2022-12

SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY

Rowen, Michael S.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71537

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY

by

Michael S. Rowen

December 2022

Thesis Advisor:	Leo J. Blanken
Second Reader:	Nicholas Dew

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael S. Rowen	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) USASOC, Fort Bragg, North Carolina 28310; 1SFC, Fort Bragg, NC 28310	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Concepts to harness positive opportunities inside the cryptocurrency ecosystem to advance national security objectives have yet to be fully explored in government organizations. This thesis, focuses on cryptocurrency as a subset of digital assets and attempts to answer the question: Is there utility for cryptocurrency in U.S. special operations (USSOF) and could it support broader U.S. national security strategies? A whole-of-government approach for the responsible development of digital assets should include Department of Defense (DOD) and USSOF perspectives. The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace. The DOD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams with the intent to develop new operational concepts. USSOF should continue to expand public-private partnerships to improve awareness, capacity, and competency in the digital asset ecosystem and leverage blockchain research and development directives to inform innovative concepts for cryptocurrency in special operations.

14. SUBJECT TERMS cryptocurrency, special operations, SOF, Bitcoin, USSOCOM, USASOC, digital assets, financial technology	**15. NUMBER OF PAGES** 111
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

SPECIAL OPERATIONS AND CRYPTOCURRENCY: CONCEPTS TO HARNESS INNOVATION FOR NATIONAL SECURITY

Michael S. Rowen
Major, United States Army
BA, Western New England College, 2010

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED DESIGN FOR INNOVATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Leo J. Blanken
Advisor

Nicholas Dew
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Concepts to harness positive opportunities inside the cryptocurrency ecosystem to advance national security objectives have yet to be fully explored in government organizations. This thesis focuses on cryptocurrency as a subset of digital assets and attempts to answer the question: Is there utility for cryptocurrency in U.S. special operations (USSOF) and could it support broader U.S. national security strategies? A whole-of-government approach for the responsible development of digital assets should include Department of Defense (DOD) and USSOF perspectives. The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace. The DOD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams with the intent to develop new operational concepts. USSOF should continue to expand public-private partnerships to improve awareness, capacity, and competency in the digital asset ecosystem and leverage blockchain research and development directives to inform innovative concepts for cryptocurrency in special operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CBDC	Central Bank Digital Currency
CoW	Coalition of the Willing
CRADA	Cooperative Research and Development Agreement
DAO	Decentralized Autonomous Organization
DApps	Decentralized Applications
DARPA	Defense Advanced Research Projects Agency
DC:BB	Distributed Consensus: Blockchain and Beyond
DID	Decentralized Identification
DLT	Distributed Ledger Technology
DOC	Department of Commerce
DOD	Department of Defense
DOT	Department of Treasury
IPFS	Interplanetary File System
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
SOCOM	Special Operations Command
TSOC	Theater Special Operations Command
USASOC	United States Army Special Operations Command
USD	United States Dollar
USDC	United States Dollar Coin
USDT	United States Dollar Tether
USSOF	United States Special Operations Forces
VEO	Violent Extremist Organizations

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Emerging financial technologies have the potential to reveal gaps in national security strategies for the United States. The presidential executive order of March 2022 and the digital asset development framework of September 2022 represent initial steps to provide a comprehensive whole-of-government model in response to this gap. Methods to harness positive opportunities inside the cryptocurrency ecosystem to advance national security objectives, however, have yet to be fully explored in government organizations. This thesis, therefore, focuses on cryptocurrency as a subset of digital assets and attempts to answer the question: Is there utility for cryptocurrency in U.S. special operations (USSOF) and could it support broader U.S. national security strategies?

A. KEY FINDINGS

The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. Beyond financial settlements, cryptocurrency offers the ability to build private and secure applications on public blockchain infrastructure to deliver valuable non-standard communication or data management tools for military operations. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace.

A whole-of-government approach for the responsible development of digital assets should include Department of Defense (DOD) and USSOF perspectives. Including USSOF concepts for cryptocurrencies could help the United States to shape global cryptocurrency adoption with the intent of countering nefarious activity and modernizing security strategies while concurrently developing novel support mechanisms in moments of crisis and conflict.

