Science & Technology Innovation Program

Wilson Center | Science and Technology Innovation Program

Image source: Stock Illustration ID: 1896598609 by KanawatTH (n.d.). Retrieved from: https://www.shutterstock.com/image-illustration/bitcoin-blockchain-crypto-currency-digital-encryption-1896598609

Author

Scott Dueweke

Global Fellow

Black Swans and Green Fields:

Exploring the Threat and Opportunity of the Alternative Payments Ecosystem to the West

August 2022

TABLE OF CONTENTS

In 2009, Satoshi Nakamoto published a white paper describing a digital cryptocurrency called Bitcoin. Fast-forward to a post-pandemic 2022, and the stability of the global financial ecosystem is being forced to adapt to what has followed, as a range of virtual currencies (VCs) gain global relevance. The West's financial hegemony is being threatened by both centralized virtual currencies (especially Chinese and Russian) and decentralized virtual currencies (e.g., Bitcoin and other cryptocurrencies) which have exploded in popularity and viability.

These new financial systems provide a growing, increasingly viable, and capable set of interconnected non-bank financial channels representing an Alternative Payments Ecosystem (APE). These systems may or may never touch the legacy financial system consisting of banks and other traditional financial institutions bound together within and across global borders through messaging networks such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) or the Automated Clearing House (ACH). Any discussion of the APE immediately turns to Bitcoin and other cryptocurrencies, and it's understandable why, as the financial world seemed to change when Satoshi Nakamoto's 2009 paper was released. Yet the APE extends far beyond these blockchain-based systems. The APE story does not begin there nor is it the only story being written.

But let's first consider what Virtual Currencies (VCs) are: digital representations of value, issued by private developers (for now, at least), and denominated in their own unit of account. VCs can be obtained, stored, accessed, transferred, and transacted digitally, and they can be used for whatever purpose the transacting parties have agreed to use them. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (e.g., vouchers, loyalty points) and VCs backed by tangible assets (e.g., precious metals) to a national "fiat" currency and even cryptocurrencies. They are used for transmitting value from one party to another without using the traditional financial system for that payment or transfer. Systems like Tether or WebMoney may be transferring U.S. dollars (USD), Russian rubles, or gold, yet that transfer is often occurring outside of the banking payment processing world. These systems are centralized virtual currencies (CVCs) —centralized because an entity runs them—or decentralized virtual currencies (DVCs) like Bitcoin and other cryptocurrencies which run themselves. These CVCs and DVCs often fall outside of any reporting requirements to western financial regulators.

Despite the popular and policymaking focus on cryptocurrencies, the largest systems found on the APE are not DVCs. By orders of magnitude, the largest are actually China's CVCs which are virtual currency, mobile, or social media payment system hybrids. No bank controls these systems, but rather large corporations. Combined, two major companies – Tencent and Ant Group – processed 294.6 trillion yuan (US$45.6 trillion) in 827.3 billion transactions in 2020, representing significant growth over 2019 (PYMNTS, 2021).

Image source: Stock Photo ID 1039844908 by stockphoto-graf (n.d.). Retrieved from: https://www.shutterstock.com/image-photo/crypto-currency-coin-panorama-set-collection-1039844908

Fungibility

The connective tissues for the APE are the Virtual Currency Exchangers (VCEs) that allow the trade and exchange, often unfettered, of all of the previously mentioned VC examples. CVCs, traditional payment systems, DVCs, and even game or esports credits can be used to purchase Bitcoins and other cryptocurrencies on the U.S.-based Paxful.com and other Peer-to-Peer (P2P) and Over-the-Counter (OTC) exchange sites. Western Union and other remittance systems can be exchanged for VCs on dozens, if not hundreds of VCEs. Most of the VCEs based in the West, such as the U.S.-based Coinbase, expend great effort and expense to meet all the requirements of being a properly certified Money Service Business (MSB). Those outside of the direct reach of relevant regulators are not always so willing to expend the resources and effort to comply with the applicable U.S. Patriot Act and Bank Secrecy Act (BSA) requirements.

MSBs are heavily regulated in the United States, both by federal law and by statutes in 49 of the 50 states. VCEs are considered MSBs if they offer financial services related to cryptocurrencies such as the exchange of CVCs, stored value cards, or the conversion of fiat currencies into digital forms—the exchange or dealing of currency or money transmission. One of the primary reasons for this tight regulatory management of MSBs is tax collection. Despite the IRS' repeated attempts to thwart cryptocurrency's use in tax evasion, which IRS Commissioner Charles Rettig continues to attribute part of the growing US$1 trillion tax gap, the IRS is in desperate need of assistance in the fight against tax evasion (Rappeport, 2021).

The cost of compliance and the lucrative opportunities provided by catering to those who want to be as anonymous as possible have resulted in dozens, even hundreds, of VCEs around the world who intentionally avoid globally accepted Know Your Customer (KYC) standards to combat financial crime. The rise in cryptocurrency use has brought many examples of these exchanges. In 2014, Mt. Gox was the first well-known VCE, and also the first VCE to implode through mismanagement, fraud, and criminality; its failure cost those who entrusted it with their VCs over US$2 billion in stolen Bitcoin by today's valuations (Redman, 2022).

With the rise of the Dark Web came illicit virtual currencies. These did not start with Bitcoin, but rather, well before the first cryptocurrency, there were illicit payment systems serving the drug trade and other illegal enterprises online. Liberty Reserve, a CVC created in 2006, had over one million users when its offices in Costa Rica shut down in 2013 in the first multi-national law enforcement action focused on virtual currency. Over US$8 billion had flowed through Liberty Reserve during its 7-year run (U.S. Department of Justice, 2016). There were other services active on the Dark Web as well in the pre-Bitcoin dark ages, most of them CVCs backed by precious metals (the grandparents to the stablecoins of today) such as CGOLD and Pecunix. E-Gold was the best known of these, and it operated until 2009 when it was forced by law enforcement to shut down due to charges of money laundering. The Silk Road marketplace, selling drugs and weapons and more on the dark web, helped to revolutionize all of this illicit use and propelled Bitcoin to be the lifeblood of the Dark Web. Well over US$1 billion of Bitcoin was used in those transactions on Silk Road (Hern, 2020).

The commonality among these examples is that all of these systems relied on their ability to exchange fiat money into digital "cash." Once converted, they could often be used and traded for one another with impunity.

Before eCash and then Bitcoin, it seemed that no one was watching or that law enforcement simply did not care as there were few direct victims of this illicit dark economy. That has changed, however, and today, there are hundreds of cryptocurrencies, CVCs, stored value cards, Mobile Payment Services (MPS), e-vouchers, and more that are traded on hundreds of exchanges. Some even have their own blockchain networks, such as Binance Coin (BNB). Stablecoins and other asset-based coins backed by fiat currencies (such as Tether which uses the U.S. dollar as its stable base) are gaining in acceptance and popularity quickly, even amongst criminals and terrorists; the same purported stability that is attractive to the average investor is attractive to these bad actors. In contrast to ordinary cryptocurrencies, because these are said to be pegged to the value of reserved fiat currencies, these coins have a lower level of volatility. Some stablecoins are following the path carved out by CGOLD and Pecunix, such as the precious metal-backed coin, ZenGold.

