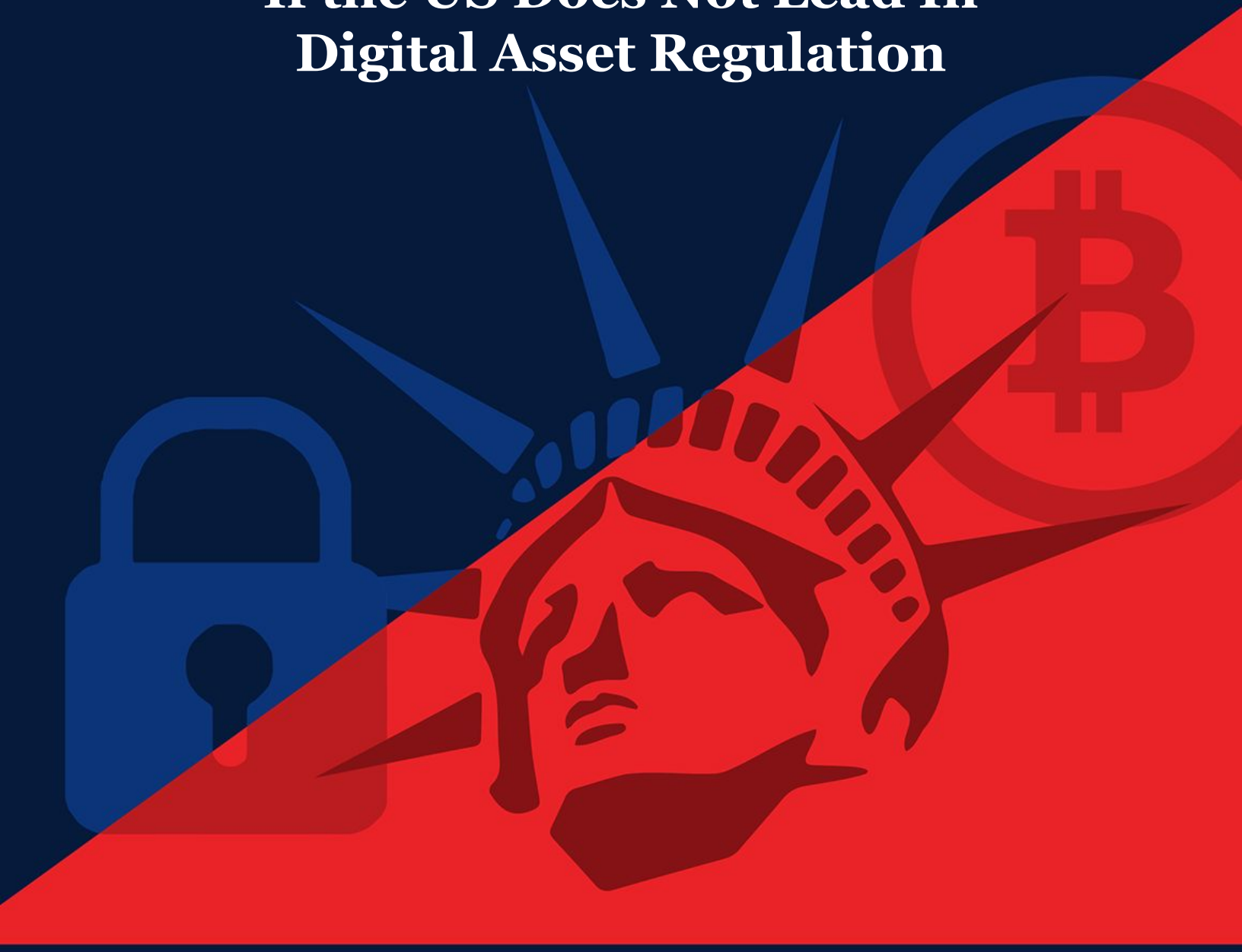
P3 NETWORK

National Security Implications If the US Does Not Lead In Digital Asset Regulation



OCT 22'
EDITION

Contributors

Pete Sessions
Congressman for Texas' 17th District
U.S. House of Representatives

Pete has served over 2 decades in the House as a conservative national leader fighting for American industry, innovation, and free-market solutions.

Jeremy Sheridan
SVP, Regulatory Affairs
Prime Trust

Jeremy was former Assistant Director of the Secret Service with a proven track record of expertise in compliance, regulatory affairs, and strategy development.

Kathy Kraninger
Vice President Regulatory Affairs
Solidus Labs

Kathy was Former Director, U.S. Consumer Financial Protection Bureau (CFPB) until January of 2021. She also served in the White House under the Trump administration in the Office of Management and Budget.