Blockchain technology is widely accepted as a valuable innovation and forms one of the foundations to digital assets. A policy window is opening for DOD leaders to stimulate innovation in emerging financial technology tactics by understanding the overlap between blockchain, digital assets, and global power dynamics. A blockchain research symposium held at NPS in September 2022 offered an opportunity to analyze the current state of blockchain adoption in the U.S. government and identify threats, opportunities, areas of friction and advocacy.

There is potential for a divergence in blockchain development and adoption between authoritarian regimes and democratic nations, underscoring the need to recognize the implications of blockchain technology in U.S. national security strategies. U.S. pacing threats view digital currency markets as an opportunity to gain hegemony with new central bank digital currencies and shape an alternative, digital financial system by exploiting early adopters and undermining the potential for public good from digital asset technologies. The United States is positioned to assist allies that are looking for regulatory clarity and policy guidance to establish global norms in line with U.S. values for blockchain and digital assets. Perspectives from USSOF operators trained and educated in cryptocurrency may offer an important feedback mechanism to U.S. policymakers.

B. RECOMMENDATIONS

- The DOD and USSOF should coordinate with allies and across U.S. government departments to develop a pilot program that places cryptocurrency in the hands of SOF operators and tactical teams with the intent to develop new operational concepts.

- The U.S. government should continue to expand public-private partnerships to quickly improve awareness, capacity, and competency in the complex blockchain and digital asset ecosystem where DOD is too often overlooked in key stakeholder positions.

- USSOF should leverage the 2023 NDAA SEC 5913 "National Research and Development Strategy for Distributed Ledger Technology" to request additional resources for advancing education and experimentation with digital assets in U.S. special operations units. USSOF in conjunction with academic and private partnerships, should conduct surveys to help illuminate the level of adoption and literacy for digital assets which will drive training requirements and experimentation.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Dr. Leo Blanken and Dr. Nicholas Dew, for their guidance, leadership, and encouragement while pushing me to explore an emerging but contentious topic.

It was a privilege to work with everyone in the cryptocurrency and financial technology sector, I learned more than I could have imagined. I am so grateful for the community's eagerness to help and trust in my research to connect me with other key leaders. The blockchain symposium was only possible because of this wonderful and patriotic network of leaders who offered their time and expertise, I am truly thankful.

I would also like to thank my peers and other NPS faculty members who patiently listened to my rhetoric about cryptocurrencies and provided valuable recommendations and feedback.

Most importantly, I am grateful for my loving family who kept me balanced through this incredible experience and appreciated the time I dedicated to this subject. My wife, Keelan, and daughters, Blair, Alice, and Ruby are truly a blessing, their love and support trumps any achievement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE INTERSECTION OF CRYPTOCURRENCY AND NATIONAL SECURITY

The operational use of cryptocurrency for U.S. special operations forces (USSOF) has the potential to serve as a forcing function to discover emerging financial technology concepts in strategic competition and modernize partnerships. Digital asset proliferation may have impacts far beyond the financial environment and the U.S. national security enterprise must continue to assess adoption trends to adequately respond to shifts in geopolitics. Fortunately, the United States is making progress toward a digital asset strategy as evident in the March 2022 presidential executive order directing a call to action from U.S. stakeholders to provide recommendations for responsible development of digital assets.[1] Following the executive order, the U.S. released a digital asset development framework in September 2022, which was intended to provide a comprehensive whole-of-government model.[2] However, one government entity largely absent from the published digital asset framework is the U.S. defense department. This is an oversight: the U.S. may miss an opportunity to gain ground-truth insights to help shape the U.S. leadership position toward digital assets and positively influence global adoption trends.

Current U.S. research and development for digital assets is focused on the implications of central bank digital currencies, addressing consumer and investor protection, and countering illicit finance.[3] The U.S. defense enterprise's supporting role centers around countering threat finance such as the recent announcement from the

[1] Exec. Order No. 14067, "Executive Order on Ensuring Responsible Development of Digital Assets" (2022), https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

[2] The White House, "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets," The White House, September 16, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

[3] Darrell Duffie and Elizabeth Economy, "Digital Currencies: The U.S., China, And The World At A Crossroads," Working Group (Hoover Institute, 2022), https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads.