Types of Exchanges

1. Decentralized simply refers to the process of being free from central authoritative control and applies primarily to cryptocurrencies. These decentralized exchanges feature:

- No identity verification — KYC/AML
- Non-custodial payments (payments are never in custody of a third party) — P2P [Peer-2-Peer]
- No fiat support
- Examples such as BTCPayServer, Blockonomics, MyCryptoCheckout fall in this category.

2. Centralized exchanges are run by an entity, usually a company that manages the exchange of funds and often provides a wallet for consumer use. These are all categorized as centralized processors as they have access to users' funds in some form or another. They may include the presence of third-party services where an investment vehicle holds the customer's funds or, in more primitive (and often illegal systems), they can simply be held by one party:

- These may be cryptocurrency only, such as Coinbase, BitPay, Coinpayments, Coingate, or Binance
- CVCs such as QIWI or Perfect Money - or a hybrid such as WebMoney.

KYC is the key to differentiating the basic legitimacy and legality of these systems. Those VCEs that dutifully meet regulatory and Financial Action Task Force (FATF) guidelines in knowing with whom they are transacting are starkly different than those who make it their business not to know. As of June 2021, FATF reported that only 58 out of 128 reporting jurisdictions implemented revised standards (FATF, 2021) and recommended that VCEs (FATF and the U.S. Financial Crimes Enforcement Network [FinCEN] refer to them as Virtual Asset Service Providers [VASPs] although there is no accepted standardization) discontinue connections with companies that operate in jurisdictions where the Travel Rule recommendation has not been implemented. However, as FATF recommendations are not laws or regulations, they are not legally binding. Following a recent survey, just 11% of VASPs (Notabene, 2022) have chosen to stop transferring funds to other brokers in countries which have not yet implemented a version of this law.

Cryptocurrency kiosks or automated teller machines (ATMs) are an extension of the VCE model, allowing a person to exchange VCs and fiat currencies. CVC examples of this are QIWI and WebMoney kiosks that are common in the Russian-speaking world. Cryptocurrency ATMs are found in most cities around the world, usually enabling only the buying of crypto, but with some allowing a bi-directional functionality to also sell cryptocurrencies through the machine. Apart from traditional ATMs, crypto-ATMs have no connection to a bank account. Instead, they are directly connected to the crypto exchanges.

Alternative Payments as a Criminal Backbone

Today, we are seeing the largest thefts of cryptocurrencies occurring in the hacking of VCEs, like Bitfinex. In February 2022, the DOJ announced the arrest of two individuals—not in Malta or Panama, but in Manhattan—for an alleged conspiracy to launder cryptocurrency that was stolen during the 2016 hack of the Bitfinex virtual currency exchange; the loss is presently valued at approximately US$4.5 billion (U.S. Department of Justice, 2022). When calculated in 2017, it was estimated that 5% of all Bitcoin ever issued had been stolen from exchanges which hosted their customer's wallets (Roberts & Rapp, 2017). Many of these thefts (and more recently, with the hacking of smart contracts) are being perpetrated by North Korea.

Cryptocurrency can be used to purchase the tools to penetrate bank's defenses, as well as ransomware as a service (RaaS) from the "consumer"-facing Dark Web sites.

But what are smart contracts? Think of them as a way to automate specific functions or business processes so all parties are informed at once. They are particularly well-suited for use in cryptocurrency transactions. The most recent example was carried out, according to the U.S. Treasury, by the North Korean hackers known as the Lazarus Group, which stole US$625 million in cryptocurrency from the Ronin network (the blockchain backing the Axie Infinity play-to-earn crypto game) (Sharma, 2022). In April, the U.S. Treasury Department sanctioned the wallet address that received the stolen funds and attributed the hack to the Lazarus Group. The weak spot targeted by the hackers was the smart contract that acted as the "bridge" that allowed users to transfer funds between other blockchains and Axie Infinity. These flagged wallet addresses currently contain over US$445 million and sent almost US$10 million to another wallet as of May 2022. North Korea's crypto-haul so far this year is estimated to be about US$1billion, offering a method to evade sanctions (Sharma, 2022).

But it's not just the VCEs that criminals are attacking. Bank, payment processors, retailer and other members of the traditional financial sector possess an array of Personally Identifiable Information (PII) that can be combined with other hacked or stolen information and credentials to enable access to cryptocurrency wallets, bank accounts, and access to loan applications. Dark Web sites allow criminals to mix and match these identity elements to effectively monetize (Kellerman & McElroy, 2021). Cryptocurrency can be used to purchase the tools to penetrate bank's defenses, as well as ransomware as a service (RaaS) from the "consumer"-facing Dark

Web sites. The Criminal-to-Criminal (C2C) transactions are more likely to use CVCs to avoid the tracking inherent in blockchain-based cryptocurrencies. These RaaS variants include ingenious business approaches including the use of affiliate programs to expand the reach of these criminal systems, while expanding their revenue model by taking a portion of the revenue generated by ransom payments for all the attacks made by their RaaS-enabled partners (Kellerman & McElroy, 2021). These payments use Bitcoin or, increasingly, anonymity-enhanced systems (AES) like Monero which avoid the public blockchain and shroud their users from identification.

What is Driving the Use of Alternative Payment Systems?

Major drivers of this revolution of alternative payment systems are not easily apparent in the Western world. We think of the speculative aspects of Bitcoin and other cryptocurrencies, of hackers and ransomware, of convenience. Yet, there is a much larger energy that is driving this change: the direct correlation between financial exclusion and poverty. The lack of access to banking or other financial services constrains the opportunities of over 700 million people, accounting for nearly 73% of all the world's poorest people (IFAD, 2015). Among the financially excluded are migrant workers and their families. These populations send remittance payments to their home countries, providing a significant, steady flow of approximately US$500 billion to these economies (IFAD, 2015). These populations also have no access to financial products like insurance, loans or mortgages. This breeds poverty, and the traditional banking system has done little to include them. In places like Somalia, they have done the opposite, cutting often desperately poor and war-weary people off from the lifeline of remittances from diaspora. Through a process called "de-risking" banks make profit-based decisions to close the accounts for remittance companies like the Somalia-based Dahabshiil, although they are thinly veiled as security or risk decisions. In the Middle East and Africa, 50% of the population is unbanked or underbanked, with South and Central America nearing 38%, Eastern Europe at 33% and Asia Pacific at 24% (Ventura, 2021).

