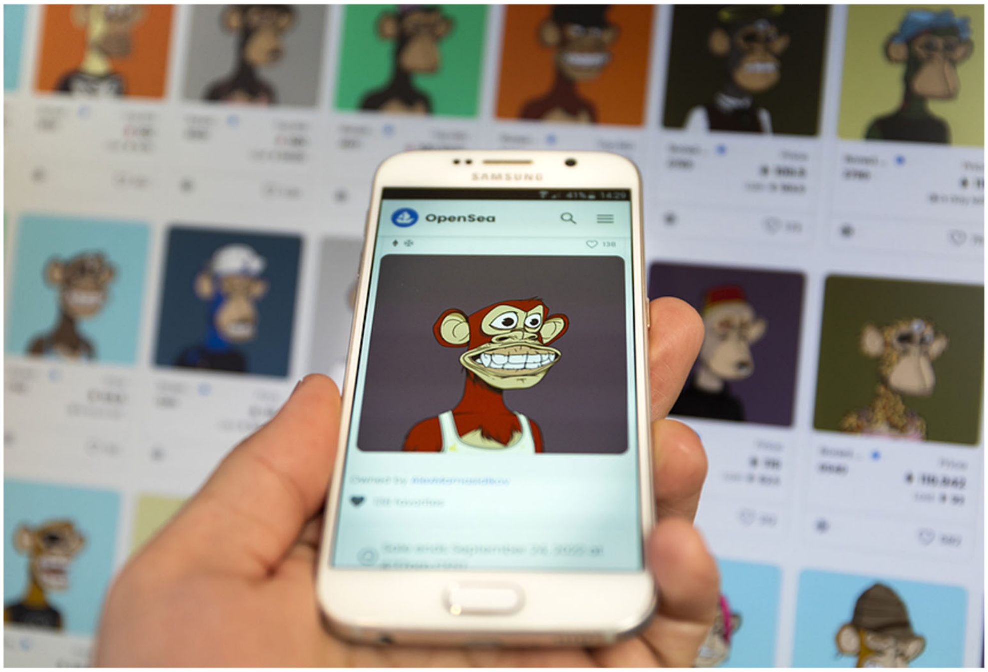
The ABCs of NFTs

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE



With the advent of blockchain technology, collecting, in the form of non-fungible tokens (or NFTs), has taken on a whole new look. NFTs can be confusing, and as with many transactions, there are risks. First and foremost, NFTs are intangible or nonfungible items, and are not insurable under standard personal or commercial insurance policies, as with NFTs there would be no direct physical loss to tangible property. This represents a challenge to insurers as they attempt to address the insurance exposures and potential losses related to the growing universe of NFTs.

According to Forbes, non-fungible tokens are unique crypto tokens that provide ownership of assets in the physical and digital world. They are also referred to as digital collectibles. They obtain their value from being a verified version of the digital asset. NFTs can be used for a variety of items including art, music, gaming, and even memes. NFTs are created using the same kind of blockchain programming as cryptocurrency, such as Bitcoin. NFTs are NOT the actual item, but they can be used to authenticate digital or physical assets. The NFT is a link to where the actual item – such as a JPEG or other media – resides on the blockchain. NFTs are unique and cannot be replicated. This does not prohibit the NFT from being sold or the actual asset from being duplicated. Even though the concept can be confusing, creation or minting of an NFT – publishing it on the blockchain – is fairly easy. There are a number of platforms, including two of the most popular, Ethereum and Open Sea, and they are not all the same.

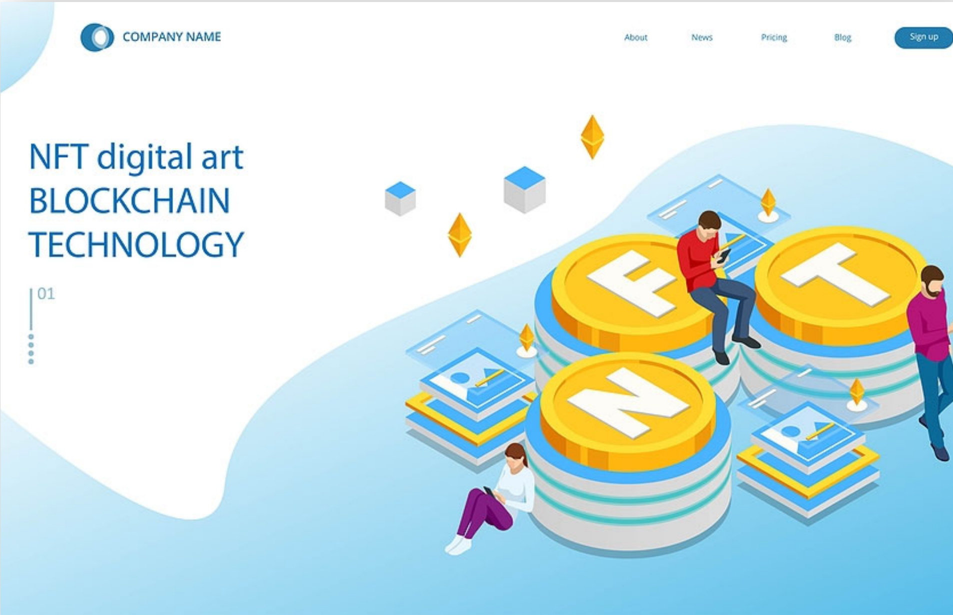
One difference is who pays the fee for creation of the NFT. Every blockchain transaction must be verified by “miners”. The fee is for the time and energy required to verify the transactions. Ethereum’s transaction fees (known as a gas fee) are paid for by the creator of the NFT, where Open Sea adds the fee to the purchaser’s cost. Currently, most NFTs are part of Ethereum blockchain. Due to the nature of blockchain, all transactions can be verified. Unlike cryptocurrency, NFTs are unique and cannot be replaced. This is in contrast to fungible tokens, which, according to Cointelegraph, are divisible and non-unique.

