CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 5 | December 15, 2020

Table of Contents

- DeFi: High yield and unregulated crypto securities market
- Microsoft uses Copyright and Trademark Law to combat botnet

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

DeFi: High yield and unregulated crypto securities market

DeFi, the acronym for Decentralized Finance, refers to a decentralized financial system built on the blockchain and governed through smart contracts and other blockchain-based applications. *See What is DeFi?*, available here. It mimics the functionality of traditional financial systems without a centralized entity tasked to facilitate transactions. *See DeFi Vs. Legacy Finance: Solving Old Issues Brings New Complexities*, available here. DeFi platforms have flourished by providing certain financial services to the cryptocurrency community. As Figure 1 illustrates, the amount of Ethereum cryptocurrency used in DeFi platforms has increased over time. The underlying mechanisms of DeFi systems are "financial smart contracts, protocols, and decentralized applications (DApps)," built on the Ethereum blockchain. *See What is DeFi?*, *supra*.

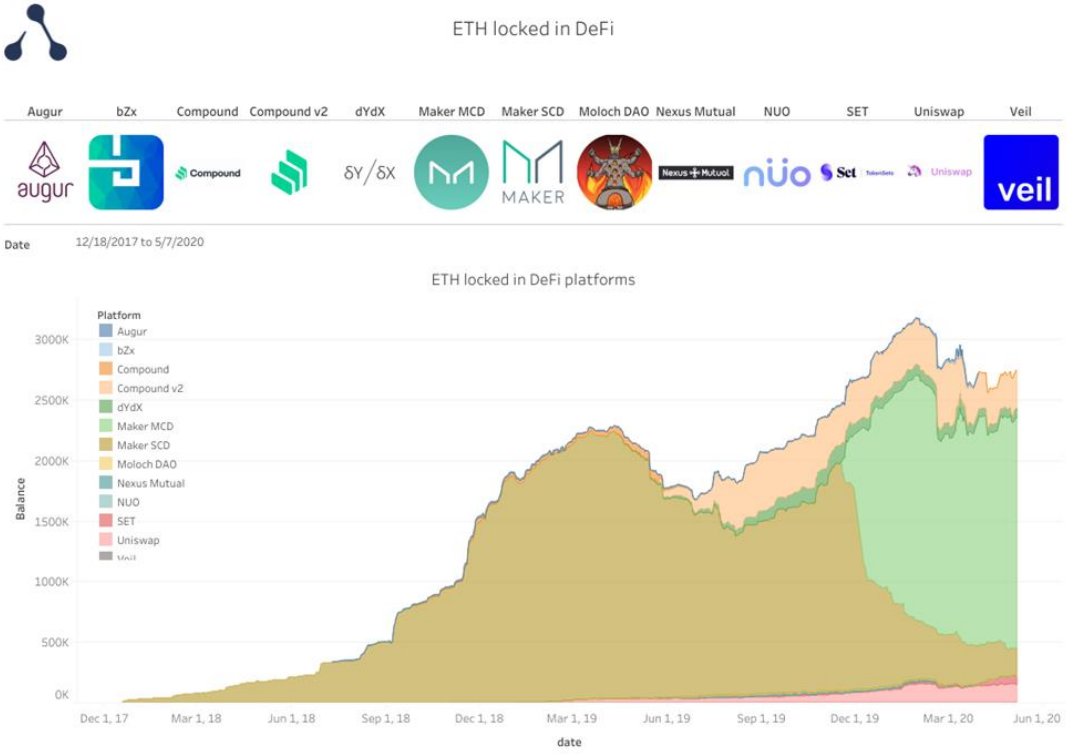

Figure 1: Number of Ethereum locked in DeFi platforms; retrieved from https://aleth.io/data/defi/eth-locked-in-defi

Most DeFi platforms do not require users to undergo Know-Your-Customer (KYC) or Anti-Money-Laundering (AML) protocols. Instead, users are only required to present a cryptocurrency wallet. These platforms currently offer financial yields that are competitive with the U.S. securities market. *See Explore DeFi Lending Rates*, available here. They have the potential to create highly lucrative but unregulated markets for crypto securities, where all users, including cyber criminals and those who are under international sanctions, can invest crypto assets for a potentially sizable return.