Traditional bank-centric financial systems are under siege as the ground beneath them shifts amid the awaking of the unbanked and underbanked, as well as the burgeoning global middle class. Frequent use of financial sanctions has contributed to this shift as Chinese and Russian new payment systems bypass SWIFT and other western-dominated financial backbones. No longer the domain of FINTECH startups, nor just limited to cryptocurrencies, nation states are playing the "Great Game" on new terrain.

In Kenya, mobile money provider M-Pesa has shown the power of new payment systems to transform economies for the better. This mobile money transfer platform is the great experiment in low-tech FINTECH that has transformed Kenya's economy, and is impacting the rest of East Africa, through connecting simple SMS-based phone communications into their own regional SWIFT network. Beginning with its 2007 launch by Vodafone and Kenya-based telco Safaricom, M-Pesa recently hit the 50 million active users mark in Africa, the largest fintech platform on the continent (O'Gardy, 2021).

M-Pesa allows its customers to instantly send money to each other. For many this was their first and often only access to financial services propelling M-Pesa's fast growth and adoption across the country. Its growth has accelerated financial inclusion across the continent. In Kenya, access to financial services and products has

increased by around 56% between 2006-2019 driven by the availability of mobile money (Central Bank of Kenya, 2019). M-Pesa has also been credited with lifting roughly 2% of Kenyan households out of extreme poverty (Suri & Jack, 2016).

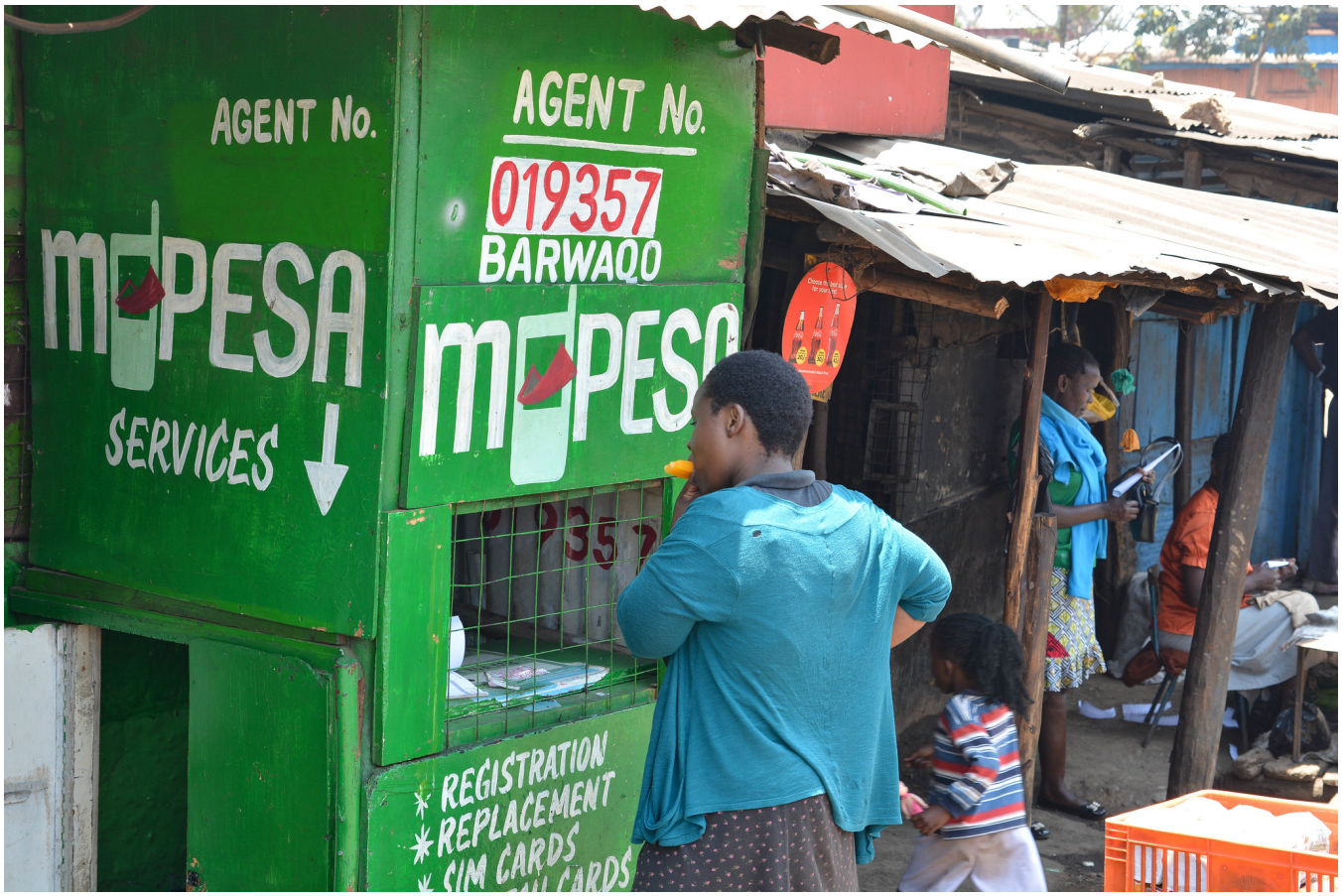

Image source: "M-PESA agent in Kibera, Nairobi" by Fiona Graham / WorldRemit is licensed under CC BY-SA 2.0

Clausewitz's Wallet

From the ashes of World War II, the U.S. dollar emerged as the dominant economic force. As the largest economy and the leader of the Free World, the U.S. was able to construct the dollar-based economic systems that route the world's transactions especially in the post–Bretton Woods world economy. Today, the U.S. is seeing its position erode having now dropped down to the world's second-largest trading partner. The U.S. has been militarily unchallenged since the demise of the Soviet Union and has used its position as a global economic as well as military superpower, using the dollar as a soft power Clausewitzian geo-political weapon. Clausewitz would clearly include in his "sum of the tools of statecraft", attaining financial dominance over an enemy (Miyata, 2021). Dominance in today's global financial system is enjoyed by the U.S. as the world's reserve currency, enabling leveraging the "payment rails" which facilitate cross-border financial transfers. The U.S.' influence on the SWIFT

network allows it to monitor global financial transactions and to wield the cudgel of economic sanctions, perhaps too frequently, to deter any challenges that may harm its national interests.

These sanctions can have serious impacts on the economies of countries affected by them. Once cut off from SWIFT's network, it becomes extremely difficult for a country to trade with the rest of the world. One recent example is Iran, which lost US$150 billion worth of revenue as a result of U.S. sanctions. Cross-border transactions made over payment rails like SWIFT are nearly always settled in dollars or involve a U.S. financial institution at some point. This payment rail dominance, combined with other dollar-based advantages, gives the U.S. a significant advantage over China, now the world's leading trading partner, as a tool for sanctions on Chinese companies, blocking transaction settlements through SWIFT (Reuters, 2020).

