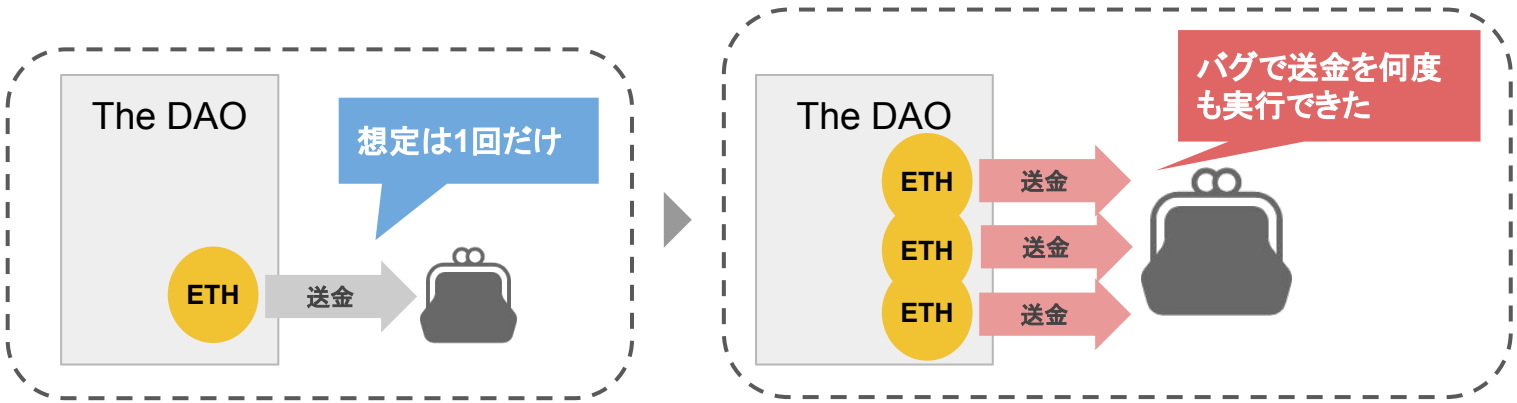
スマートコントラクトを使用した
事故事例集

フレセッツ株式会社

①The DAO事件

スマートコントラクトの脆弱性による約 360万ETH（当時約52億円）の盗難

2016年ファンドをスマートコントラクトによって実現した”The DAO”
DAOには運営に賛同しない場合、預けていた資金を切り離せる”Split”機能がある
ファンドでの報酬送金を何回も実行できるバグがあり、ハッカーが資金を盗みだすことに成功



盗難を無効化するハードフォークが実施され、
元のチェーンはEthereum Classicとして残った

▼参考リンク
https://gentosha-go.com/articles/-/17332

②Parityマルチシグウォレットでeth凍結

マルチシグウォレットの脆弱性で約 60万ETH(当時約150億円)が凍結

2017年11月、Ethereumのウォレット「Parity」にて
“Kill”コマンドでウォレットを破壊できるバグ

Parityマルチシグウォレットは587個あり、全てが凍結されて復旧できない状態に

この事故を無かったことにするハードフォークを
実施すべきかの議論が巻き起こったが行われず

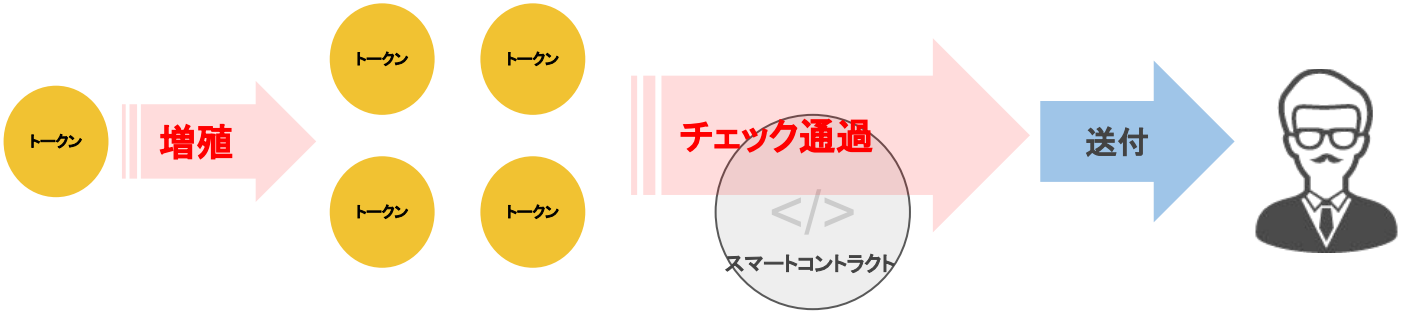
▼参考リンク

https://japan.zdnet.com/article/35110116/
https://coinpost.jp/?p=8479

③ERC20準拠トークン BatchOverflowのバグ

2018年4月、暗号資産取引業者での一部 ERC20トークン取引停止

スマートコントラクトの“BatchOverFlow”関数のバグにより
オーバーフロー(桁溢れ)によって想定していない巨額のERC20の送付が可能に

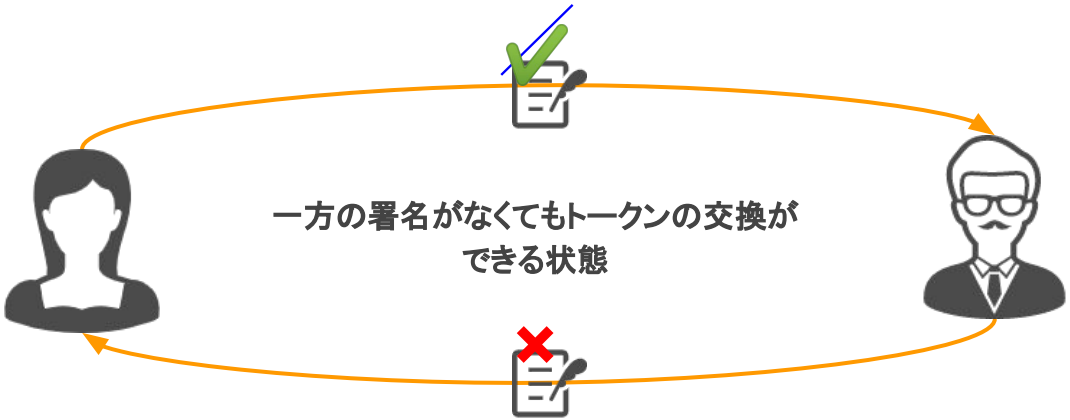


▼参考リンク
https://blockchain.gunosy.io/entry/erc20-token-Vulnerability

④分散型取引所「AirSwap」で脆弱性発見

2019年9月、スマートコントラクトの脆弱性により資金損失のリスクが発生

MakerとTakerをP2Pで直接取引させる分散型取引所のAirSwapでスマートコントラクトの脆弱性が発見された。
24時間以内にコントラクトは修復されたものの、一部のアドレスはその後も資金損失のリスクに晒された。



▼参考リンク

https://jp.cointelegraph.com/news/developers-of-ethereum-dex-protocol-airswap-disclose-critical-exploit
https://medium.com/fluidity/critical-vulnerability-in-a-new-airswap-smart-contract-c1204e04d7d3