DeFi ecosystem

A brief overview of blockchain and smart contracts, the main mechanisms powering DeFi, is appropriate before moving to the analysis of the risks and benefits that the DeFi ecosystem poses.

Blockchain is a decentralized record-keeping system in which data blocks are sequentially linked to each other and secured through hash functions. *See Bitcoin: A Peer-to-Peer Electronic Cash System*, available here. Cryptocurrencies use blockchain as a ledger to manage and store cryptocurrency transactions among users. Figure 2 illustrates how blocks of transaction data are linked with each other.

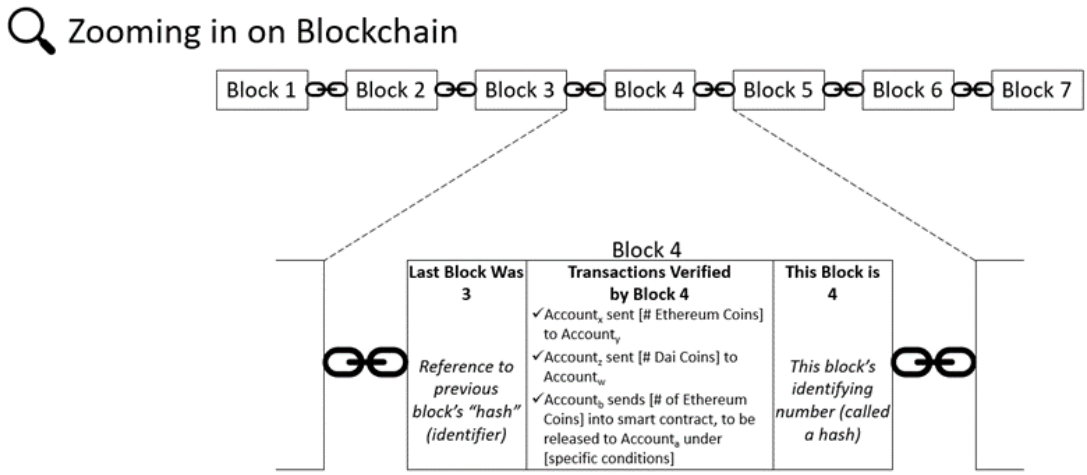

Figure 2: How blockchain works; graphic by Scott Meyer, CLCT

In this context, smart contracts are computer programs that can automatically allocate crypto assets among different parties based on different conditions coded in the program. *See smart contract*, available here. Figure 3 summarizes the core characteristics of smart contracts. For DeFi platforms, smart contracts are stored and executed within the blockchain.