As of December 2021, countries sanctioned by the U.S. include Afghanistan, the Balkans, Belarus, Burma, Central African Republic, China, Cuba, Democratic Republic of Congo, Ethiopia, Hong Kong, Iran, Iraq, Lebanon, Libya, Mali, Nicaragua, North Korea, Russia, Somalia, Sudan and Darfur, South Sudan, Syria, Venezuela, Yemen, and Zimbabwe (OFAC, 2022). It is also noteworthy that many of the U.S. sanctions are unilateral rather than multilateral, enforcing crippling sanctions on countries without significant multilateral support. This cross-border financial foundation may not be as stable as the U.S. believe, and many countries harbor desires for alternatives.

With billions of people around the world already embracing new payment systems, or ready to move to non-Western dominated systems, dramatic change is possible, perhaps likely. The internet age has provided the evidence and the vehicle for financial system disruption, disintermediation, and a reshuffling of traditional relationships.

The Black Swan...or is it a Gray Rhino?

A "gray rhino" is a highly probable, high-impact yet neglected threat: kin to both the elephant in the room and the improbable and unforeseeable black swan. Gray rhinos are not random surprises but occur after a series of warnings and visible evidence. The fall of the Soviet Union, Climate Change, the 1928 and 2008 economic crashes, and even the advent of the internet age all exhibited signals well in advance heralding those events. We are now seeing a global financial great rhino in large part as a response to the U.S. government's threats to disconnect Russia from the SWIFT system. Russia has developed its own financial messaging system, called the System for Transfer of Financial Messages (SPFS) and banking card system (MIR). Russia's Deputy Foreign Minister, Alexander Pankin, stated that Russia echoes China's concerns around SWIFT being used as a geopolitical weapon by the West and that there is a need to modernize their payment methods (Bansal & Singh, 2021). Recently, Russia has also launched efforts to integrate SPFS and MIR with China's CIPS and UnionPay counterparts, as well as integrating SPFS across the Eurasian Economic Zone. China has built CIPS in twenty-five major countries, including the U.S., Singapore, Britain, France, Germany, South Korea, Russia, and Japan (Bansal & Singh, 2021). Yet risks to the financial system cut both ways, the German daily Die Welt wrote on February 27, 2022. "CIPS already handles US$50 billion of daily transactions. That is considerably less than the US$400 billion of transactions that pass every day through SWIFT, but CIPS volume has increased rapidly," the German

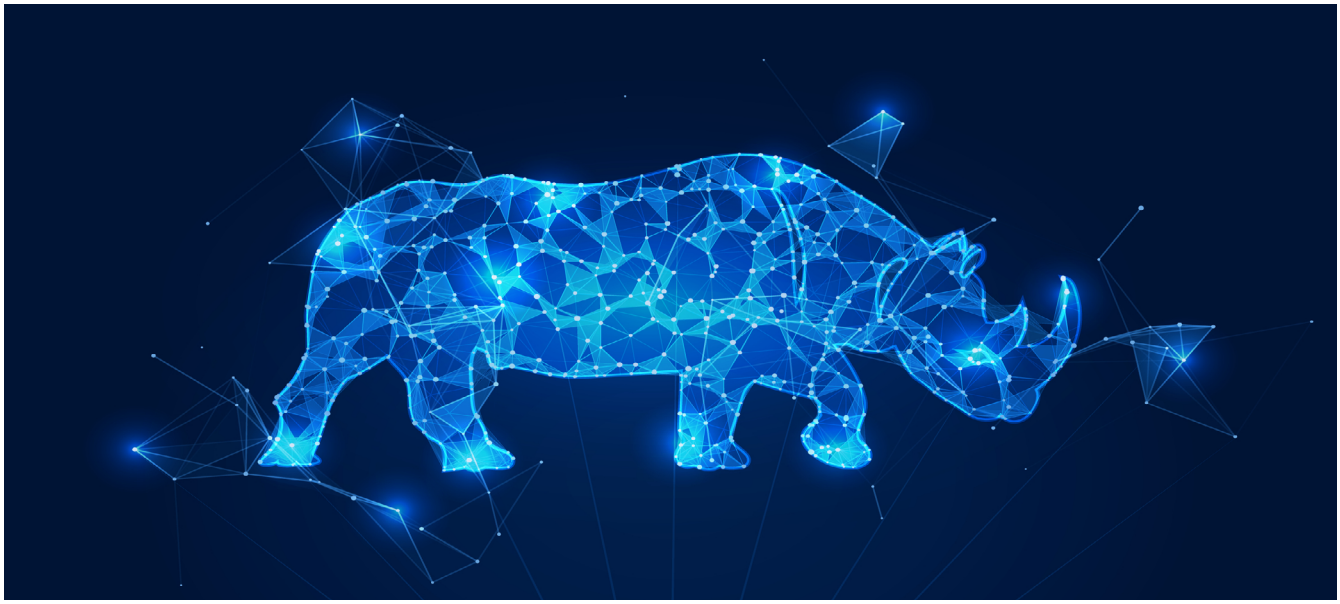

Image source: Stock Vector ID: 1688047045 by Maxim Gaigul (n.d.). Retrieved from: https://www.shutterstock.com/image-vector/rhino-hologram-rhinoceros-made-polygons-triangles-1688047045

newspaper reported. However, Die Welt concluded, "If Russia and China linked their systems and offered an alternative to other authoritarian states, this could threaten American domination of financial markets" (Reuters, 2022a).

Many members of the Chinese elite—even longtime advocates of market reform and economic opening—see a dark future for U.S.-China relations—and are increasingly focused on America's global financial hegemony as a long-term risk for their country. With China's growing wealth and prominence, they see the global economy as a legitimate area for defending their sovereignty and even as a way to retaliate (Gewirtz, 2019). The reality of financial war has been thrust upon the West in 2022 by Russia's return to war as a political tool resulting in the declaration, explicit or not, of near total economic war by the West. Notably absent from this economic coalition has been China, Brazil, India, and South Africa (the BRIC bloc) along with other countries unwilling to criticize their current or past patron. Will this be the catalyst to drive their adoption of an alternative to SWIFT and other Western-dominated financial networks?

On April 9th, 2022, Russia's Finance Minister, Anton Siluanov, told a ministerial meeting with BRICS, that they should integrate their payment systems. Sanctions have exacted a heavy toll on Russia's economy, losing access to more than US$600 billion of its gold and foreign exchange reserves (Reuters, 2022a). In 2017, Russia approved a cryptocurrency regulation framework, which would allow the government to "levy a 13% tax on individuals and organizations who attempt to trade their 'cryptorubles' for a flat currency but cannot demonstrate that the coins were obtained legally" (Kellerman, 2017). This policy reflects the Russian government's de-facto policy to profit from money laundering and other financial crimes as long as the victims are not Russian speakers.

