Consequências de contratos inteligentes mal escritos

PUC Minas

Aplicações Descentralizadas e Blockchain

Prof. Carlos Leonardo dos S. Mendes

Ethereum DAO Attack

A história de como uma falha em um smart contract gerou uma grande discordânica na comunidade Ethereum e a divisão em duas redes Ethereum.

Ethereum DAO Attack

DAO = Descentralized Autonomous Organization (Organização Autônoma Descentralizada)

- As regras que definem como a organização funciona são escritas e executadas em contratos inteligentes em uma rede de blockchain.
- Existe um período inicial de financiamento coletivo (*crowdfunding*), onde pessoas podem adicionar dinheiro para a organização comprando *tokens* que representam a sua "parte" na organização. Isto é chamado de ICO (*Initial Coin Offering*).
- Quando o período inicial de financiamento termina, a organização começa a operar. Pessoas podem realizar propostas de como gastar o dinheiro da organização e os financiadores votam nas propostas.

The DAO

- “The DAO” era o nome de um DAO específico, criado e programado por um time da Slock.it.
- A Slock.it era uma compania cujo propósito era construir “travas inteligentes” para permitir às pessoas compartilhar suas coisas (carros, apartamentos, etc.), algo como um AirBNB descentralizado.
- Foi lançado em 30/04/2016 com um período de 28 dias de financiamento inicial (ICO).
- Por alguma razão inexplicada, o DAO foi extremamente popular, atingindo em 11/05/2016 $100mi e mais de $150mi no total (mais de 11.000 financiadores).

O ataque

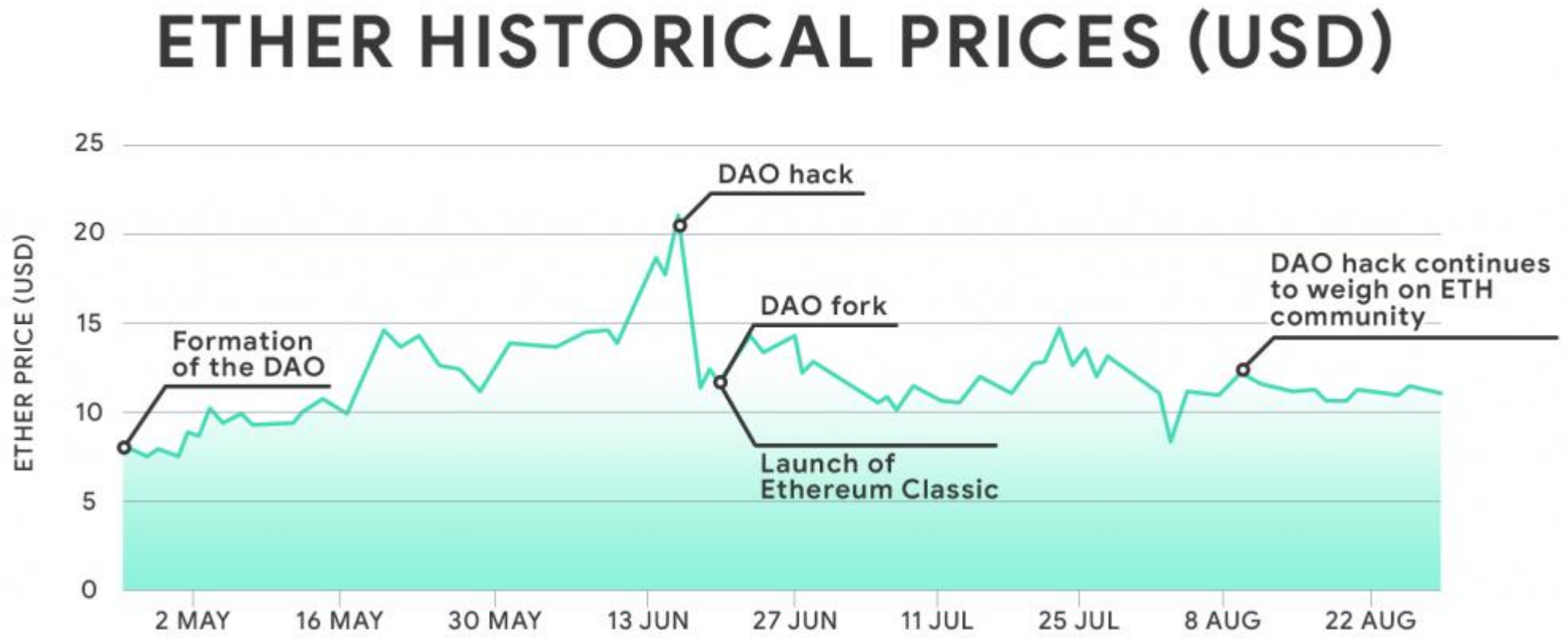
Em 18/06/2016, um ataque começou a drenar 3,6 milhões de Ether para um “DAO filho” que tinha a mesma estrutura do “The DAO”.