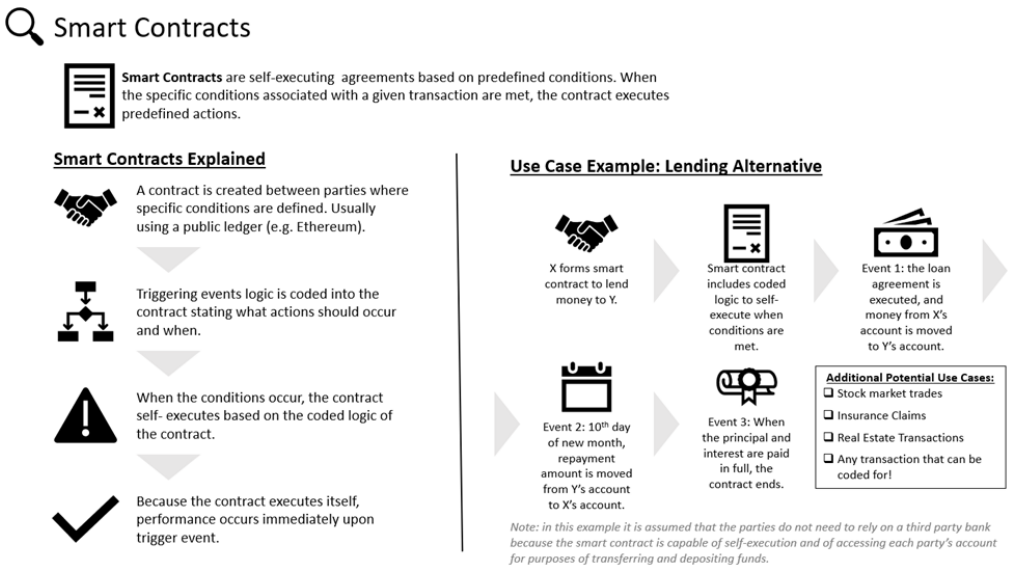

Figure 3: How Smart Contracts Work; graphic by Scott Meyer, CLCT

Keeping in the spirit of the decentralized autonomous architecture of blockchain systems, the objective of DeFi is to create a system where financial services are available to everyone, and centralized entities are unnecessary.

One of the most popular DeFi services is lending and borrowing. Users can lend crypto assets with a competitive interest rate, while others can borrow. Each DeFi platform has its own rule governing lending and borrowing.

In general, users can lend any amount of crypto assets that they possess. For borrowing, users must first offer other crypto assets as collateral. Each DeFi borrowing platform sets a collateral factor, which is used to calculate the maximum amount that a user can borrow. *See, e.g., Borrowing Assets from the Compound Protocol*, available here. For example, if a user offers crypto assets worth $100 and the collateral factor is 75%, the maximum amount the user can borrow is $75 worth of crypto assets. This, once the user borrows a crypto asset, interest accumulates immediately. If the value of the asset borrowed with interest exceeds the maximum amount that the user can borrow, then the DeFi platform begins to liquidate the user's collateral.

As Figure 4 shows, the interest rates of borrowing and lending crypto assets are much higher than yields offered by traditional U.S. securities, which makes DeFi lending services much more lucrative. For comparison, the national average of annual percentage yield for a non-jumbo 60-month Certified Deposit is 0.35%, *See Weekly rate cap information for the week of November 16, 2020.*, available here. For those who do not have access to the U.S. securities markets, DeFi services provide an alternative to invest and grow assets.

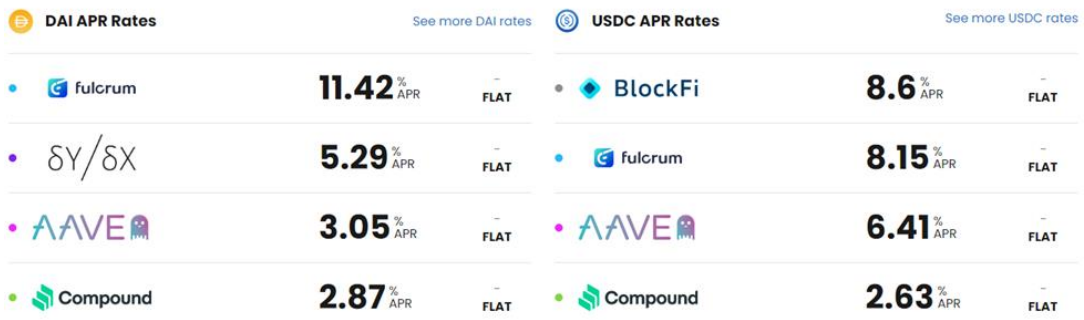

Figure 4: Cryptocurrency lending rates among different DeFi platforms; retrieved from https://defirate.com/

Until recently, cryptocurrency users had to utilize centralized cryptocurrency exchanges to exchange crypto assets. This process involved users having to rely on an intermediary to complete crypto exchange transactions.

For example, Coinbase, incorporated in Delaware, is one of the largest centralized cryptocurrency exchanges in the U.S. To exchange crypto assets, Coinbase users first have to transfer crypto assets to a Coinbase-controlled wallet. While the underlying asset is under Coinbase's control, users can exchange their crypto assets into another form, such as a different crypto token, via the company's internal exchange market. During each step of the exchange, Coinbase can delay or disrupt the process by placing a hold on the underlying crypto asset. In fact, in the past, some users have claimed that the exchange held funds for several days for unknown reasons. *See CoinBase funds on hold for 13 days?*, available here. As such, users assume the risk of temporarily losing control over crypto assets while utilizing a centralized cryptocurrency exchange.