Russia's political ruling class is indivisible from the oligarchs who have profited under Putin's rule. As much of the world has turned against Russia and imposed sanctions, increasing attention has been paid to the capital flight as they attempt to leak their funds out of the country. Without access to SWIFT and other sanctioned financial channels, these fund have sought out the weak spot in the global financial monitoring systems: decentralized

exchanges and the purchase of Non-Fungible Tokens or privacy coins (Gromek, 2022). Those are not their only options though: WebMoney, Yandex Money and Perfect Money are three of the larger Russian CVCs which enable money transfers around the world. In 2019, Sberbank said that WebMoney had joined its instant transfer ecosystem, allowing clients to connect their Sberbank accounts showing the degree of integration into the Russian banking system (Finextra, 2019). That integration was strangely interrupted on February 11th, 2022, when Russian authorities halted the ability to trade in rubles by revoking the license of their settling bank (Tass, 2022).

As of March 2022, Russia is actively trying to bypass SWIFT with its System for Transfer of Financial Messages (SPFS) developed by the Central Bank of Russia. SPFS has over 399 users, including more than 20 Belarusian banks, the Armenian Arshidbank, and the Kyrgyz Bank of Asia. Subsidiaries of large Russian banks in Germany and Switzerland have access to SPFS although this may change due to sanctions. Russia's central bank will stop disclosing the names of those participating in its alternative to the SWIFT payment system. Some Russian banks have been banned from the SWIFT banking system as part of the sweeping sanctions against the country over the Ukraine war. The ban has hampered cross-border transactions for Russia's trade and financial systems, isolating the country economically. The SPFS network extends beyond most Russian banks and now includes more than 50 foreign organizations (Reuters, 2022b).

Banks from Germany, Switzerland, France, Japan, Sweden, Turkey, and Cuba were among those connected to SPFS, according to a March 2022 report from Coface, a French credit insurer (Coface Economic, 2022). Until there was such a threat of being cut off from SWIFT, foreign partners were not in much of a rush to join, but now we expect their readiness to be greater," Nabiullina said of SPFS. An example is the Indian government's consideration of a Russian proposal to use the SPFS for payments in rubles, Bloomberg reported in March. India has been buying cargoes of cheap Russian oil amid international sanctions and boycotts of products from the energy powerhouse. Russian oil accounted for just 2% of India's total imports in 2021(Bloomberg News, 2022). Russia is currently negotiating with China to join the system. This alternative financial infrastructure enables Russian corporations and individuals to retain some access, albeit limited, to global markets despite sanctions (Liu & Papa, 2022). Should the other BRICS join SPFS and MIR, a viable, but limited alternative would exist with access to more than 3.23 billion people, which is over 40 percent of the world population.

This gray rhino may have a gray dragon close behind. As of end January 2022, there were 1,280 participants in China's Cross-border Interbank Payment Systems (CIPS), representing 103 countries and regions around the world.

However, this gray rhino may have a gray dragon close behind. As of end January 2022, there were 1,280 participants in China's Cross-border Interbank Payment Systems (CIPS), representing 103 countries and regions around the world. Participants include 11 foreign banks including some of the World's largest (DBS, Citibank, JPMorgan, Standard Chartered, HSBC, Deutsche, BNP Paribas, ANZ, MUFJ, Mizuho, and SMBC), 934 companies in Asia (541 companies in China), 159 companies in Europe, 43 companies in Africa, 29 companies in North America, 23 companies in Oceania, and 17 companies in South America. At least 23 Russian banks are connected to CIPS (as indirect participants), and Russia will have no trouble doing business in yuan through CIPS. Moreover, major

Russian private and state-owned institutions have only been accepting yuan payments in recent years. For instance, in September 2021, Gazprom switched from accepting U.S. dollar payments to yuan payments for aviation fuel. Although it has more participants than SPFS, its ubiquity is also not comparable to SWIFT (Coface Economic, 2022).

China has been working on an alternative to traditional "payment rails" as well. They have been working on their own digital currency since 2014, leading the world in efforts to field a large-scale Central Bank Digital Currency (CBDC). In 2016, the People's Bank of China (PBoC) successfully built the digital yuan prototype (e-CNY). At the end of 2017, the PBoC started the digital yuan research and development project, which saw participation from large commercial banks, internet companies, and telecommunications players. May of 2019 witnessed the launch of a large-scale pilot spanning four major cities in China. This was the first scale CBDC pilot in the world (Bansal & Singh, 2021).

In January 2022, the PBOC launched an app to allow users in 10 areas, including the major cities of Shanghai and Beijing, to sign up and use the e-CNY. The two dominant payment systems in China are Tencent's WeChat Pay and Alipay, which is run by Alibaba affiliate, Ant Group. Tencent announced that it would support the e-CNY in its WeChat Pay and Alipay which have over 1 billion users (Kharpal, 2022). The potential convenience of the e-CNY could extend WeChat Pay and Alipay's reach as the digital yuan can be used to make transactions without an internet connection, through proximity reading only. This could prove to be the digital yuan's most attractive feature, as it gives it helps digital payments act more like cash. As part of the e-CNY in Beijing, ATMs have been added to the city that convert the digital yuan to cash and vice versa (Zhao, 2021).

Many Other Central Banks are on the Move Too

Nine countries have launched CBDCs, another fifteen are in pilot stages, and sixteen are in development; the U.S. is NOT one of them. The Bahamas (their CBDC is named "Sand Dollar") along with the eight countries of the Eastern Caribbean Central Bank (ECCB) are among the first rolling out their CBDCs. The latter's pilot involves a securely minted and issued digital version of the Eastern Caribbean (EC) dollar, called DCash. Through this pilot the ECCU hopes to build resiliency from climate and political adversities, and create a more competitive economic system as well as broadening financial inclusion (ECCB, n.d.). This is, in part, to come up with alternatives to the correspondent banking which has been drying up in the region for over a decade due to a few Anti Money Laundering (AML) issues, and lingering perception issues, but mostly volume-to-profit problems that make the big banks not want to bother. This could be considered a response to the general de-risking trend from commercial banks.

Currently, the U.S. can monitor and regulate most global digital payment flows of dollars, but new payment systems could limit the ability of policymakers to track cross-border money flows. In the long term, the absence of U.S. leadership and standards-setting will have geopolitical consequences, especially if China maintains its first-mover advantage in the development of CBDCs. Considering the growing alternative payments ecosystem leadership shown by China (remember the US$60 trillion+ transaction value of Alipay and WePay), if combined

with their development of a viable CBDC, eventually a real financial (and law enforcement) nightmare could confront the West.