Scott Richards
Vice President
Fluent Finance

Scott is a highly experienced political and economic development consultant. He has organized trade delegations, structured business development strategies for global corporations, and has served as a media and information technology strategist for government and private sectors.

Published by P3 Network

Special thanks to Jonathan Leigh, Adrien Yule, Joanna Yela, Andres Olsen-Rodriguez, Josy Jaramillo, Anthony Vavra, and the entire P3 Network team for their hard work and dedication.

Table of Contents

Contributors	1
P3 Network Lead Sponsor Fluent Finance – the Future of Stablecoins	2
Quotes From Our Speakers	4
What are the Implications of a Nation Failing to Adopt Blockchain Technology and Innovation in an Increasingly Multipolar World?	5
How do we Understand the Transnational Threats and Crimes that Terrorist Organizations Pose?	9
What Vulnerabilities Exist From Adversarial Phishing & Market Manipulation Compared to Crypto?	12
National Security Legislation in Congress	14
Recommendations to Members of Congress	18
Become a Member of the P3 Network	Back

Visit https://www.p3network.com to learn more.

Click here to watch the full panel on National Security

Sponsoring Partner

Fluent Tackles Regulatory Compliance with US+ Stablecoin Launch

Building a cryptocurrency can be an arduous endeavor. While the concept of digital money is simple, maintaining its value and stability is where things get challenging. However, even the basic benefits of cryptocurrency makes the effort well worth the effort; instant payments, conditional smart contracts, and **traceable** records not only reduce the costs of transactions, but also offer the ability to monitor and manage financial activities with pinpoint accuracy. The potential of digital money is most evident in stablecoins, which are simply cryptocurrencies that are paired in value, or "pegged," to a fiat currency or other asset.

When Fluent set out to build their flagship US+ stablecoin, it had to be collateralized, auditable, and **immune** to any incident that might cause a sudden exodus of users leading to a "de-peg" event. Fluent overcame these issues by creating a federation of banks, which removes the possibility of a single point of failure — if any banking partner experiences liquidity issues, the other partners step in to help course correct. Additionally, by implementing a programmatic set of rules, or "protocol," Fluent ensures that each US+ stablecoin minted has a physical dollar or more behind it.

Having a de-risked stablecoin is one important part of the equation, but ensuring its usage remains lawful is just as critical. Embedded in the Fluent process is a powerful "Know Your Customer" (KYC) system that can **validate** any account holder's identity. The KYC mechanism helps Fluent reduce the risk of illicit financial trade and money laundering, making US+ the most secure and reliable stablecoin available anywhere in the world. This efficiency, with the U.S. dollar being a preferred global currency, offers tremendous value in providing a more secure and safe environment for businesses, not just in America, but all over the world.

Visit **www.fluent.finance** to learn more

Development of blockchain technologies has proven to be necessary for bolstering a Nation's infrastructure and cyber security systems.

"The primary driver is trying to make sure that the embedded opportunities that people have to invest will become **ubiquitous** across the system for people no matter where they live and work" (Click Here)

~Pete Sessions
Congressman for Texas' 17th District
U.S. House of Representatives

Without the proper application of blockchain technology we are **blind** to hidden vulnerabilities, in other words: "We don't know what we can't see." (Click Here)

~Scott Richards
Vice President, Fluent Finance
Former International
Special Advisor

"The only way to protect people, frankly, in many respects, is to **educate** them and give them the tools around investing in general." (Click Here)

~Kathy Kraninger
VP Regulatory Affairs, Solidus Labs
Former director of the CFPB

"Traditional financial crime is still a major problem in the criminal element. Just using this as a **tool** is really a consequence of this new technology. Lastly, the who, to address your question, is still the human element." (Click Here)

~Jeremy Sheridan
SVP, Prime Trust
Former Assistant Director
Secret Service

National Security is directly tied to the fostering of cutting-edge technologies; furthermore, security is linked to major infrastructure systems, such as water, power, and transport.

What are the Implications of a Nation Failing to Adopt Blockchain Technology and Innovation in an Increasingly Multipolar World?

The world has evolved to the point where important decisions are influenced by Russia, China, India and other major superpowers. Under this reality, the US and the West find themselves competing for a voice. Failure to adopt new technologies can have negative **consequences** on the future of American competitiveness. Therefore, in a multipolar world (graph 1) stimulating technological innovation is an important consideration regarding national security.