Como os projetistas do DAO não esperavam tanto financiamento, todos os recursos estavam em um único endereço (má ideia).

Muitos financiadores tentaram provocar uma divisão dos recursos em outras carteiras, mas não obtiveram votos suficientes no curto período de tempo.

O ataque foi cessado voluntariamente pelo responsável.

Ether após o ataque DAO



PUC Minas

O tamanho do problema...

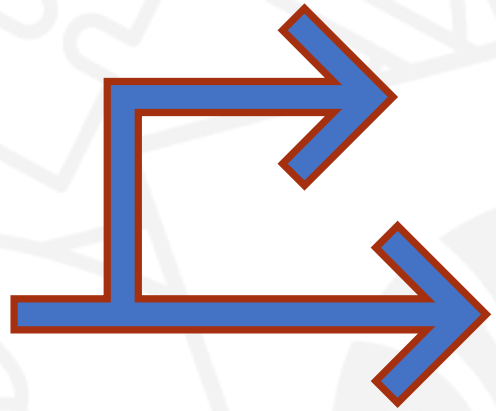
- O DAO da Slock.it continha naquele momento aproximadamente 15% de todo o Ether da plataforma Ethereum.
- Dezenas de startups estavam lançando seus projetos como DAOs na plataforma.
- Embora haja um vácuo normativo para investimentos em criptomoedas, processos judiciais poderiam responsabilizar os criadores da Ethereum e do The DAO (Slock.it).
- O Ether e todos os tokens usados em financiamento coletivo poderiam virar “fumaça”
- Todo o ecossistema Ethereum poderia ruir...

Como a Ethereum se envolveu e propôs resolver o problema...

*"Um **soft fork** foi proposto que tornará inválida qualquer transação que faça invocações que reduzam o balanço da conta 0x7278d050619a624f84f51987149ddb439cdaadfba5966f7cfae a7ad44340a4ba (The DAO e filhos)."*

"Mineradores devem esperar pelo soft fork, realizar o download e executá-lo se estiverem de acordo. Proprietários de tokens DAO e usuários da Ethereum devem ficar firmes e manter a calma."

Vitalik Buterin



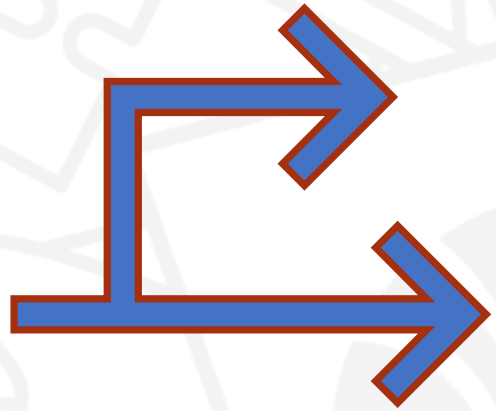
- Em resumo, uma condição foi colocada no código da Ethereum para impedir o hacker de resgatar "seu prêmio".

Como a Ethereum se envolveu e propôs resolver o problema...

*"... O consenso foi que um soft fork deva ser publicado em no máximo 27 dias, o hacker não será capaz de retirar os recursos que ele colocou em um DAO filho. Um subsequente **hard fork** poderia retornar todo o ether, incluindo os recursos roubados, para um smart contract. O smart contract poderia conter uma única operação: withdraw()."*

Stephan Tual

- Em resumo, os blocos onde o contrato The DAO foi escrito e a transação do hacker ocorreu, seriam sobrescritos.