This battle is nowhere near lost, and indeed is just beginning. In a talk given to the Bank of England conference on "Central Banking and Fintech" in 2017, then head of the IMF Christine Lagarde (now the President of the European Central Bank) said that virtual currencies could actually become more stable than fiat currencies. She says, "for instance, they could be issued one-for-one for dollars, or a stable basket of currencies" while also leveraging the benefits of securely managed digital identities(Lagarde, 2017). However, in 2022, the current IMF Managing Director Kristalina Georgieva, has a less rosy vision, fraught with concern for "a world that could fragment into 'economic blocs', creating obstacles to the cross-border flow of capital, goods, services, ideas, and technologies" (Georgieva, 2022).

The respected payment guru David Birch shared his perspective that technology will be the key to providing secure transactions privately. Blockchain-based systems, "in particular, privacy-enhancing technology gives us the apparently paradoxical ability to keep private data on a shared or public ledger, which I think will form the basis of new financial institutions" (Birch, 2017).

Managing the Threat while Nurturing the Opportunity

"Our regulatory frameworks should be designed to support responsible innovation while managing risks—especially those that could disrupt the financial system and economy," U.S. Treasury Secretary Janet Yellen said recently in a speech on digital asset policy delivered at American University, arguing that new regulatory frameworks will be needed to manage those risks (Lawder, 2022).

U.S. President Biden's recent Executive Order requires the U.S. Department of the Treasury and U.S. Department of Commerce and other agencies to prepare reports on "the future of money" and the role cryptocurrencies will play (The White House, 2022). The internet, however, is not SWIFT. Regulation of the massive APE is not going to be as effective globally as regulators hope. With events in Ukraine driving a wedge into familiar Cold War fault lines, a schism is growing between familiar payment systems and new ones specifically created as an alternative to avoid regulation and oversight by the West.

The internet, however, is not SWIFT. Regulation of the massive APE is not going to be as effective globally as regulators hope.

Current financial intelligence systems rely upon signals being generated and detected through the network of financial institutions, including MSBs, submitted in the form of Suspicious Activity Reports (SARs). The efficacy of the SAR reporting system, and the ability of institutions like the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) to manage the flood of SARs (more than 2 million per year) limits the system's effectiveness, especially to detect new or unusual signals (Weiner Brodsky Kider PC, 2020). The SARs system also does not actively encourage the investigation

of secondary or tertiary connections that may be criminal usage indicators – especially in virtual currency use. While public blockchain intelligence systems like Chainalysis and CipherTrace are beginning to do "peel-chain" analysis where cryptocurrencies are exchanged for others to obfuscate their origins or usage, they do poorly when assessing where the money goes after conversion into a privacy coin, CVC, or other APS.

To understand where the money flows, as it moves through, into and out of the Alternative Payments Ecosystem (APE), a new Financial Open Source Intelligence (FOSINT) approach is required. Traditional follow-the-money approaches often miss the role played by the APE, especially when executed without a generalized understanding of this varied and constantly morphing set of companies and services.

Taming the APE: A Call to Action

As the use of the Alternative Payments Ecosystem (APE) continues to increase and diversify, so does the need to both encourage its development while enhancing systemic transparency. Our institutional abilities to expose adversarial and criminal applications require innovation. This includes not only the tech and financial industries, but policymakers and regulators alike. Incentives must be created for fintech firms to limit their 'operational risks' through the implementation of KYC/AML protocols. Incentives, or conversely disincentives, should also be created to limit the de-risking of APS such as remitters, as these systems provide vital lifelines to beleaguered and impoverished populations from Somalia to Ukraine to Guatemala.

The U.S. needs to follow our private sector's global technology leadership by setting the standards for the APE in the international arena. Regardless of whichever direction the U.S. government takes the digital dollar, CBDCs, stablecoins, eCash, or other new payment technologies, it cannot wait to engage the world through international organizations. To wait for a domestic decision may mean ceding leadership of FATF, waiting for the BRICs to create a viable alternative to SWIFT, or ignoring arenas where China and others are dominating (such as mobile or CVCs) and thus setting the standards that might be used for law, regulation, interoperability, digital illiberalism, and integrated digital payment systems. Instead, this leadership should extend beyond regulations, law enforcement, and Counter Threat Finance (CTF) to using the APE to enable financial inclusion. Offering greater support to the World Bank's Financial Inclusion Global Initiative (World Bank Group, 2021) through the U.S. Agency for International Development (USAID) would be a good place to start.

When we do need to create laws and regulations to manage the illicit use of the APE, it is critical that legislators be better educated and have permanent committee staff who are expert on these topics. With bad actors and adversaries gaining leverage quickly, Congress must be serious about the risks and opportunities of the APE, in part by committing to understanding the terms and embracing realistic solutions to the risks of this evolving financial system. These include weaknesses with investor and consumer protection and the ongoing or potential abuse of the APE by our adversaries, including criminals and nation-states. Differences between political parties and jurisdictional debates (e.g., whether a cryptocurrency is a security, a deposit, or a commodity) have resulted in a constant, but unproductive, legislative churn.

Authorities for regulatory agencies need to be modernized to enforce the existing laws, as well as prepare for new ones that need to be written. Many current laws and regulations were written for traditional banking systems (SWIFT and ACH) and are ill-suited for managing the APE. Blocking actions by FinCEN, for example, can only be applied to "correspondent banking or payable-through accounts." Technically, as it currently stands, its outdated special measures authorities cannot be applied to a VCE, remittance system, any kind of MSB, or other cross-border transfer system if and when FinCEN and partner agencies find an entity to be a "Primary Money Laundering Concern." Modernized authorities like this are critical if our regulators are to be effective in oversight and engagement of the APE.

The following are possible ways to enable the U.S. to better cope with the threat and opportunity provided by the APE:

- Education of law enforcement investigators and intelligence analysts in APE and how it integrates with criminal and adversary systems. Regulators including the Security and Exchange Commission (SEC), the Financial Crimes Enforcement Network (FinCEN), as well as policy makers in various Executive Agencies, and the US Congress must understand these issues better as well. This should also include creating a common APE lexicon across agencies, law, and regulation.
- Financial Open Source Intelligence (FOSINT) platforms must be created and synthesized with existing OSINT tools. These platforms must look beyond blockchain analysis systems for cryptocurrencies and integrate with all available data on non-public blockchain-based VCs, including CVCs, MPSs, and Remitters. This would include creating new Internet collection and analysis tools and combine with other data (e.g., law enforcement data, SARs, or proprietary financial institution data).
- Regulations should be modernized to support the Financial Action Task Force (FATF) prioritization of including VCEs in Country Scorecards. These regulations should also encourage policy and incentives for banks to end de-risking practices which hurt the poor and drive illicit payments further underground.
- Government FININT coordination through the creation of a "National Counter Threat" capability through the Office of the Director of National Intelligence (ODNI). By providing a central point for collaboration and data sharing this capability would include all aspects of national intelligence and law enforcement. This new function could be part of a modified National Counter Terrorism Center (NCTC) with a mission to examine the intersection of crime, terrorism, and nation state threats across all the ODNI Centers (NCTC, CTIIC, NCPC, NCSC).