Pentagon for a Defense Advanced Research Projects Agency (DARPA) project to help authorities crack down on illicit uses of digital assets.[4] U.S. government organizations have yet to fully develop proven methods to explore the cryptocurrency ecosystem and harness positive opportunities for national security objectives.

Of all the subsets of digital assets, cryptocurrency is the most contentious and typically holds a negative connotation. However, USSOF are comfortable when surrounded by uncertainty and would likely embrace the opportunity to shine light on the murky world of cryptocurrencies to help understand both positive and negative use cases. The positive solutions for cryptocurrency in military operations are largely unknown and the untapped potential for programmable digital currency in the hands of creative special operations members may reveal more opportunities beyond countering illicit activity. Cryptocurrencies such as Bitcoin and Ethereum offer a novel medium of exchange for peer-to-peer communication, instantly transferring value around the world, or developing more applications beyond the original function, albeit with proper risk mitigation.

A comprehensive strategy will need to reach the diverse subsets of digital assets; central bank digital currency, cryptocurrencies, non-fungible tokens, and stablecoins which all demand time and attention to fully understand. This thesis is focused on cryptocurrency as a subset of digital assets and attempts to answer the question; is there utility for cryptocurrency in U.S. special operations and could it support broader U.S. national security strategies?

B. APPROACH

The approach taken for this research project intends to offer a wide range of concepts for cryptocurrencies but observed through the lens of a U.S. national security practitioner. Cryptocurrency is an emerging technology, and the fundamentals are not commonly understood among the general population. This led to the decision to offer a conceptual thesis focused on stating the relevance for cryptocurrency in U.S. special

[4] Tory Newmyer, “Pentagon Launches Effort to Assess Crypto’s Threat to National Security,” *Washington Post*, September 23, 2022, https://www.washingtonpost.com/business/2022/09/23/darpa-crypto-national-security/.

operations. The complicated nature of cryptocurrency and the underlying blockchain technology may leave some readers with more questions than answers. That result may still offer positive commentary within the U.S. national security enterprise and maintain cryptocurrency in the mind of practitioners. The research revealed that most resources and articles discussing the DOD and cryptocurrency are limited to countering illicit activity. This thesis intends to offer additional scenarios where special operations forces could harness the positive benefits surrounding a novel financial technology. This paper offers general concepts for how special operations could leverage the cryptocurrency ecosystem by citing examples of cryptocurrency and digital asset use cases around the world.

Of note, Chapter IV summarizes several key points from the planning and execution of a blockchain research symposium conducted on the Naval Postgraduate Schools campus from 12 to 13 September 2022. It is recommended for readers to reference the appendices for each panel concept sheet which offers the moderator questions and may offer more context to the key findings listed in Chapter IV. Please note that we did not develop a panel 5 concept sheet. The summary was co-authored with an NPS faculty member, LTC Michael "Kelly" McCoy who helped organize and lead the symposium. This event aggregated various national security practitioners and U.S. Defense Department leaders to debate the threats and opportunities for blockchain technology, cryptocurrencies, and the intersection of national security for two financial technology innovations.

A blockchain symposium was a deliberate approach used to support this thesis largely due to the contentious narrative surrounding cryptocurrency in U.S. national security circles. The author and faculty members from NPS, believed that starting with cryptocurrency's foundational technology, blockchain, offered a more acceptable model to introduce potential benefits of cryptocurrency. Overall, the blockchain symposium presented an opportunity to analyze the broader support and adoption potential of cryptocurrency in both the private and public sectors which may prove useful for future research and development.

