Question: 09. TBD How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?

Return to CBDC Benefits, Risks, and Policy Considerations

Question

Return to Top

How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?

Answer

Return to Top

According to Jason Bloomberg,

Figure 1: Eight Common Cryptocurrency Transaction Types.
Table 1:

Rank	Cryptocurrency Transaction Type	Description	Comment
1	**Speculation**	Speculation is far from being the only reason to conduct transactions with crypto.	
2	**Darknet Transactions**	The Darknet consists of parts of the Internet that standard search engines cannot reach – those dark corners of the Web where purveyors of contraband from illegal drugs to child pornography do business. In fact, if it weren't for crypto, the Darknet would be a mere shadow of its current self – and Bitcoin remains the coin of the realm. "Bitcoin is the most common form of payment for drug sales on darknet marketplaces and is emerging as a desirable method to transfer illicit drug proceeds internationally," according to the US Drug Enforcement Agency's (DEA's) 2017 National Drug Threat Assessment Report. "Bitcoin is the most widely used virtual currency due to its longevity and growing acceptance at legitimate businesses and institutions worldwide."	

Rank	Cryptocurrency Transaction Type	Description	Comment
3	**Money Laundering**	Remember the piles of illicit currency from Scarface, or for that matter, Breaking Bad? Back in the day, turning criminal gains into legitimate assets required processing mountains of cash. Not so much anymore. Today, in spite of (or perhaps because of) dramatic improvement in anti-money laundering (AML) regulatory enforcement, the money laundering action has largely moved to crypto. “97% of criminal Bitcoin directly received by [crypto] exchanges flowed into those Located in countries with weak AML laws,” writes CipherTrace Cryptocurrency Intelligence in its report Cryptocurrency Anti-Money Laundering Report 2018 Q3. “Cryptocurrency exchanges in countries with weak AML regulation receive nearly 5% of their payments directly from criminal sources.” In particular, given China’s restrictions on the movement of capital, crypto has become quite popular for evading its laws. “CUBS [Chinese Underground Banking Systems] money brokers sell Bitcoin to drug traffickers for cash earned from drug sales in the US, Australia, and Europe. This drug cash is then sold to Chinese nationals in exchange for Bitcoin the Chinese nationals use to transfer the value of their assets outside of China,” according to the DEA report. “Many China-based firms manufacturing goods used in TBML [Trade Based Money Laundering] schemes now prefer to accept Bitcoin. Bitcoin is widely popular in China because it can be used to anonymously transfer value overseas, circumventing China’s capital controls.”	
4	**Ransomware**	Ransomware may now be less popular than cryptojacking, but it still remains a potent form of criminal extortion – and it’s simpler than ever. “Easy-to-use ‘ransomware as a service’ can be purchased cheaply on the Darknet, and at least one vendor offers customer support for users of its malware,” writes Michael Baker, Founder and Principal at Mosaic451, a bespoke cybersecurity service provider and consultancy, and a member of the Forbes Technology Council. “Would-be hackers who don’t want to purchase off-the-shelf ransomware can hire black-hat coders for custom development. All of these services are bought and sold using – you guessed it – cryptocurrency.” Even our phones aren’t safe from this pernicious application of crypto. “It is likely that ransomware will target connected devices containing personal data such as photos, emails, and even fitness progress information,” according to The cyber threat to UK business 2016/2017 Report by the National Cyber Security Centre of the National Crime Agency in the UK. “Ransomware on connected watches, fitness trackers, and TVs will present a challenge to manufacturers,” the report continues. “This data may not be inherently valuable, and might not be sold on criminal forums but the device and data will be sufficiently valuable to the victim that they will be willing to pay for it.”	

Rank	Cryptocurrency Transaction Type	Description	Comment
5	**Evading Sanctions**	It's no surprise that countries like North Korea are desperate for hard currency – and crypto gives them one avenue to obtain it. "Crypto-currencies have the added advantage to the DPRK [North Korea] of giving them more ways to circumvent US sanctions," according to Lourdes Miranda, cryptocurrency analyst and financial crimes investigator at MirandaFinIntel Consulting, and Ross Delston, an attorney and certified AML specialist who frequently serves as an expert witness. "DPRK can create their own crypto-currencies or use established ones like Bitcoin. Having their own crypto-currency would also facilitate their ability to open online accounts under the guise of a non-adversarial nation using anonymous communication to conceal the user's locations and usage on the internet." Furthermore, while the United States and many of its allies have sanctions against such countries as North Korea and Iran, there are also economic sanctions against much larger economies like Russia's that encourage Mr. Putin's empire to make serious investments in crypto. Such investments, in fact, take place at the nation-state level. "[The] Russian government is about to make a step to start diversifying financial reserves into Bitcoin since Russia [is] forced by US sanctions to dump US Treasury bonds and [take] back US dollars," according to Vladislav Ginko, an economist at the Russian Presidential Academy of National Economy and Public Administration, which is ironically funded by the Russian government itself. "These sanctions and the will to adopt modern financial technologies lead Russia to the way of investing its reserves into Bitcoin."	
6	**Crypto Theft**	Money laundering, ransomware, and state-sponsored sanctions evasion all have a spine-tingling James Bond flavor to them – but what about simple theft? "CipherTrace revealed a three-fold increase in cryptocurrency thefts during the first half of 2018 compared with the entire year of 2017," according to the Cryptocurrency Anti-Money Laundering Report 2018 Q3 by CipherTrace Cryptocurrency Intelligence. "CipherTrace estimates this trend will bring the total stolen and reported in 2018 to well over $1 billion by the end of [2018]." The FBI, in fact, is warning about a type of theft that is targeting holders of small amounts of crypto. "Virtual currency is increasingly targeted by tech support criminals, with individual victim losses often in the thousands of dollars," according to the FBI Public Service Announcement I-032818-PSA from March 2018. "Victims contact fraudulent virtual currency support numbers usually located via open source searches. The fraudulent support asks for access to the victim's virtual currency wallet and transfers the victim's virtual currency to another wallet for temporary holding during maintenance. The virtual currency is never returned to the victim."	

Rank	Cryptocurrency Transaction Type	Description	Comment
7	**Hacking Crypto**	Why bother stealing crypto if you can simply print more for yourself? That's exactly what a particular group of criminals accomplished earlier in 2019 by targeting weaknesses in Ethereum Classic, one of the most popular crypto behind Bitcoin. "We observed repeated deep reorganizations of the Ethereum Classic blockchain, most of which contained double spends," reports Mark Nesbitt, Security Engineer at Coinbase . "The total value of the double spends that we have observed thus far is 219,500 ETC (~$1.1M)." Double spending means taking the same unit of crypto and spending it twice – the online equivalent of running your greenbacks through a copier. A victimless crime, perhaps? You be the judge.	
8	**Legal Use**	Let us not forget the eighth type of crypto transaction: legal transactions that exchange crypto for goods and services – you know, like real money. Some crypto fans would have you believe that using crypto at your local coffee shop – or even sending funds to your relatives in Venezuela for buying food there – will be the prominent use of crypto at some point in the near future. Don't believe it. "Cryptocurrencies will likely become a bigger part of the cybercrime realm," concludes Yaya Jata Fanusie, director of analysis for the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies. "Any police and intelligence departments dealing with cyber issues need to deepen their expertise on cryptocurrencies and blockchain technology."	