Without an integrated and comprehensive approach, the APE will continue to grow and strengthen. If that day comes—and it could arrive sooner than most think—the West's ability to dominate the world's financial sphere of soft power will lessen. Without action, our ability to live in a rules-based financial system will fade with it.

About the Author

The opinions expressed here are those of the author and do not represent the Wilson Center.

Scott Dueweke, Global Fellow, The Wilson Center's Science and Technology Innovation Program

Scott Dueweke is an expert on *identity*, the *blockchain*, the *dark web* and *alternative payment systems* at Leidos and in 2021 was appointed as a Global Fellow at the Wilson Center. He has advised senior leadership within financial institutions, the U.S. government, as well as international law enforcement. In 2012 he sparked the Silk Road dark market investigation by the US Secret Service while presenting at a EUROPOL money laundering conference. Mr. Dueweke has provided training on digital identity, the blockchain and other digital value systems to non-profits, corporations and governments, including Citigroup, the National Health Care Innovation Summit, the US Intelligence Community, FBI, Department of State, USAID, INTERPOL, EUROPOL, and the UNODC to name a few. Through his knowledge of the Dark Web and anonymous payments he supported Operation Underground Railroad in their efforts to stop global child sex slavery rings. In June 2018 Mr. Dueweke testified on the role of anonymous payment systems in allowing foreign influence on US elections, and in 2017 on cybercrime before the House Banking Committee.

Mr. Dueweke has provided public and private sector clients an understanding of identities and alternative payment systems, both risks and rewards. In 2015 he provided *Anti-Money Laundering (AML)* and *Counter Terrorism Funding (CTF)* training for more than 40 countries' Financial Intelligence Units (FIU) including sessions in the Philippines, Turkmenistan, Kazakhstan and Turkey. He helped lead, along with the US Department of State's Counter-Terrorism Bureau and USAID, the New Payment Systems Workshop at the Asia Pacific Economic Cooperation (APEC) Senior Leaders Working Group at Subic Bay, Philippines.

He began his career with the U.S. Agency for International Development, where Mr. Dueweke contributing to the Armenian earthquake and Hurricane Gilbert responses. He also co-founded Freedom Flight International in the mid-1990s where, working with the U.S. Coast Guard, his organization flew private aircraft over the Florida Straits to assist the rescue of Cuban rafters as profiled in the book, "Dying to Get Here: A Story of Coming to America".

References

Bansal, R & Singh, S. (2021, August 31). China's Digital Yuan: An Alternative to the Dollar-Dominated Financial System. Carnegie India. Retrieved May 22, 2022, from https://carnegieendowment.org/files/202108-Bansal_Singh_-_Chinas_Digital_Yuan.pdf

Birch, D. G. W. (2017, October 3). Don't listen to me, listen to Christine Lagarde. 15Mb. Retrieved May 22, 2022, from https://blog.dgwbirch.com/?p=211

Bloomberg News. (2022, April 19). Russia Touts SWIFT Alternative, But Will Keep Its Members Secret. Bloomberg News. Retrieved May 22, 2022, from https://www.bloomberg.com/news/articles/2022-04-19/russia-touts-swift-alternative-but-will-keep-its-members-secret

Coface Economic (2022, March). Economic Consequences of the Russian-Ukraine conflict: Stagflation ahead. Coface Economic. Retrieved May 22, 2022, from https://www.cofacegk.no/ResourceServlet/i70c5f1f-7a4c41ce927243eff6e2222c

Central Bank of Kenya. (2019, April 14). 2019 FinAccess Household Survey. Central Bank of Kenya. Retrieved May 22, 2022, from https://www.centralbank.go.ke/uploads/financial_inclusion/1035460079_2019%20FinAcces%20Report%20(web).pdf

ECCB. (n.d.). About the Project. Eastern Caribbean Central Bank. Retrieved May 22, 2022, from https://www.eccb-centralbank.org/p/about-the-project

FATF. (2021, June 25). Outcomes FATF plenary, 20-25 June 2021. Financial Action Task Force (FATF). Retrieved May 22, 2022, from https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2021.html

Finextra. (2019, February 22). Sberbank customers can now transfer money from their cards using recipient phone number. Finextra Research. Retrieved May 22, 2022, from https://www.finextra.com/pressarticle/77372/sberbank-customers-can-now-transfer-money-from-their-cards-using-recipient-phone-number

Georgieva, K. (2022, May 10). Confronting fragmentation: How to modernize the international payment system – Speech. Eurasia Review. Retrieved May 22, 2022, from https://www.eurasiareview.com/10052022-confronting-fragmentation-how-to-modernize-the-international-payment-system-speech/

Gewirtz, J. (2019, December 17). Look out: Some Chinese thinkers are girding for a "Financial War". POLITICO. Retrieved May 22, 2022, from https://www.politico.com/news/magazine/2019/12/17/look-out-some-chinese-thinkers-are-girding-for-a-financial-war-086610

Gromek, M. (2022, April 27). Wrestling russia on the blockchain - six most likely sanctions to be imposed. Forbes. Retrieved May 22, 2022, from https://www.forbes.com/sites/michalgromek/2022/04/27/wrestling-russia-on-the-blockchainsix-most-likely-sanctions-to-be-imposed/?sh=a176803e1885

Hern, A. (2020, November 4). Silk road bitcoins worth $1bn change hands after seven years. The Guardian. Retrieved May 22, 2022, from https://www.theguardian.com/technology/2020/nov/04/silk-road-bitcoins-worth-1bn-change-hands-after-seven-years

IFAD. (2015, September). The use of remittances and financial n=inclusion. International Fund for Agriculture Development (IFAD). Retrieved May 22, 2022, from https://www.ifad.org/documents/38714170/40187309/gpfi.pdf/58ce7a06-7ec0-42e8-82dc-c069227edb79

Kellerman, T. (2017, November). Follow the Money: Civilizing the Darkweb Economy. Wilson Center. Retrieved May 22, 2022, from https://www.wilsoncenter.org/sites/default/files/media/documents/publication/dfp_follow_money_kellermann.pdf

Kellerman, T. & McElroy, R. (2021). Modern Bank Heists 4.0. VMware. Retrieved May 22, 2022, from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists-2021.pdf

Kharpal, A. (2022, January 11). China is pushing for broader use of its digital currency. CNBC. Retrieved May 22, 2022, from https://www.cnbc.com/2022/01/11/china-digital-yuan-pboc-to-expand-e-cny-use-but-challenges-remain.html