As Kathy said during the webinar regarding blockchain technology:

Kathy Kraninger

VP Regulatory Affairs, Solidus Labs

*"It's the **next iteration** of the internet and it really is going to touch everyone's lives in a myriad ways" (graph 2), and furthermore she said: "The implications of the technologies are substantial to national security interests."*

We are seeing the technology as an unstoppable force, and a new phase of the internet is being established, which necessitates a clear need for US-led policies guiding the technology being implemented across the globe. The direct effect the technology has on national security must be understood in its full context not just organized violence as terrorism or military action against US interests. National security gives full coverage to the economy, **infrastructure**, and global competitiveness: "Nat Sec" is a holistic view of strategic interests in society. As Scott said during the webinar:

Scott Richards

Vice President, Fluent Finance

"A lot of people immediately think of threats when we talk about national security, but what we're really talking about is the whole holistic description of a nation state: economy, infrastructure, everything else like that."

Simply put, blockchain is becoming a powerful part of the internet infrastructure; therefore, the US must take the driver's seat as innovation sweeps the globe. Avoiding such leadership threatens the competitive security advantage of the US. Kathy eloquently elaborated further:

*"Certainly there are concerns about social media and even the engineering of information by nation state actors, by the way, to **influence** election outcomes in different countries, so, the implications of the technologies are substantial to national security interests."*

Failing to innovate also means failing to attract...

Failing to innovate also means failing to attract talent, further diminishing the competitive edge a country has to offer the world. We see outcomes such as loss of advanced jobs in the US, and lost chances for financial inclusion in a new system of wealth exchange:

Kathy Kraninger

VP Regulatory Affairs, Solidus Labs

"Recognizing that…our economic security and interests, the opportunities that we're providing for our own citizens and residents in the United States to really address some issues around financial ***inclusion****, while at the same time, really helping us be a continued source of innovation in the world."*

Besides losing out on economic opportunities, failing to adopt blockchain innovation will also threaten the power and influence of the global dollar-denominated system as large nation states move further away from it. For instance, the **digital RMB** for China is intended to be used eventually for all imports and exports. If you want Chinese products you will pay in digital currency (see legislation in Senate).

In this analysis, we must continue to look at the contextual consideration of a move towards the world being multi-polar, and actively driven in this direction over the past decade by nations-not just large powers like Russia and China-but middling States that have "stressed" the **global order**:

Scott Richards

Vice President, Fluent Finance

"Adversarial states such as Russia, Iran, China, North Korea can look at the perspective of sanctions and other activities as a threat to their national security, from a perspective point of view. So when we look at what blockchain can mean in terms of the ability of these organizations to create a digital currency, whether it's a digital RMB, to be able to evade sanctions, which is the primary tool of pressure to create conformity. And, so in this kind of context, you need to look at what the technology means to ***innovation*** *for other states that may not be friendly to the international order that we've had since World War 2."*

Thus, we should not only look at targets, we need to understand how adversarial states might use blockchain for their own resilience. The United States' primary method of pressuring states back toward the international norm and conventions are sanctions, but the RMB and digital autonomous organizations have the potential to **obfuscate** the norms and methods sanctions were intended to create.

Taking this view, blockchain and technology in general, becomes a more expansive and informative topic because we start to look at the potential of convergence, which will have a multiplier effect on technological-induced change in a multipolar world.

In such a world of multiple superpowers…

In such a world of multiple superpowers, we need to be radically prepared for new paradigms. Most fundamentally, the U.S. needs to put itself first to maintain the narrative of US superiority and protect the dollar-denominated system that has fostered global prosperity since the post-war agreements:

Kathy Kraninger

VP Regulatory Affairs, Solidus Labs

"The bottom line is that the US really does need to lead, think carefully and support continued innovation in this space."