C. LITERATURE REVIEW

1. The Narrative of Digital Assets in U.S. Government

The discussion within DOD circles regarding cryptocurrency centers on the negative implications from cryptocurrency in support to nefarious activity and possible counter-measure U.S. forces could take to reduce those threats. Violent extremist organizations (VEOs) and criminal organizations are leveraging cryptocurrency to remain undetected while transferring value, communicating, and laundering money. Nation states have embraced the cryptocurrency ecosystem to attempt sanctions avoidance and build a new network to transfer value or trade commodities. In the article *Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency*, the authors offer that "cryptocurrency transactions expand the international financial competitive space by creating an alternative to a fiat-based monetary system that skirts international financial mechanisms set to detect and intercept suspicious activities."[5] The negative repercussions for the United States and allies if an alternative international financial market without the U.S. dollar as the reserve currency are significant and expert analysis, research, and security strategies should continue to prevent those conditions. A gap in research still exists to determine where the responsible integration of cryptocurrency and other digital assets into the current U.S. led, international trade markets and security enterprise may benefit.

The DOD, and specifically financial management commands recently added a 40-hour digital asset training course and executive level cryptocurrency classes.[6] Comptrollers in the DOD typically apply counter threat financing doctrine which is often absent with cryptocurrency references or connects digital currency to illicit activity. The DOD's focus and experience for disrupting terror financing cells is likely driving most of the current literature on cryptocurrency but as digital asset literacy grows so too will the scope of research. The Fall 2022 issue of *Armed Forces Comptroller* is a positive adoption signal

[5] Sara Dudley et al., "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *Joint Force Quarterly*, no. 92 (2019): 60.

[6] Joint Knowledge Online, "New USSOCOM J35 Counter Threat Finance (CTF) Curriculum," Joint Chiefs of Staff, August 4, 2022, https://www.jcs.mil/JKO/Latest-News/JKO-Customer-Spotlights/Article/3115355/new-ussocom-j35-counter-threat-finance-ctf-curriculum/.

for financial technologies and the editions subtitle, *Operationalizing the Army's Universe of Transactions* presents several articles sharing methods to implement data analytics and dynamic value transfer systems.[7] Specifically, the article *Applying Financial Capabilities to Achieve Multi-Domain Effects* by COL Brian Smith, details a process the U.S. Army could implement for financial instruments to achieve tangible operational effects.[8]

Two reports from the Center for Naval Analyses (CNA), offer relevant cryptocurrency information for military organizations. Both reports were published in 2019 and authored by Megan McBride and Zack Gold who present in depth analysis and helpful background information.[9] The reports titled "Cryptocurrency: A Primer for Policy-Makers" and "Cryptocurrency: The Implications of Special Operations Forces" are recommended as an early reference to help understand the connection of cryptocurrency to military operations.[10]

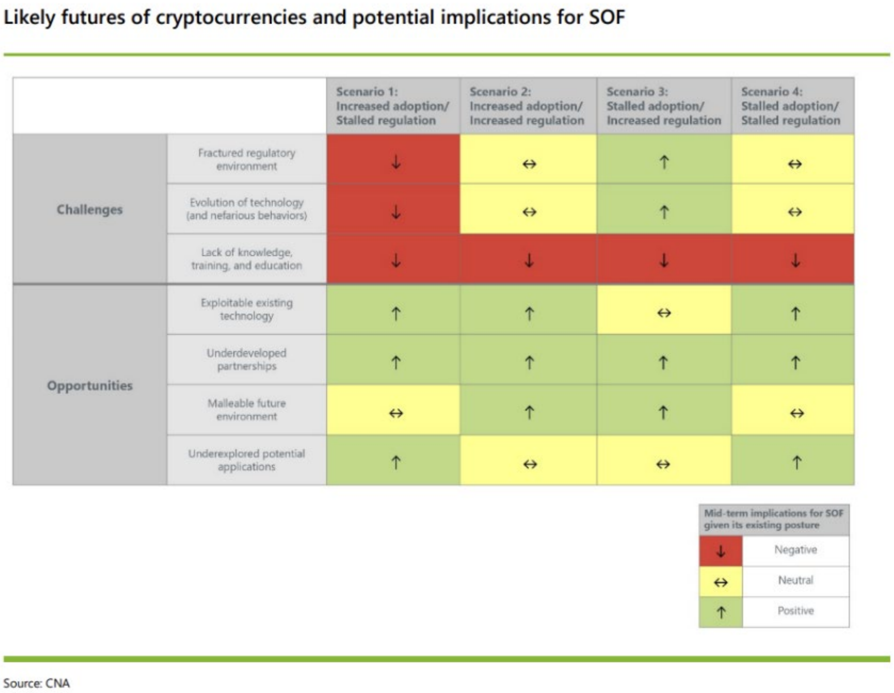
In Figure 1, the CNA report on the implications for SOF presents a chart outlining potential challenges and opportunities for special operations units correlated to various levels of cryptocurrency adoption. This tool remains useful when applying the current state of cryptocurrency adoption and then incorporating analysis from McBride and Gold to build context for military specific research and development.

