
<ブロックチェーン・スマートコントラクト>

質問
ブロックチェーンでの取引の修正は非常に困難だと言われてましたが，実際の取引中でのミスを避ける方法はあるんでしょうか？

回答
取引中でのミスという点では，呼び出すコントラクトのバイトコードがブロックチェーン上に公開されているため，使用前にそのコードに対して脆弱性の有無を確認する，といった対策が考えられます．

質問
smart contractにおいて，現状最も大きな課題は何になっているのでしょうか．

回答
課題点は大きく2つあります．1つ目はスマートコントラクト自体のセキュリティの問題点です．発表でも述べたように，コードに脆弱性があった場合，攻撃に利用されて不正送金が行われてしまうという点．2つ目はプライバシーに関する問題点です．スマートコントラクトの内容は公開されるため，医療データなどセンシティブなデータを扱うシステムへの応用が課題点として考えられます．

質問
盗られた通貨はどのようにして換金されてるのか，それとも換金されないのか．

回答
基本的には換金されませんが，盗まれた通貨の流れから攻撃者を特定することで返却されることはあります．
また，送金関数が削除されるなどして通貨が凍結してしまった場合など換金できない場合があります．

ただし，紹介したTheDAOのように，莫大な被害が発生した事件においては，状態を元に戻すといった対処がとられた例も存在します．

<脆弱性>

質問
聞き手側にも問題があったかもしれませんが， ブロックチェーンにはなくてEthereum Smart Contractにある特徴がいまいち伝わりにくかった印象でした．
Ethereum Smart Contractのみにある脆弱性や利点等ありましたらお伝えいただけるとありがたいです．

回答
まずスマートコントラクトとは，ブロックチェーン上で動作するプログラムのプラットフォームのことなので，関係はあるものの異なった概念です．
スマートコントラクトを使用しない仮想通貨と，使用した仮想通貨という意味での比較であれば，使用しない場合は単純な通過の送金のみが可能であり，使用する場合であれば，プログラムに

よって送金する相手を条件判定によって選択可能であったり，NFTなどを扱うことが可能であるといった特徴があります．
脆弱性に関しては，今回紹介した脆弱性が，Ethereumスマートコントラクトのコードに含まれる脆弱性なので，Etheruemスマートコントラクト独自の脆弱性となります．

質問
脆弱性全般についての質問なのですが，ブロックチェーンの技術は，一般的にセキュリティが高そうな感じがするのですが，smart contractでは不注意による脆弱性ををついて基本被害が出てから脆弱性の対策が始まるといったような，結局セキュリティにおけるいたちごっこみたいになってちゃっているのが現状なのでしょうか？

回答
質問内容を解釈すると，ブロックチェーン技術のセキュリティの高さといった点は，ブロックを生成する際に不特定多数のノードによって生成されるブロックの検証が行われるため，生成時に不正を行うことが難しいといった点や，一度発生した取引はマイニングの困難さから改ざんが難しいといった点についてのことだと思われます．
またスマートコントラクトでは，被害が発生したことにより脆弱性が発見される場合と，研究などによって脆弱性が発見される場合が考えられます．そのため，ご指摘の通りいたちごっこの状態になる可能性もありますが，事前に発見することでその被害を抑えるといったことも可能であると考えられます．
—---
<NFT>

質問
NFTは今後広く使われると思われますか．

回答
あらゆるデジタルデータを扱える点から，アートをはじめとし音楽やゲームなどさまざまな分野に応用されつつあります．分野が拡大するにつれて，NFTに触れる人が増えることで，広く使われる可能性は十分にあります．

質問
NFTは新しい技術であり課題や脆弱性が多くあるとのことでしたが，実際にNFTの改ざんや攻撃事例は数多くあるのでしょうか．

回答

NFTの流出やNFT上でのフィッシング詐欺の事例などの攻撃事例があります．
実際の例は多くないものの，NFTを共謀したノード間での取引を繰り返し行い，NFTの価格を意図的に上昇させる仮装売買といったものも存在します．

質問
What is the difference in nature between “Top to Bottom” and “Bottom to Top” NFTs?