To prevent this, some users have turned towards decentralized exchanges (DEXs, a type of DeFi), where they can exchange their crypto assets using liquidity pools without transferring the custody of the underlying collateral to a third party. *See DeFi Projects*, available here.

Liquidity pools are managed by smart contracts and made up of crypto assets staked by other users, who act as liquidity providers. As shown in Figure 5, DEXs effectively provide automated peer-to-peer crypto asset swaps that allow one group of users to exchange crypto assets while another group collects the nominal fee for providing the necessary asset liquidity to facilitate the exchange transaction. At present, DEXs cannot exchange different types of cryptocurrencies (e.g., exchange Bitcoin for Ethereum) but only facilitate exchanges among different Ethereum tokens.

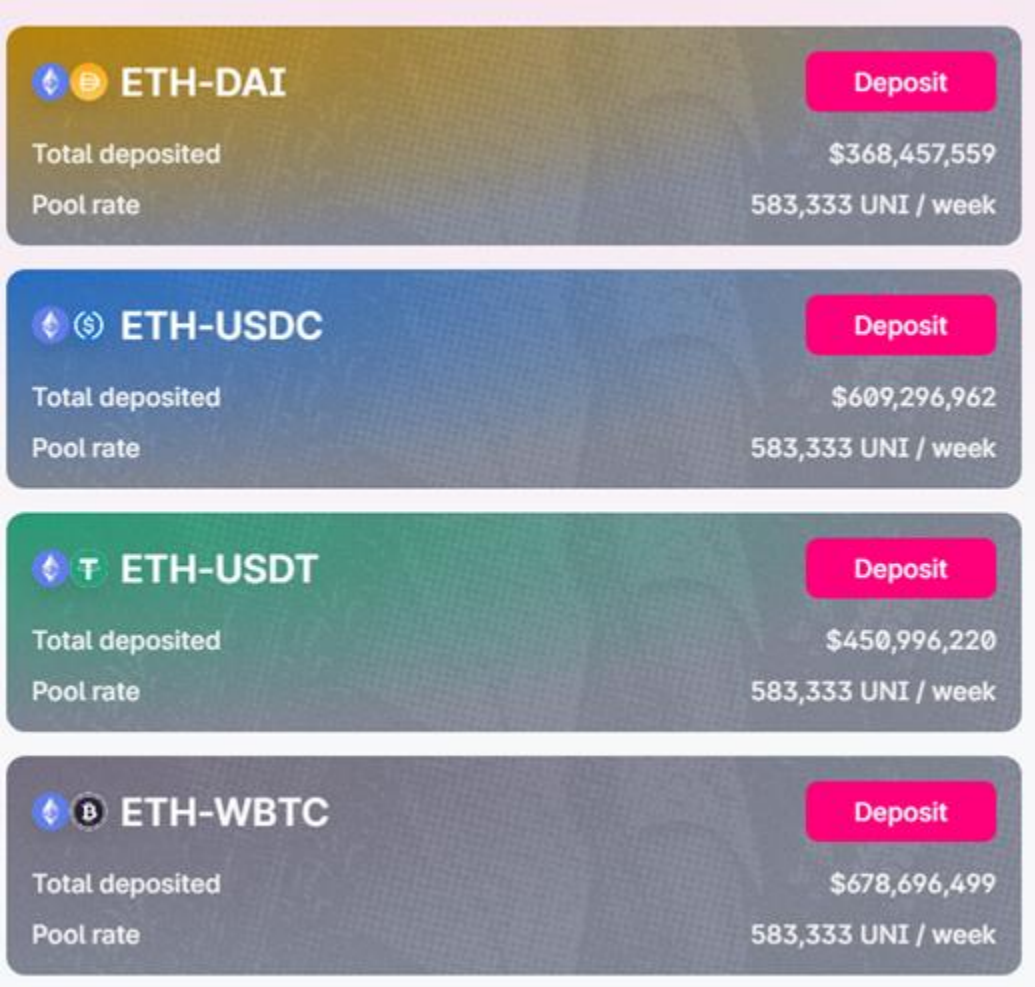

Figure 5: Liquidity pools from Uniswap; retrieved from https://app.uniswap.org/#/uni