Lagarde, C. (2017, September 29). Central Banking and Fintech-A Brave New World? IMF. Retrieved May 22, 2022, from https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

Lawder, D. (2022, April 7). Yellen says U.S. crypto rules should support innovation, manage risks. Reuters. Retrieved May 22, 2022, from https://www.reuters.com/business/finance/yellen-says-us-crypto-rules-should-support-innovation-manage-risks-2022-04-07/

Liu, Z. Z., & Papa, M. (2022, May 18). The Anti-Dollar Axis. Foreign Affairs. Retrieved May 22, 2022, from https://www.foreignaffairs.com/articles/russian-federation/2022-03-07/anti-dollar-axis

Miyata, F. (2021, March 26). The grand strategy of Carl von Clausewitz. War Room - U.S. Army War College. Retrieved May 22, 2022, from https://warroom.armywarcollege.edu/articles/grand-strategy-clausewitz/

Notabene. (2022). The "Sunrise Issue" of the Crypto Travel Rule. Notabene. Retrieved May 22, 2022, from https://notabene.id/sunrise-issue#:~:text=The%20FATF%20recognizes%20the%20compliance,at%20which%20their%20counterparties%20operate.

OFAC. (2022). Sanctions Programs and Country Information. U.S. Department of the Treasury. Retrieved May 22, 2022, from https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

O'Gardy, V. (2021, September 7). M-Pesa hits the 50 million mark. Developing Telecoms. Retrieved May 22, 2022, from https://developingtelecoms.com/telecom-technology/financial-services/11851-m-pesa-hits-the-50-million-mark.html

O'Neill, A. (2021, November 26). Total population of the BRICS countries 2026. Statista. Retrieved May 22, 2022, from https://www.statista.com/statistics/254205/total-population-of-the-bric-countries/#:~:text=In%202021%2C%20it%20is%20estimated,percent%20of%20the%20world%20population.

PYMNTS. (2021, September 24). China Widens Mobile Payments antitrust probe. PYMNTS.com. Retrieved May 22, 2022, from https://www.pymnts.com/antitrust/2021/china-widens-mobile-payments-antitrust-probe/

Rappeport, A. (2021, April 13). Tax cheats cost the U.S. $1 trillion per year, I.R.S. chief says. The New York Times. Retrieved May 22, 2022, from https://www.nytimes.com/2021/04/13/business/irs-tax-gap.html

Redman, J. (2022, April 4). Bitcoin cold case: The tale of the dormant wallet with close to 80,000 BTC from Mt Gox. Bitcoin News. Retrieved May 22, 2022, from https://news.bitcoin.com/bitcoin-cold-case-the-tale-of-the-dormant-wallet-with-close-to-80000-btc-from-mt-gox/

Reuters. (2020, July 29). Chinese banks urged to switch away from Swift as U.S. sanctions loom. Reuters. Retrieved May 22, 2022, from https://www.reuters.com/article/us-china-banks-usa-sanctions/chinese-banks-urged-to-switch-away-from-swift-as-u-s-sanctions-loom-idUSKCN24U0SN

Reuters. (2022a, April 9). Russia calls for integrating BRICS payment systems. Reuters. Retrieved May 22, 2022, from https://www.reuters.com/business/finance/russia-calls-integrating-brics-payment-systems-2022-04-09/

Reuters. (2022b, April 19). Russia Central Bank will not name banks linked to swift alternative. Reuters. Retrieved

May 22, 2022, from https://www.reuters.com/world/europe/russia-central-bank-will-not-name-banks-linked-swift-alternative-2022-04-19/

Roberts, J. J., & Rapp, N. (2017, November 25). Exclusive: Nearly 4 million bitcoins lost forever, new study says. Fortune. Retrieved May 22, 2022, from https://fortune.com/2017/11/25/lost-Bitcoins/

Sharma, R. (2022, April 16). North Korean attackers snipes Axie Infinity Gamers in $620 million burgle: FBI. The Coin Republic. Retrieved May 22, 2022, from https://www.thecoinrepublic.com/2022/04/16/north-korean-attackers-snipes-axie-infinity-gamers-in-620-million-burgle-fbi/

Suri, T., & Jack, W. (2016, December 9). The long-run poverty and gender impacts of Mobile Money. Science, 354(6317), 1288–1292. https://doi.org/10.1126/science.aah5309

Tass. (2022, February 11). WebMoney halts operations with Russian wallets from February 11th. Tass. Retrieved May 22, 2022, from https://tass.com/economy/1401755?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

The White House. (2022, March 9). Executive order on ensuring responsible development of Digital assets. The White House. Retrieved May 22, 2022, from https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

U.S. Department of Justice. (2016, August 10). Liberty Reserve founder sentenced to 20 years for laundering hundreds of millions of dollars. The United States Department of Justice. Retrieved May 22, 2022, from https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars

U.S. Department of Justice. (2022, February 8). Two arrested for alleged conspiracy to launder $4.5 billion in stolen cryptocurrency. The United States Department of Justice. Retrieved May 22, 2022, from https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

Ventura, L. (2021, February 17). World's most unbanked countries 2021. Global Finance Magazine. Retrieved May 22, 2022, from https://www.gfmag.com/global-data/economic-data/worlds-most-unbanked-countries

Weiner Brodsky Kider PC. (2020, October 13). FinCEN's data shows continued increase in SAR filings. JD Supra. Retrieved May 22, 2022, from https://www.jdsupra.com/legalnews/fincen-s-data-shows-continued-increase-58306/

World Bank Group. (2021, March 10). Financial Inclusion Global Initiative (FIGI). World Bank. Retrieved May 22, 2022, from https://www.worldbank.org/en/topic/financialinclusion/brief/figi

Zhao, W. (2021, February 18). Beijing's new digital yuan test features ATMs that convert digital currency to cash. The Block. Retrieved May 22, 2022, from https://www.theblockcrypto.com/post/95266/beijing-digital-yuan-cash-

WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

The Wilson Center, chartered by Congress in 1968 as the official memorial to President Woodrow Wilson, is the nation's key non-partisan policy forum for tackling global issues through independent research and open dialogue to inform actionable ideas for the policy community.

THE SCIENCE AND TECHNOLOGY INNOVATION PROGRAM (STIP)

The Science and Technology Innovation Program (STIP) brings foresight to the frontier. Our experts explore emerging technologies through vital conversations, making science policy accessible to everyone.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

The Wilson Center

- www.wilsoncenter.org
- wwics@wilsoncenter.org
- facebook.com/woodrowwilsoncenter
- @thewilsoncenter
- 202.691.4000

STIP

- www.wilsoncenter.org/program/science-and-technology-innovation-program
- stip@wilsoncenter.org
- @WilsonSTIP
- 202.691.4321

Wilson Center

Science and Technology Innovation Program