşmeye harici bir çağrı yaptığında meydana gelir. ++



Ardından güvenilmeyen kontrat, fonları boşaltmak amacıyla orijinal fonksiyona özyinelemeli bir geri çağrı yapar.

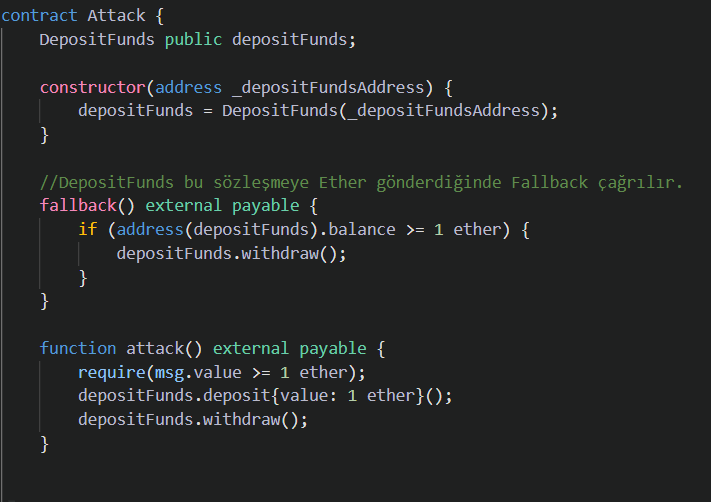
Ufak bir örnekle bunu açıklayalım:++

  
Ali aklına gelen bir proje fikri için bir akıllı sözleşme yazıyor. Bundan sonra sözleşmesine 20 Eth atarak bir hacim sağlıyor. Ali’yi sevmeyen Mehmet sözleşmeyi inceler ve zafiyeti görür. Hemen işe koyulan Mehmet para yatırma işlevini kullanarak 1 Eth depolar. ++

Mehmet kendine kötü niyetli bir sözleşme oluşturur ve Ali tarafından yazılan withdraw fonksiyonunu çağırırken kendi sözleşmesini işaret ettirir. ++

Bunun üzerine Ali’nin yazmış olduğu withdraw fonksiyonu işlemi onaylayıp onaylamayacağına karar verir. “Mehmet’İn hesabında 1 Eth mevcut mu?, evet Mehmet kendine 1 Eth atmıştı. ++

Alınan eth üzerindeki fallback işlevi, withdraw işlevini tekrar çağırıyor. Ve tekrardan Ali’nin yazmış olduğu withdraw fonksiyonu Mehmet’e para aktarır. Bu böyle devam eder. Ve mutsuz son; Ali’nin 5 kuruş parası kalmadı.++



Peki Ali bu Reentrancy saldırısı korkusundan akıllı sözleşme geliştiremeyecek mi? Tabii ki de hayır. Şimdi zamanı geri alalım ve Ali’nin sözleşme yazdığı ana dönelim:

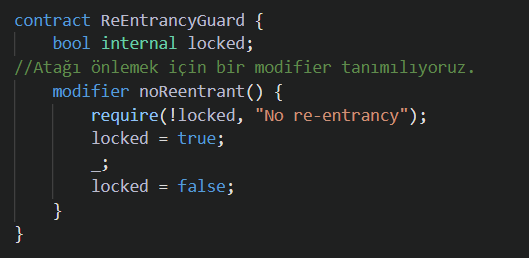
Ali sözleşmesinin üzerine bu modifieri tanımlarsa saldırıdan kurtulur. Kodu biraz açıklamak gerekirse: ++

1-Bool bir öngörücü değer tanımlayalım,

2-Modifier tanımlayalım,

3-Modifier üzerinde require yapısı kullanarak öngörücüyü kontrol edelim,

4-Require sonrası öngörücüyü true atayarak işlemlerin devam etmesine izin verelim.



Kaynaklar:  
https://www.securing.pl/pl/author/pawelkurylowicz/  
https://arxiv.org/pdf/2105.02881.pdf?ref=hackernoon.com