回答

"Top to Bottom"で生成されるNFTは，アート作品のように個々が完全にユニークなものであり，一方，"Bottom to Top"はテンプレートから作られる元となるデータは共通されるものの，その後付与される属性のデータなどによって，個々のデータがユニークになっていく，といった特徴の差があると考えられます．

質問
NFTについての質問で，特にゲームキャラクターの例で，このようなユニークなキャラクターの獲得はブロックチェーンを使わずに現在の中央集権的な実装出来そうな気がするのですがどうなのでしょうか？実装できるかどうかより価値を与えられるところに良さがあるのですか？

回答
中央集権方の実装で可能かどうかでいうと，既存のゲームにおいてユニークなキャラクターや装備は存在しているため，可能であると思われます．
そのため，NFTとしてキャラクターを作ることの意味としては，そのユニーク性とそれに対する所有権が保証されるといった点が重要であると考えられます．

質問
NFTと暗号資産は何か違いがありますか？

回答
NFTは暗号資産の一種です．
ただし，暗号資産には2種類のトークンというものがあり，ビットコインやイーサリアムのように通貨やコインのように扱われるものをFungible token，NFTをNon-fungible tokenと言います．
Fungible token（代替性トークン）は，それぞれのトークンごと（コインごと）の価値が等しいものである一方で，Non-fungible token（非代替性トークン）は，それぞれのトークンがユニークで価値が異なり，代替品が存在しないもの，という特徴があります．

質問
NFTを生成する際に，同一のもの(とても類似しているもの)でも別のNFTとして取り扱われるのでしょうか？例えば，Top-to-Bottomで絵のNFTを生成する際に，同一の絵を別のデジタルデータとして生成や本物と贋作の絵によって生成すると，これらのNFTはどのように扱われるのかが気になりました．

回答
NFTは，1つのトークンに対して，1つのデジタルデータが割り当てられるということから，データを複製して2つの絵が作られた場合は，それぞれが別のNFTとして扱われます．
ただし，絵の製作者ではない人物が，入手したNFTのデータをコピーしてそのデータを新たなNFTとして扱う場合，ブロックチェーン上にそれをNFTとして送信することは可能であると思われます．ただし，それがコピーであると発覚した場合，ブロックチェーンには全ての取引情報が記録されており，NFTでは製作者のデータなども記録されているため，初めにそのデータをブロックチェーンに送信した人が，コピーされたものを偽物であると主張できると考えられます．次の質問回答も関連すると思うので，参考にしてください．

質問
ちょっと改変したものや，コラージュ等はどうなるのでしょうか？
取引されると元作品の権利者に何%みたいな話になりますか？

回答
NFTのデータをコピーし，それによって作成されたコラージュなどが新たなNFTとして作られる場合，それは元のNFTは異なるものであるため，直接権利者に対して還元が行われうることはないと思われます．しかし，デジタルアートなども著作物であるため，NFTにも著作権が存在するため，著作権を考慮した行動が必要です．また，元作品の権利者とコラージュ作成者の間において，取引の1部を権利者に還元するといった条件になった場合，スマートコントラクトによってその条件を満たす取引を記述することも可能です．

<発表時質問>

質問
デフォルトがpublic じゃなくprivate にしておくと安全だと思うのですが，デフォルトがpublic なのは利便性の面でメリットがあるのですか．

回答
多くの人に使われることが前提として作られているため，デフォルトはpublic に設定されていると考えられます．

質問
UncheckedCall でお金が送られなかったあと，どうなりますか．

回答
コントラクトAにイーサが残った状態となります．コントラクトBはログからコントラクトAが送金していないことを主張することで，コントラクトAに再度送金処理を求めることができます．

質問
DoS攻撃を受けているかどうかはどう確認するのですか．DoS攻撃を受けた場合どんな挙動になりますか．

回答
Dos攻撃を受けた場合Gasの制限を越えて動作できなくなります．
コードによってはどんなアクセスがされているかを確認することでDos攻撃かどうかを見分けることができると考えられます．

質問
ガスを支払うのは，どのタイミングですか．

回答
コードを実行する際に，ガスの量を指定して実行します．コードの実行で残ったガスは返ってきます．ガスが足りなかった場合は，実行途中で終了してしまいます．

質問
取引のログか個人が特定されてしまうような，プライバシーに関する問題点はありますか

回答

取引のログから個人を特定されてしまう可能性はあり，どのように取引のログから個人の情報を守るかがブロックチェーンの課題点の一つとなっています．

質問
NFTで現実世界のものに活用されている例はありますか．

回答
デジタルで管理できるものであればNFTを活用することができます．今後，ARなどの発展によって，現実のものにもNFTが付与される可能性はあります．

質問
戻り値を確認しないというのが，初歩的なミスだと思うのですが，このような事例はたくさんありますか．

回答
独自の言語でコントラクトは作成されているため，全てのコントラクト作成者が関数の戻り値まで詳しく把握していることはないためこのような初歩的なミスによる脆弱性が存在します．