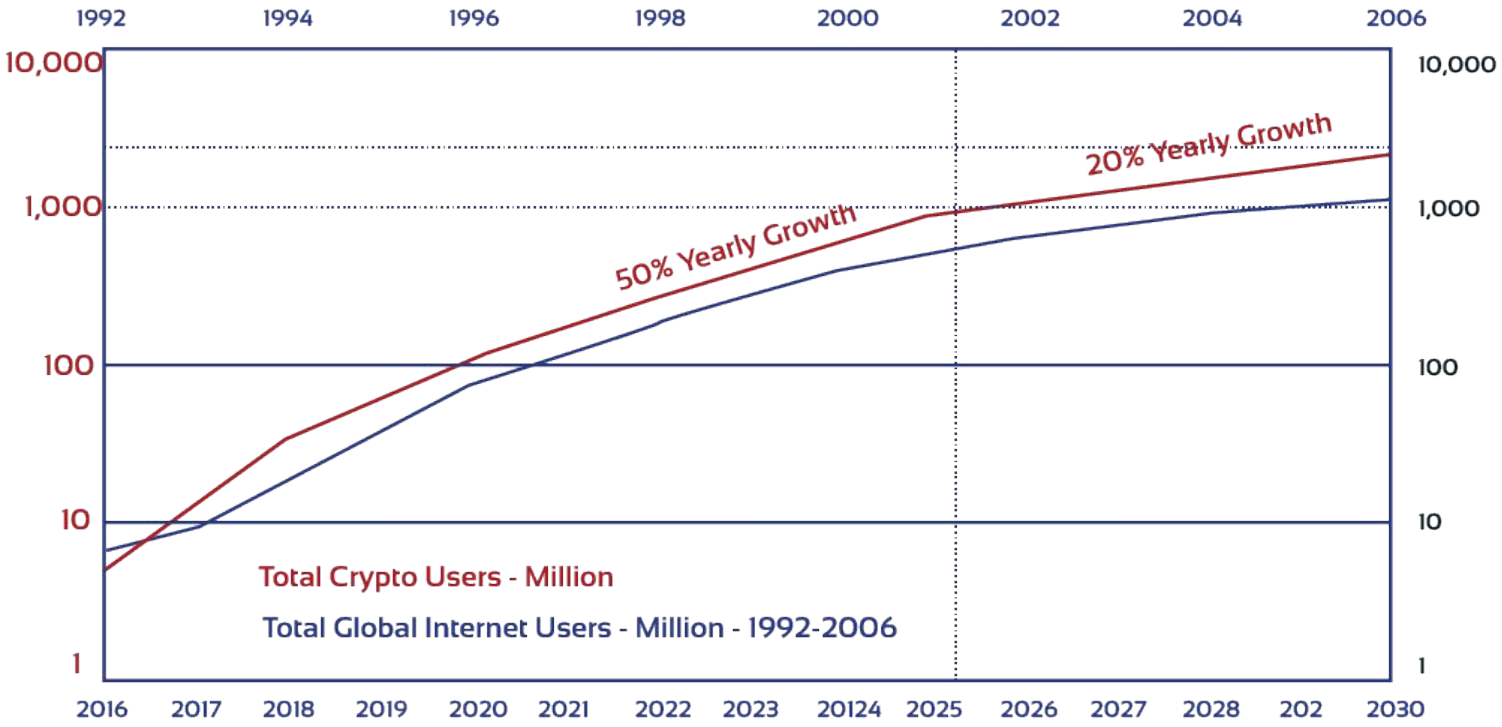
Overall, if we do not lead the technological transformation happening within the **infrastructure** of the internet itself, consequences will follow; such as, lack of opportunities for disadvantaged communities, skilled jobs going to adversaries, threats to the dollar as a world currency of settlement, security risks from inferior technological systems, failure to detect new forms of money laundering affecting elections, and lastly, sanctions losing their effectiveness.

With all this in mind, we see that innovation is absolutely more critical now for national security than ever before in a multi-polar world.

The Leading Superpowers in a Multipolar World

Graph 1

Internet and Crypto Growth
The Next Iteration of the Internet



Graph 2

Crypto.com - World Bank

Definitions

Blockchain technology: Blockchain technology is a decentralized, distributed ledger that stores the record of ownership of digital assets. Any data stored on blockchain is unable to be modified, making the technology a legitimate disruptor for industries like payments, cybersecurity, and healthcare.

Multi-polar world: It is the idea that power is not dominated by one country but distributed among multiple countries. With the rise of Russia, China, and India, the world is no longer a unipolar world dominated by western democracy.

Digital RMB (renminbi): Digital Currency Electronic Payment, is a central bank digital currency issued by China's central bank, the People's Bank of China.

Red Cell: "Red Cell" refers to a "group of contrarian thinkers that challenges conventional wisdom in the intelligence community and mitigates the threat of additional surprises through alternative analysis."

Zero Knowledge Proofs: A method of authentication in which no passwords are shared, making them impossible to steal.

How do we Understand the Transnational Threats and Crimes that Terrorist Organizations Pose?

The majority of market participants are engaged in responsible activities. A small minority are not: these bad actors **suggest** that most threats to financial institutions are caused by the human element. We see human methods with terrorist organizations who specialize in money laundering. In this section, we will discuss the threats that blockchain technology faces and how terrorist organizations may utilize an **unregulated** digital currency to funnel their initiatives.