For example, fiat currencies like the dollar are fungible as is Bitcoin, no matter where it is issued the value is the same. Fungible items, including bitcoin cryptocurrency, can be traded.

A digital wallet is needed in order to store the NFTs and manage cryptocurrency and tokens, both fungible and nonfungible. Each wallet requires a unique key or recovery phrase to enable the owner to buy and sell cryptocurrency. The wallet can be either “hot” or “cold”. Hot wallets are connected to the internet and therefore vulnerable to attack including phishing, scams, and viruses. A cold wallet is not connected to the internet and therefore not hackable.

Some cold wallets are totally removed from the internet and accessible only via a smartphone app. A paper document that lists the public and private keys is the most basic form of a cold wallet. Hot wallets are more convenient to use than cold wallets, as they are already connected to the internet. Wallets contain public and private keys. Public keys are readily discoverable, similar to an address. Private keys are in essence passwords, available only to the owner of the wallet. Although usually a numerical sequence, the key can also be a “seed phrase” – a random series of words that must be used to access the information in the wallet.

There are a number of risks related to non-fungible tokens. First and foremost is access. If the recovery phrase or key for the wallet is lost, the user loses access to the wallet and its contents. As mentioned previously, traditional insurance coverage does not apply to NFTs. Although there is a record of



every transaction on the blockchain, it may be impossible to trace where the money went. Criminals may set up fake platforms or sell fraudulent NFTs.

Another risk related to NFTs is money laundering. Although the NFT itself can be verified, and each transaction is recorded on the blockchain, there may not be a way to trace where the money went.

The accounts can be set up anonymously and funds can be transferred to multiple accounts. The potential buyer must use due diligence to ensure they are not being scammed.

A red flag could be an asset whose selling price is significantly different from its fair market value. However, this can be challenging with something like artwork. As with any digital transaction, cyber security is crucial. The Bored Ape Yacht Club is a collection of 10,000 unique digital ape collectibles. There have been multiple instances of scamming, phishing, and theft of these NFTs – resulting in hundreds of thousands of dollars in losses.

The numbers involved with NFTs are nothing to joke about. One piece of artwork by Beeple sold for $69 million. The first quarter of 2022 saw NFT funding of $2.4 billion. In February 2022, a home in Gulfport, Florida was sold as an NFT for over $600,000. Alfa Romeo is introducing an SUV whose service record is an NFT. As mentioned previously, insurance for NFTs is not available under most standard insurance policies. Crime coverage has traditionally been offered to protect the value of assets, while cyber insurance addresses the first- and third-party liability risks associated with exposures such as hacking, network security and system failure. Any potential coverage needs to address the cyber and crime aspects. It is important to note that in the cases where the NFT represents a physical object, such as a piece of artwork, traditional insurance would be available to cover the artwork even if it does not cover the NFT.

The exposures to loss vary based on who is looking for coverage. Third party repositories of keys have potential liability to the NFT if access to the keys is lost or stolen. There are also third parties who may store the NFT, or the digital assets associated with the NFT. The owner of the NFT may be concerned about third party storage of the NFT and assets. A tech-savvy owner may be more concerned with their own blockchain and digital wallet, rather than just a single NFT asset.

A number of companies have started to offer specialty coverage for NFTs. In April 2022, Shield Coin introduced blanket insurance coverage to owners of digital wallets containing Shield Coin NFTs. Coverage is offered for various scams including “rug pulls” and other potential loss of assets. Munich Re teamed up with Marsh and Curv to offer custom hybrid crime and cyber coverage for Curv’s Institutional Digital Asset Wallet Service. Curv offers infrastructure for digital asset security.

As technology and society continue to evolve, it is essential that insurance companies adapt.

Coverage for digital assets requires a creative blend of crime and cyber. NFTs are a growing market to be explored.

Sue Quimby is a vice president, media editor, client services & training and a senior product development analyst at MSO, Inc (The Mutual Service Office, Inc.).

You can reach Sue at
squimby@msonet.com or
201.857.9128.