Soft fork X Hard fork

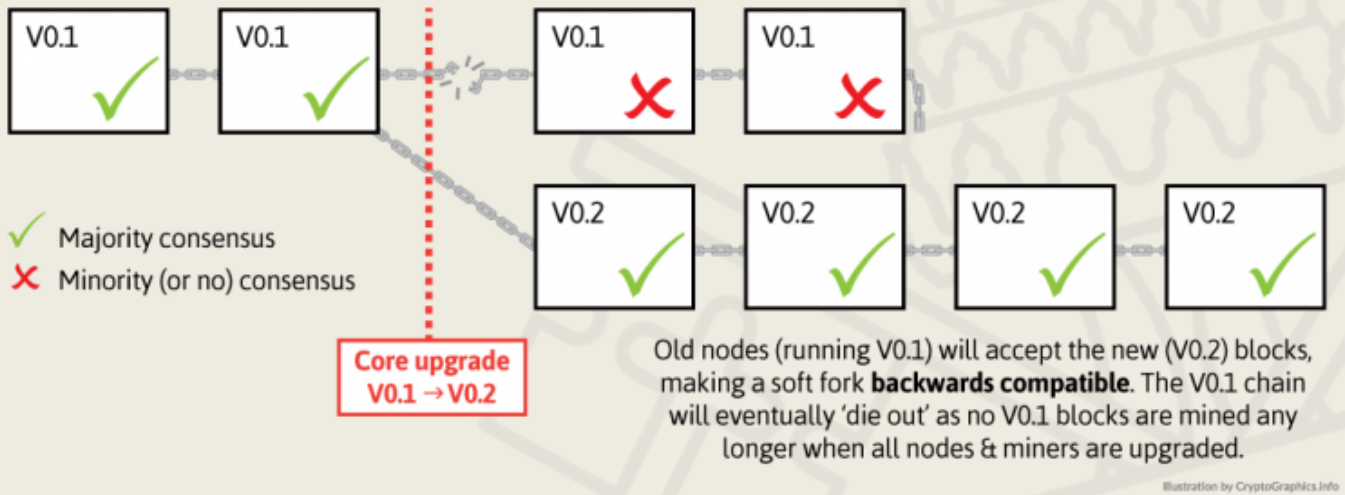
Soft fork

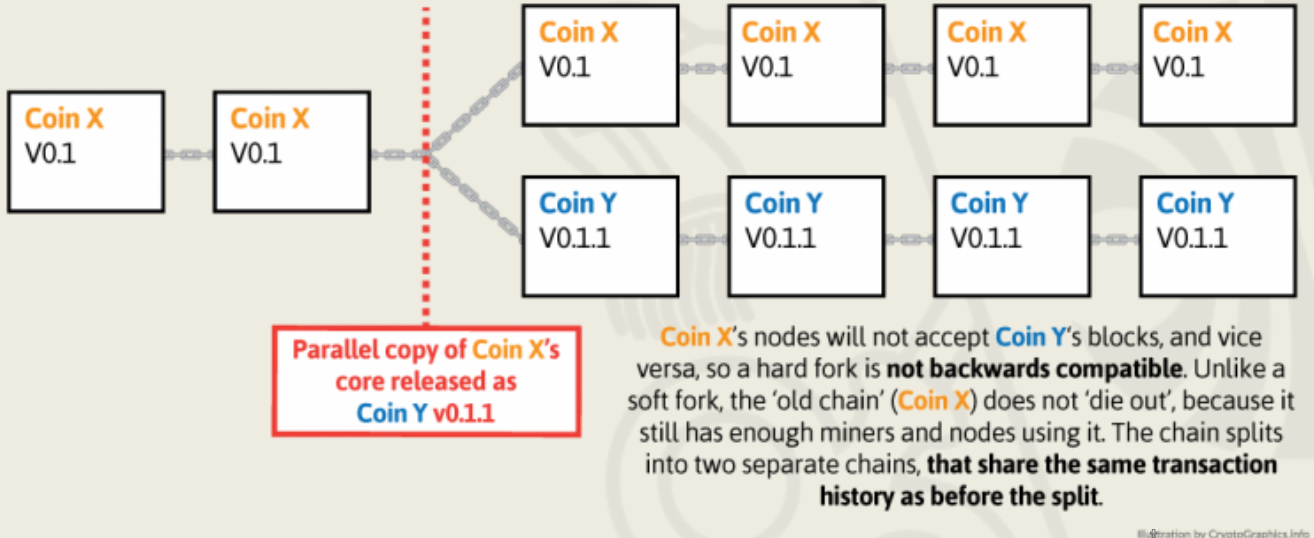
- É um evento comum e ocorre em atualização de versão da especificação da plataforma.
- Apenas durante o período de atualização, haverá coexistência entre nós na versão antiga e na nova.
- É retro-compatível, ou seja, nodos na versão antiga são capazes de processar blocos na nova versão.