Other forms of DeFi services cover derivative markets, asset management, and insurance services. *See DeFi Projects*, *supra*. With continued smart contract development, DeFi platforms can expand the functionality of blockchain technology beyond currency transactions.

DeFi vs. Traditional financial institutions

One of the significant characteristics of DeFi is that the underlying smart contracts reside within the Ethereum blockchain. This makes DeFi platforms decentralized because copies of smart contracts are interspersed among the decentralized network of Ethereum nodes, which maintain the Ethereum blockchain. DeFi's decentralized blockchain infrastructure makes it difficult for third-party actors to disrupt or shut down the platform's services.

Traditional financial institutions are centralized entities, where the operational nexuses are consolidated. They reserve a level of transactional control that can delay, pause, and even reverse financial transactions. Also, these institutions are subject to extensive governmental regulations, which require, amongst others, the implementation of know-your-customer (KYC) and anti-money-laundering (AML) protocols. KYC protocols, in particular, prevent individuals and organizations listed on Specially Designated Nationals and Blocked Persons List (SDN) of Office of Foreign Assets Control, U.S. Department of Treasury, from accessing the U.S.

financial markets and services. *See A Framework for OFAC Compliance Commitments*, available here.

On the contrary, DeFi platforms are decentralized and are governed through smart contracts alone. As such, there are no external mechanisms to delay, pause, or reverse executed transactions within the DeFi platform, except for occasional hindrance from the congestion of the Ethereum blockchain.

Because there is no centralized authority representing DeFi platforms in the physical world, governmental entities find major obstacles in forcing DeFi platforms to implement necessary regulations, including KYC and AML protocols. Consequently, any user worldwide has unrestricted access to crypto-based financial instruments. This unrestricted access may pose cybersecurity problems, especially in the area of ransomware.

Cybersecurity

Cryptocurrencies are often used to facilitate illicit transactions. For example, a major illegal drug marketplace website hosted within The Onion Router network used Bitcoin to facilitate payment between customers and drug suppliers. *See Acting Manhattan U.S. Attorney Announces Forfeiture Of $48 Million From Sale Of Silk Road Bitcoins*, available here. A recent report from the U.S. Department of Justice disclosed that terrorist networks had conducted fundraising efforts using cryptocurrency. *See Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Network* at 7, available here.

In recent years, one of the most notorious uses of cryptocurrencies has been to facilitate ransomware payments between malicious actors and cybersecurity victims. DeFi services may provide another set of tools for malicious actors to increase the value of stolen assets while maintaining their anonymity. For example, a malicious actor can utilize a DeFi lending platform to invest stolen crypto assets without worrying about government seizure of assets or sudden shut down of the lending platform. The malicious actor can also use DEXs to exchange parts of the stolen crypto assets into another form without undergoing any KYC protocols.

Despite the risk of attracting malicious actors as users, DeFi provides a unique semi-democratic and semi-autonomous means of establishing complex financial frameworks governed by its stakeholders. Government regulators, policymakers, and law enforcement should study the technology and monitor the DeFi ecosystem to determine the best approaches for regulation and enforcement.

Microsoft uses Copyright and Trademark Law to combat botnet

The United States District Court for the Eastern District of Virginia (the Court) granted Microsoft a preliminary injunction to shut down servers supporting the TrickBot botnet. A botnet is a network of computer systems that have been infected with malware, where a malicious actor uses command-and-control servers (C2 servers) to exert control over the infected systems. *See What is a DDoS Botnet?*, available here. TrickBot has been reported "to steal passwords from millions of infected computers, and reportedly to hijack access to

well more than 250 million email accounts from which new copies of the malware are sent to the victim's contacts." *See Microsoft Uses Trademark Law to Disrupt Trickbot Botnet*, available here. This botnet reportedly also could deploy ransomware on corporate networks.