Understanding the Human Element Starts with the Relationships Between Terrorist Organizations and Their Techniques

When discussing a threat coming from terrorist organizations, one has to remember that these groups—the Haqqanis, ISIS, Al Qaeda, LIFG, and the Taliban—have known each other since the early '80s. They communicate and coordinate to share tactics, techniques, and procedures **(TTPs)**, and the purpose of these TTPs is to avoid detection or to increase effectiveness. During the webinar on national security, Scott further elaborated on the length of time these groups have known each other:

Scott Richards

Vice President, Fluent Finance

"You also have to remember when we talk about Islamic extremism we are talking about a very specific set of a small number of people who have known each other for the past 30-40 years. They communicate regularly, they exchange regularly, they host regularly and so it's there and it's happening." 15:53

From this, we see the threat was built over generations through relationships that go back many years. Over decades of warfare, individuals inside these groups have fought on different sides and sometimes on the same side as the West. Consequently, terrorists are **fluid**, either through their innovations, porous borders, or with nation-state support when they serve as proxies. Individuals have moved from Africa to Pakistan and then back to Africa. We've seen a surge of ISIS insurgents moving from Syria and Iraq to Afghanistan, particularly moving to the northern states. With such fluidity and **flexibility** of mindset coming from years of engagements in multi-level assymmetric warfare, individuals and entire terrorist groups are often very innovative:

Scott Richards

Vice President, Fluent Finance

"They innovate and they constantly have to innovate to innovate again back to detection." 15:19

Relationships and Innovation are Seen in Terrorist...

Relationships and Innovation are Seen in Terrorist Crypto-Currency Seizures.

Innovation and human relationships span across different terrorist organizations. ISIS, for example, has relationships with Ndrangheta in the narco-sector, what we call Jihadist candy: amphetamine and opioids. This relationship was documented in 2016 and later reported by the RAND GROUP and others. In these kinds of settings, a capture of a single ISIS shipment of narcotics contained 26 million tramadol pills. Here you see them learning to use technology and relationships to succeed:

Examples:

1. *In August 2020, the US.Department of Justice (DOJ) reported their largest seizure of terrorist crypto-currency accounts, although, the exact figure was unspecified as millions of dollars across 300 hundred accounts, and the funds were taken from three separate groups, the military wing of Hamas, Al Qaeda, and ISIS. The report also noted that they use telegram, facebook, and social media to solicit crypto-currencies.*
2. *North Korea is the most isolated state of all, with no means of entering the international community, it has nothing to lose. They have become effective in hacking, and with the Lazarus Group reported to have laundered US$455m and used Tornado Cash - they're significant and use Tumblers to anonymize coins.*

Fighting with Solutions

To combat the human **threat** coming from terrorist innovation, we need more resources and support to track human interactions. Entities like Chainlink have been a valuable addition to the detection and security infrastructure. Despite such contributions, there are also state actors like Russia and North Korea integrating technologies faster than we can understand. Such speed of development will also require more intelligence sharing between foes and allies.

How Much of a Threat Is This?

For the most part, "officially" terrorists using crypto are regarded as low-level, but that's also because "we don't know what we can't see." We're heavily reliant on technology to detect; whereas, to truly **understand** the threat we need to re-examine human inventiveness. However, detection is difficult, especially in an unregulated space. We find the actors building relationships across all social channels in order to escape detection:

Scott Richards

Vice President, Fluent Finance

"It's generally sort of said that this is occurring at a cellular level, this is where I come back to the notion of detection." 14:46

Where to Look for a Relationship Between Innovation…

Where to Look for a Relationship Between Innovation and Human Interaction.

If you were to look for the intersection of crypto, because you have to cash out to buy ammonium nitrate for an improvised explosive device (IED) or purchase a role playing game (RPG), I'd watch where the Hawala system and blockchain intersect for just one example:

Scott Richards

Vice President, Fluent Finance

"What cryptocurrency would do for Hawala, is remove the necessity for large cash presence. Instead of having to have, you know, $50,000, $100,000, a million dollars in one country and a million in the other where they trade ownership, you can just trade ownership of crypto. Much less risks of detection, you don't have to house and store the cash in the same kind of way." 16:19 (click here)

The main lesson we must understand here is that governments must **provide** human resources to combat such relationships, and be more advanced in the digital space than the cross border and multinational threats posed by terrorist and adverserial nations.

Why Does the US Need to Lead This Regulation?

Terrorist organizations are constantly communicating and sharing TTPs to innovate and avoid detection. There are always going to be threats to blockchain technology, just like there are in traditional finance, but it is taking place at a **cellular** level. The majority of activity is legal and full of people attempting to build wealth, which is why regulation is the key.