Hard fork

- Não é um evento comum e normalmente ocorre quando há diferença de opinião na comunidade.
- Irá dividir a cadeia em duas cadeias separadas, com uma história comum até o fork.
- Não é retro-compatível.

Soft fork
X
Hard fork





PUC Minas

Como o hacker reagiu...

- Em carta aberta à comunidade Ethereum o hacker publicou:

"Eu examinei cuidadosamente o código do "The DAO" e decidi participar após encontrar o recurso do contrato que permitia ser recompensado com ether. Eu fiz uso desse recurso e obtive de maneira correta 3.641.694 ether (...). O meu entendimento é que o contrato do DAO possuia esse recurso para promover a descentralização e encorajar a criação de DAOs filhos."

- À proposta de fork da Ethereum:

"Em breve teremos um contrato inteligente para recompensar os mineradores que se opuserem ao soft-fork e mineirarem a transação. 1 milhão de ether + 100 btc serão distribuídos aos mineradores.

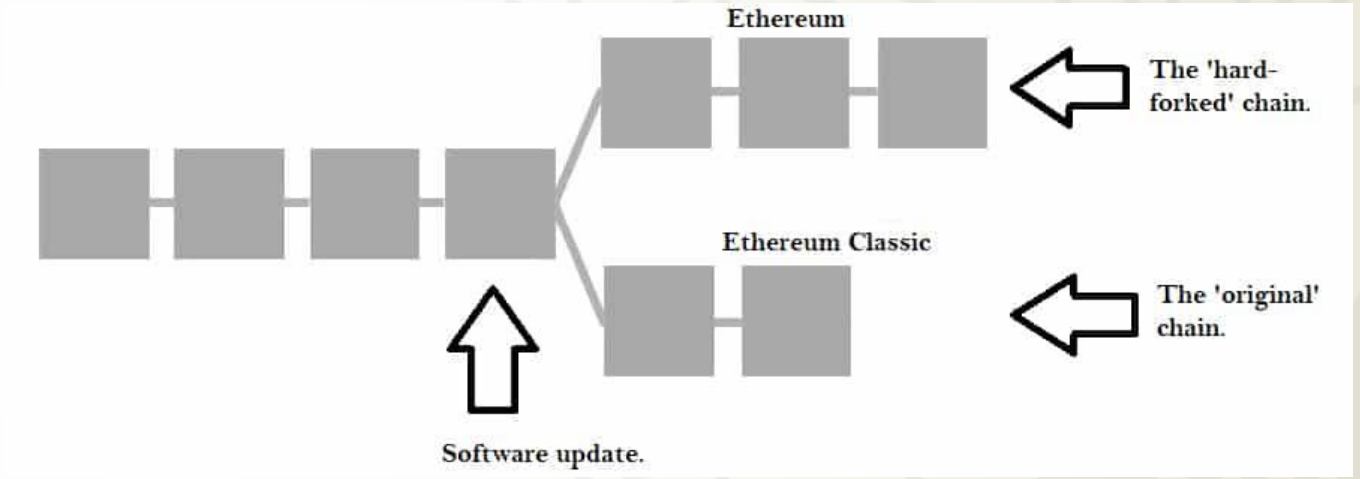
Como parte da comunidade reagiu...