Arguing in support of the motion, Microsoft alleged that, among others, the malicious actors running the botnet violated (1) the Copyright Act, and (2) the Lanham Act (federal statute governing trademark and unfair competition). The Court found good cause to determine that the Trickbot hackers infringed Microsoft's copyrighted works and trademarks. Taking into account other alleged violations put forward by Microsoft, the Court ordered server hosting companies to identify and shut down TrickBot compromised servers and cooperate with Microsoft to identify individuals behind the botnet operation.

By disabling the botnet servers, Microsoft claimed that hacker groups behind TrickBot would not be able to spread new malware infections or activate previously deployed ransomware that is already installed into computer systems. *See New action to combat ransomware ahead of U.S. elections*, available here.

Legal Arguments

Although copyright and trademark violations have not previously been used as legal maneuvers to shut down botnet servers, the Court recognized the validity of these claims and granted injunctive relief. Specifically, the Court noted that TrickBot hackers "infring[ed] Microsoft's Copyrighted Work by reproducing, distributing, and creating derivative works in their malicious software, which includes code that is literally copied from . . . the Copyrighted Works." *See Microsoft v. John Does 1-2, No. 1:20-cv-1171 (AJT/IDD) (E.D. Va. 2020)*, available here. The Court also noted that TrickBot hackers deceptively created fake Microsoft websites that were not associated with the company. *Id.*

Microsoft acknowledged that this novel application of copyright and trademark law "is an important development . . . to stop the spread of malware, allowing [Microsoft] to take civil action to protect customers in the large number of countries around the world that have these laws in place." *See New action to combat ransomware ahead of U.S. elections*, *supra.*

Although there were hundreds of TrickBot C2 servers around the world, most of them are offline. As shown in Figure 1, as of the time of publication, there are only four servers left online supporting the TrickBot botnet. *See Feodo Tracker*, available here. Microsoft has severely disrupted the TrickBot's capability to conduct cyber intrusion operations, but there is a possibility of the botnet to recover its attack arsenal.

Firstseen (UTC)	Host	Malware	Status	SBL	Network (ASN)	Country
2020-12-12 02:00:45	13.56.227.131	TrickBot	Online	Not listed	AS16509 AMAZON-02	US
2020-12-12 02:00:45	3.101.12.202	TrickBot	Online	Not listed	AS16509 AMAZON-02	US
2020-12-08 20:45:53	186.47.209.222	TrickBot	Online	Not listed	AS28006 CORPORACION NACIONAL DE TELECOMUNICACIONES...	EC
2020-12-08 16:40:56	45.141.59.212	TrickBot	Online	Not listed	AS213373 IPCONNECT	DE
2020-12-08 16:52:03	192.3.73.165	TrickBot	Offline	Not listed	AS36352 AS-COLOCROSSING	US
2020-12-08 16:52:03	45.12.110.195	TrickBot	Offline	Not listed	AS35913 DEDIPATH-LLC	US
2020-12-08 16:40:56	45.12.110.193	TrickBot	Offline	Not listed	AS35913 DEDIPATH-LLC	US

Figure 1: List of TrickBot botnet servers; retrieved from https://feodotracker.abuse.ch/browse/trickbot/

U.S. cyber crime laws, including the Computer Fraud and Abuse Act, do not allow private actors to offensively cyber attack suspected cybercriminals' computer systems. *See 18 U.S.C. § 1030(a)(2)* (prohibiting intentionally accessing a computer without authorization and obtaining information from any protected computer), available here. Instead, victims of cyber crimes must either (1) persuade law enforcement to pursue the matter or (2) ask a court to order an injunction that legally empowers the victims to offensively disrupt cyber crime operations. Microsoft's novel approach of using Copyright and Trademark Law opens additional legal avenues for others looking to offensively combat cyber crimes.