Regulation has to do two things: create an apparatus that protects the consumer and the country, but also not **stifle** innovation. The moment a company goes to the public for an initial coin offering (ICO) and promises a certain type of return, they make an assurance: hence, there needs to be governance anytime people's personal wealth is at risk.

In terms of threats regarding detection, the centralized exchanges can be instructed to block wallets, but there are some decentralized exchanges that are harder to handle. **Detection** takes place in things like telegram channels or discord, but as previously stated, it's important to regulate blockchain technology without hindering its innovation.

Definitions

Hamas: A Palestinian nationalist organization
Ndrangheta: A prominent Italian Mafia dating back to the late 18th century
Jihadist: A term used to reference militant Islamic movements that are seen as threatening to the West
RAND Group: Non-profit organization that improves policy and research analysis
TTPs: The tactics, techniques, and procedures terrorist groups share to avoid detection or increase the effectiveness of their work
Lazarus Group: A cybercrime group run by the North Korean state
Tornado Cash: An Ethereum-based virtual currency tumbler

What Vulnerabilities Exist From Adversarial Phishing & Market Manipulations Compared to Crypto?

When we think of Russia, or other large potential state-led attacks, we must ask what are the areas of **vulnerabilities**? One focus point is unrelated to blockchain technology, a system used by the major banks: the SWIFT network. In a full spectrum attack, SWIFT would be one primary target. Since many banks of Russia have been banned from the SWIFT network, Russia may see the network as a possible target. Despite such attack possibilities, fraud is a much more daily concerning issue.

Attacks are Not as Common as Fraud, we Saw a Direct Instance of Large Scale Fraud Eclipsing Crypto Exchanges During the Pandemic:

Jeremy Sheridan

SVP, Prime Trust

"It's important to note, that this is still eclipsed massively by traditional financial problems. If you look at the amount of exchanges that have seen funds, seen attacks, $2.6 billion worth of crypto was stolen across 46 exchanges but that's since 2006. The pandemic fraud that has occurred in this country the past two years alone has eclipsed 100 billion dollars." 28:15

We see here that fraud is **larger** in traditional means of exchange. Similarly, in a large scale financial attack the most vulnerable entities are traditional systems. It's important to note that we have not yet seen full-spectrum cyber-warfare. At the start of the Ukrainian conflict, we saw a hint of it with attack vectors that could be used against the shutdown of particular systems with technologies that are purposed towards the financial sectors.

In further analysis, **neither** the new tool of blockchain nor traditional finance are to blame, the crux of the issue is the human element, comprising a small minority of criminal minded people that take advantage of systems to commit fraud or attacks:

Jeremy Sheridan

SVP, Prime Trust

"Traditional financial crime is still a major problem in the criminal element. Just using this as a tool [blockchain] is really a consequence of this new technology. Lastly, the who, to address your question is still the human element. This still continues to be the weakest link." 28:43 (click here)

Hacks do not Justify a Ban...

Hacks do not Justify a Ban, When the Human Element is to Blame for Most Traditional and Non-Traditional Failures.

In order to advance blockchain technology and digital asset adoption, we need to continue applying the technology **correctly** to minimize stigma. Here are some examples of known fraud. Despite improvement in distributed storage, large successful hacks have gotten larger:

- *Ronin coin lost US$620 million in March 2022.*
- *Poly lost US$600 million in August 2021*

Lazarus Groups' hack of Harmony took US$100m is an example of a state-linked actor going after an exchange; though this is a heist, not a strategic attack. These examples are not a reason to ban the technology, but in fact further evidence to **integrate** known solutions to prevent fraud. A challenge with blockchain is stated by Jeremy succinctly:

Jeremy Sheridan

SVP, Prime Trust

"The challenge is because of the open source code that allows criminal actors with an unfettered access, hammer on those systems and explores them for vulnerabilities, evaluates the code, as well as lack of compliance control due to their decentralized nature, you have non-compliant exchanges that we in the Secret Service took down, BTCE and others, 2X attacks, and so forth, that don't have a central administrator with oversight of user accounts, records, identity, and activities." 26:50

Thus, the issue is not the technology, but **lack** of proper regulation and oversight of rogue actors using the technology inappropriately. Also, the incorrect application or lack of solutions has led to higher risk vulnerabilities in the digital asset space.

A Solution in a Time of **Blackouts**

In Venezuela, for example, during a power outage while the node network could not connect, some people innovated with mesh networks to allow them to transact with bitcoin.

Once again, blockchain is a **tool** that can solve financial problems, and with the proper applications, could be safer for the consumer than traditional financial methods. Ultimately, the human mind will always target the vulnerabilities of the system to commit fraud and compromise security. Therefore, blockchain and digital assets will continue to remain a smaller vector point of attack as compared to other means of traditional transactions in the foreseeable future.

