Cryptocurrency past is prologue: before and after FTX

By John Bandler, Esq., Bandler Law Firm PLLC

JANUARY 17, 2023

FTX is not the first nor last but a recent and enormous implosion in the cryptocurrency industry. Previously we have seen examples parade by of external theft, internal theft, anti-money laundering failures, cybercrime enablement, loss of cryptographic keys and skewed investor playing fields. More will come, and we should reevaluate whether crypto investment is a helpful development or a zero-sum game where hucksters, charlatans and the lucky can make money at the expense of others.

The management and regulation of banks and investment houses have evolved over hundreds of years. It will never be perfect, but we have rules and controls to protect against bank robbery, embezzlement, failure, and even losing keys to the bank or vault. Basic protections have not been implemented by many crypto organizations.

Put aside the technology and jargon

New technology and lingo generate excitement and confusion, but we can simplify the concepts with this framework:

- **Currency**: an official currency of a government, such as the U.S. dollar.
- **Virtual currency**: like a currency but not issued by government, it could be issued by anyone and is a way to transfer value.
- **Cryptocurrency**: a type of virtual currency on a type of software. Describing it would leave most people dazed and their eyes glazed. Just think of cryptocurrency as a subset of virtual currency.
- **Virtual asset**: The use of virtual currency or cryptocurrency for an investment purpose. When people try to "buy low and sell high."
- **Value other than currency**: A method to store or transfer value that does not involve an official currency (includes virtual currency).

Important events in our timeline

Early humans traded and stored value without any currency, including through barter and other methods. People gave and received value informally, each performing tasks to benefit another person or the community.

Commodity money, such as gold and salt, became useful where direct barter was inconvenient or impossible, and facilitated payments, trade, and value storage.

An early precursor to virtual currency was Hawala, which came as early as the 8th century along the original Silk Road and still exists today. It was a method to informally transfer value from a sender in one place to a recipient in another. Each person used a hawala broker (hawaladar) in their respective location, and the hawaladars facilitated the transfer of value by acting as intermediaries.

We should reevaluate whether crypto investment is a helpful development or a zero-sum game where hucksters, charlatans and the lucky can make money at the expense of others.

Eventually governments saw the need for official currencies. They are essential today, yet informal value transfer remains part of life and commerce.

More recently the internet was born and with it a new twist on value transfer using cyberspace. In 1996 e-gold was created, the first widely used virtual currency, and next came WebMoney in 1998. Illegal uses of these platforms proliferated and were investigated during a groundbreaking case (*People v. Western Express International, Inc., et al*, or The Western Express Case) by the New York County District Attorney's Office (DANY) under the legendary Robert M. Morgenthau. (The author, as assistant district attorney at the time, led this investigation which revealed how cybercriminals used these early virtual currencies to do business and launder their ill-gotten gains).

Bitcoin was invented around 2008, an evolution of virtual currency and the first "cryptocurrency." It was a "decentralized" payment platform, meaning no one was officially in charge of it. The technical details are irrelevant here so we can skip discussion of "blockchain" and other terms.

The value of Bitcoin eventually rose significantly, a few got rich, and others saw opportunity. More cryptocurrencies spawned, and the crypto-investment boom began. Trading platforms proliferated with plenty of marketing hype, and ordinary people started to invest.

Laws and regulations

Existing laws and regulations applied to these new virtual currencies and cryptocurrencies. But existence of laws does not mean everyone complies with them. Some claimed that old laws do not apply to new crypto.

But imagine a driver of an early electric car speeding down the highway at 100 miles per hour and stopped by the state trooper. The driver claims that the existing speeding laws — enacted decades prior — could not possibly apply to his new electric car. This defense fails, the ticket is issued and the judge ultimately convicts.

The DANY money laundering and cybercrime investigation revealed a wild west of improper activity, not because of an absence of laws but because of law breakers and limited enforcement.

For example, as established in various court proceedings, guilty pleas, and trial, including in the Western Express case, the e-gold platform and early virtual currency exchangers had practically no anti-money laundering controls. From 1996 to about 2007 users could open e-gold accounts and transact enormous amounts of value with no customer verification — just an email address. Cybercriminals and identity thieves sent illicit funds around the world with no oversight.

Virtual currencies and cryptocurrencies are here to stay, and wrongdoers will continue to use them. Cybercrime is also here to stay, and government will adapt and catch some offenders but never all.

This DANY prosecution was one of the first to examine cybercrime and virtual currency money laundering. Existing state criminal laws were applied to this new area of crime, and cybercriminals were apprehended within the U.S. and abroad.

e-gold was eventually indicted by federal prosecutors and shut down, but the need for virtual currency remained. New ones arose including Liberty Reserve, Bitcoin and more.

In 2013 the Financial Crimes Enforcement Network (FinCEN, an arm of our Treasury Department and our anti-money laundering regulator) made clear that virtual currency and cryptocurrency fall within their existing regulations. It took time for this guidance to arrive, but the underlying rules were already there. Subsequent guidance made clear that regulatory oversight exists in this space, whatever technology or jargon is used.

Other federal and state government regulators have weighed in on investor protection and consumer protection.

We should not blame the rules for implosions if rules exist but are disregarded. Crypto failures occur because of bad actions, bad actors, bad management, or all three. Enforcement lags significantly in cyberspace and virtual currency, but we should also remember that it trails (though to a lesser extent) everywhere.

We can see the future

Having seen the past, we can see the general future.

FTX will not be the last crypto company in the headlines. For example, it was reported about the major cryptocurrency player Binance that until August 2021 they allowed users "to open accounts with solely an email address." ("U.S. Justice Dept is split over charging Binance as crypto world falters," Reuters Business, Dec. 12, 2022, https://reut.rs/3CyxEpN) We see a similarity to e-gold decades before. Today's prosecutors and regulators are evaluating next steps, equipped with the legal precedent from their predecessors.

Virtual currencies and cryptocurrencies are here to stay, and wrongdoers will continue to use them. Cybercrime is also here to stay, and government will adapt and catch some offenders but never all. Cybercrime and virtual currencies will remain symbiotic. Investors and consumers will remain fascinated. The rules will be tweaked, and we will continue to debate whether government should do more or less.

A guide to choose our destiny

Here is a general direction for moving forward.

In the civil arena, more should be done by government to enforce rules for anti-money laundering and investor protection. In the criminal realm, government needs to do *much* more to better investigate cybercrime and money laundering, because wrongdoers thrive without enforcement and deterrence.

Organizations need to prioritize cybersecurity and cybercrime protection.

Individuals need to beware of investment hype and always conduct due diligence.

Readers should stay tuned to current events because the future will be as interesting as the past.

About the author

John Bandler is a lawyer, consultant, speaker, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better manage information assets. His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com. Bandler was formerly an assistant district attorney with the New York County District Attorney's Office, where he led the investigation in *People v. Western Express International, Inc., et al.*, discussed in this article, into cybercrime and virtual currencies.

This article was first published on Reuters Legal News and Westlaw Today on January 17, 2023.