"Eu criei um contrato com um bug no ínicio da Ethereum e perdi 2k ETH. Também posso ter meus ETHs de volta? Obrigado."

"A Ethereum funcionou exatamente como esperado. Eu não acredito que um software deva ser atualizado quando ele faz exatamente o que se espera."

"Você assume os riscos de seu investimento. Se você não entende seu investimento, assume riscos desconhecidos. Qualquer coisa diferente disso é um resgate por uma autoridade central, ou seja, a antítese do mundo blockchain."

Como a história terminou...



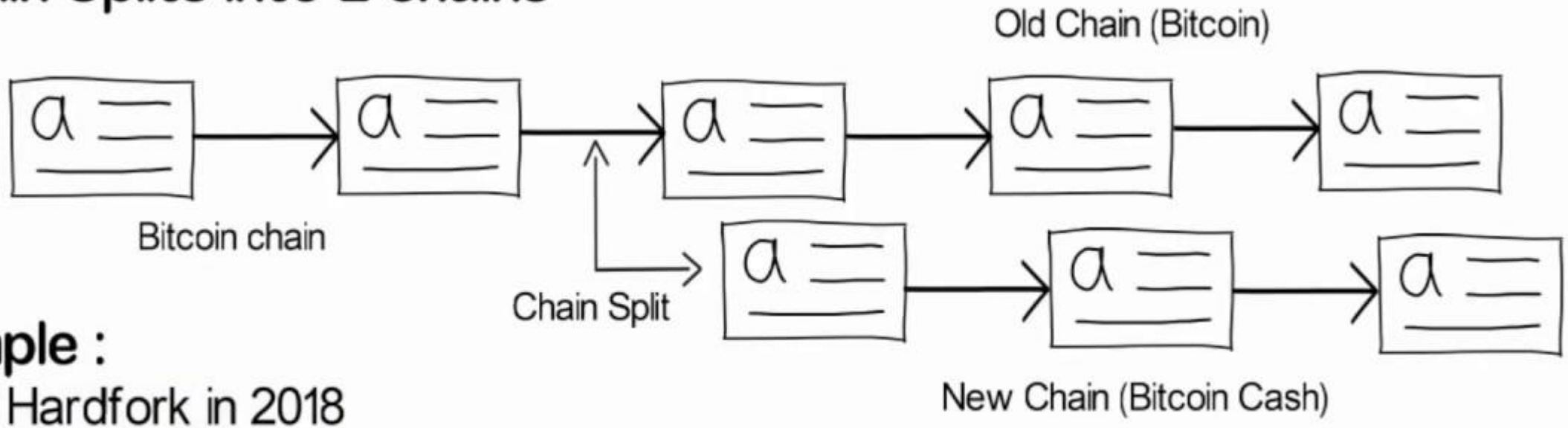
3.641.694 ETC x US$ 6 ~ US$ 21mi

Setembro 2020

PUC Minas

Hard Fork

1. Backward Incompatible
2. Chain Splits into 2 chains



Example :

Bitcoin Hardfork in 2018

New Coin : Bit

O Bitcoin também teve seu hard fork...

Melhores práticas para escrita de smart contracts

OpenZeppelin

- Fundada em 2015, a OpenZeppelin é uma empresa especializada na auditoria de segurança de sistemas distribuídos.
- A OpenZeppelin oferece um ***framework open source*** para o desenvolvimento de **contratos inteligentes seguros**.
- Baseado nas **melhores práticas** de escrita de *smart contracts* e em vários **anti-padrões já observados**, a OpenZeppelin fornece **padrões abertos** para a **escrita segura de contratos inteligentes**.
- Por exemplo, a OpenZeppelin fornece uma biblioteca de padrões para escrita de tokens ERC20, ERC721, ERC777 e ERC1155.
- A **biblioteca de padrões para contratos** pode ser consultada em https://docs.openzeppelin.com/contracts/4.x/

PUC Minas