Definitions

SWIFT Network: Society for Worldwide Interbank Financial Telecommunication is used by the major banks of the world to settle transactions. SWIFT is also heavily invested in blockchain technology.

National Security Legislation in Congress

The P3 Network would like the Members to be aware and informed about blockchain subject matters in Congress. The following list of blockchain bills is relevant to this October edition topic on National Security. Based on the content inside this periodical and accompanying webinar, we hope that you become an **advocate** *of technological change and the benefits new systems have for our digital infrastructure. Please inform your representative that National Security is inextricably linked to development and innovation. Look over the list, give them a call, and have them contact the P3 Network. Send them the pdf digital copy and webinar. Help us give them the tools to make informed decisions.*

H.R.296 Financial Technology Protection Act

a. Rep. Ted Budd (R-NC)
b. Committees: House - Financial Services; Budget

Co-sponsors:

1. Reps. Warren Davidson (R-OH)
2. Darren Soto (D-FL)
3. Abigail Spanberger (D-VA)
4. Stephen Lynch (D-MA)
5. Bryan Donalds (R-FL)

This bill, in the 117th Congress, establishes initiatives aimed at curbing illicit use of digital currencies particularly in funding terrorism.
Specifically, the bill:

- Provides for the investigation of new financial technologies (e.g., digital currencies) and their use in terrorism and other illicit activities.
- Specifically, the bill establishes the Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing, which must research terrorist and illicit use of new financial technologies and issue an annual report.
- The Department of the Treasury must establish a fund to provide a reward for a person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies.
- Additionally, the bill establishes the FinTech Leadership in Innovation and Financial Intelligence Program to support the development of tools and programs to detect terrorist and illicit use of digital currencies.

National Security Legislation in Congress

S.2666 Sanctions and Stop Ransomware Act of 2021

a. Sen. Marco Rubio (R-FL)
b. Committees: Senate - Homeland Security and Governmental Affairs

Co-sponsors: Introduced with Sen. Diane Feinstein (D-CA)

1. Roy Blunt (R-MO)

This bill, in the 117th Congress, addresses ransomware threats to national security. Specifically, the bill

- Requires the promulgation of mandatory cybersecurity standards for critical infrastructure entities;
- Requires the instituting of regulatory requirements for cryptocurrency exchanges operating within the United States to reduce the anonymity of users and accounts suspected of ransomware activity;
- Deems ransomware threats to critical infrastructure a national intelligence priority component to the National Intelligence Priorities Framework; and
- Authorizes monitoring of the internet, including the dark web, for evidence of a compromise to critical infrastructure.

S. 3867 Digital Asset Sanctions Compliance Act of 2022

a. Sen. Elizabeth Warren (D-MA)
b. Committees: Senate - Banking, Housing, and Urban Affairs

Co-sponsors:

1. Tom Reed (R-NY)
2. Mark Warner (D-VA)
3. Raymond Tester (D-MO)
4. Tammy Duckworth (D-IL)
5. Debbie Stabenow (D-MI)
6. Raphael Warnock (D-GA)
7. Chris Van Hollen (D-MD)
8. Cindy Hyde-Smith (R-MS)
9. Catherine Masto (D-NV)
10. Bob Menendez (D-NJ)

This bill, in the 117th Congress, imposes sanctions with respect to the use of cryptocurrency to facilitate transactions by Russian persons subject to sanctions.
Specifically in the bill,

- The President must periodically identify foreign persons who facilitate evasion of Russian sanctions using digital assets. The bill authorizes sanctions against such persons.
- The bill requires a U.S. taxpayer engaged in offshore digital asset transactions greater than $10,000 to file an annual Report of Foreign Bank and Financial Accounts with the Financial Crimes Enforcement Network.

National Security Legislation in Congress

H.R. 7338 To require congressional notification prior to payments of Department of State rewards using cryptocurrencies, authorize the appointment of a Director of Digital Currency Security in the Office of Economic Sanctions Policy and Implementation of the Department of State, and for other purposes.

a. Rep. Gregory W. Meeks (D-NY-5) with co-sponsors Rep. Michael McCaul (R-TX-10)
b. Committee: Foreign Affairs and Financial Services

This bill, in the 117th Congress, requires the Department of State to appoint a Director of Digital Currency Security and take other actions related to digital currencies. Specifically the bill,

- The director shall be a part of the State Department's Office of Economic Sanctions Policy and Implementation and shall be responsible for issues related to digital currencies and U.S. sanctions, including assisting in the development of sanctions policies that are resilient to digital currency use by malevolent actors.
- The bill requires the State Department to notify Congress before making a reward in cryptocurrency under an existing program that authorizes rewards for information leading to the arrest or conviction of parties responsible for certain criminal acts and any cryptocurrency payments made under the rewards program, including any justification for using cryptocurrency for such rewards.
- The bill also requires the State Department to report to Congress on
  - the possible uses of cryptocurrencies or other blockchain-related technologies to provide aid to Ukraine, and
  - an assessment of how digital currencies can affect the effectiveness and enforcement of U.S. sanctions relating to Russia's invasion of Ukraine.

S. 3666 Accountability for Cryptocurrency in El Salvador (ACES) Act

a. Sen. Jim Risch (R-ID); legislation introduced with co-sponsors; Sens. Bob Menendez (D-NJ); Bill Cassidy (R-LA)
b. Committee.. Foreign Relations

Co-sponsors:

1. Sen. Bob Menendez (D-NJ)
2. Bill Cassidy (R-LA)

This bill, in the 117th Congress, advises and promotes a better course of action for our local neighbors in the adoption of cryptocurrency
Specifically the bill,

- Requires reports on the adoption of a cryptocurrency as legal tender in El Salvador, and for other purposes.
- Directs the Secretary of State to study and report on El Salvador's adoption of Bitcoin as a legal tender.

National Security Legislation in Congress

S. 2543 To require a study on the national security implications of the people's republic of China's efforts to create an official digital currency.

a. Sen. Bill, Haggerty (R-TN)
b. Committee: Foreign Relations

Co-sponsors:

1. Mark Warner (D-VA)
2. Cynthia Lummis (R-WY)
3. Kevin Cramer (R-ND)
4. Chuck Grassley (R-IO)
5. Ted Cruz (R-TX)
6. David Scott (D-FL)
7. Michael Braun (R-IN)
8. Donald Young (R-AL)

This bill, in the 117th Congress, is a baseline study of the security issues associated with China's decision to create a digital currency.

Specifically in the bill,

- The President shall submit to the appropriate committees of Congress a report on the short, medium, and long-term national security risks associated with the creation and use of the official digital renminbi of the People's Republic of China, not later than one year after the date of the enactment of this Act.

- Form Of Report.—The report required by subsection shall be submitted in unclassified form but may include a classified annex.

Recommendations to Members of Congress

- The essence of the issue regarding **national security**, which blockchain technology is currently facing, is the responsibility of the individual person that is taking the risk to invest. There are always criminal elements lurking at our doors and if something sounds too good to be true, it probably is. Blockchain is a fairly new technology, which is why education is key to responsible and safe consumer investment. The aim is to ensure these investments provide healthy opportunities for growth, security and safety.

- Blockchain technology is for the most part unregulated and decentralized. It is vital for Congress to implement regulation in order to **protect** consumers just as they've done for consumers in traditional finance. The implementation of regulatory structures must simply protect and not hinder the innovation of crypto technology.

- The role of Congress is to create a proper **application** of these new technologies in order to protect the market participants who are engaged in responsible legal activities. P3 Network acknowledges that Congress already has some regulatory structures set in place but there needs to be an efficient application of those structures.

- There are currently gaps at the State, Federal, and international levels allowing for criminal opportunity and activity. This is often viewed as a stringent, binary choice between centralization or decentralization. However, while **creating** legislation, we have to consider that crypto is difficult to define. The bottom line is that the U.S. needs to lead and support continued innovation in this space, while educating and protecting its consumers.

- By not innovating, there are risks to US competitiveness, economic security interests, as well as lost financial inclusion opportunities for US citizens.

Dear Members of Congress,

The P3 Network would love to discuss your legislation more in depth. We are neither for nor opposed to your current bills. If we can provide market input from the blockchain community for your legislation, please connect us with your staff.

Thank you for your efforts in Congress,
The P3 Network team

Become a Member of the P3 Network

Our Mission

The P3 Network is a convening force of public officials, private industry professionals, and thought leaders working to build stable grids, currencies, and governments around the world. Most importantly, we provide recommendations to Congress that will stimulate innovation and increase American strength in a multipolar world.

Participate

- Private Roundtables Connecting the Public Sector with Private Industry
- Virtual Thought Leadership
- Monthly Periodical, eBooks & Newsletters
- Hear Input from the Crypto Technology Advisory Group (CTAG)

Contributors

Fluent

SOLIDUS LABS

Prime Trust

CRYPTO TUTORS

Learn More

- https://www.p3network.com
- info@p3network.com
- Adrien Yule