[7] Rich Brady and Bill Arnold, "Data Analytics: From Raw Data to Informed Decisions," *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022), https://asmconline.org/armed-forces-comptroller/.

[8] Brian A. Smith, "Applying Financial Capabilities to Achieve Multi-Domain Effects: Using Financial Capabilities Operationally Rather Than Transactionally," *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022): 54, https://asmconline.org/armed-forces-comptroller/.

[9] Megan McBride and Zack Gold, "Cryptocurrency: A Primer for Policy-Makers" (Arlington, VA: Center for Naval Analyses: Analysis and Solutions), accessed October 26, 2022, https://www.cna.org/reports/2019/08/cryptocurrency-primer-for-policymakers.

[10] Megan McBride and Zack Gold, "Cryptocurrency: Implications for Special Operations Forces" (Arlington, VA: Center for Naval Analyses: Analysis and Solutions, August 2019), https://www.cna.org/reports/2019/08/cryptocurrency-implications.



Likely futures of cryptocurrencies and potential implications for SOF

		Scenario 1: Increased adoption/ Stalled regulation	Scenario 2: Increased adoption/ Increased regulation	Scenario 3: Stalled adoption/ Increased regulation	Scenario 4: Stalled adoption/ Stalled regulation
Challenges	Fractured regulatory environment	↓	↔	↑	↔
	Evolution of technology (and nefarious behaviors)	↓	↔	↑	↔
	Lack of knowledge, training, and education	↓	↓	↓	↓
Opportunities	Exploitable existing technology	↑	↑	↔	↑
	Underdeveloped partnerships	↑	↑	↑	↑
	Malleable future environment	↔	↑	↑	↔
	Underexplored potential applications	↑	↔	↔	↑

Mid-term implications for SOF given its existing posture	
↓	Negative
↔	Neutral
↑	Positive

Source: CNA

Figure 1. Cryptocurrency Adoption and Implications Tool.[11]

In general, there is a consensus for continued collaboration to share methods for managing the emergence of cryptocurrency across U.S. government departments and agencies. The U.S. State Department published a success story and positive use case after cryptocurrency rewards helped to gather intelligence on cybercriminals.[12] Harnessing the benefits from alternative incentive structures provided by cryptocurrency may spark more creativity from other national security organizations. As other government agencies spread best practices for disrupting nefarious cryptocurrency it helps improve awareness of the capabilities and limitations for cryptocurrency. The book *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* includes multiple articles discussing blockchain, cryptocurrencies, and

[11] Source: McBride and Gold.

[12] Martin Leo Rivers, "Got Bitcoin, Will Buy Intel: U.S. Government Offers Cryptocurrency Bounty In Radical New Approach To Fighting Cybercrime," Forbes, accessed October 27, 2022, https://www.forbes.com/sites/martinrivers/2021/07/18/got-bitcoin-will-buy-intel-us-government-offers-cryptocurrency-bounty-in-radical-new-approach-to-fighting-cybercrime/.

nation agnostics digital networks.[13] The thought leadership provided by forward leaning technologists and service members in these publications is vital to help steer research and development efforts in SOF. A 2020 report from the Cyber Defense Review offers a supporting argument for including SOF units in digital threat finance efforts at the operational level such as at the Theater Special Operations Commands (TSOC).[14] The author, Hugh Harsono, states that SOF is postured to increase support to digital threat finance operations and the application of SOF specific instruments and relationships, it could help U.S. national security objectives combating VEO finance capabilities.

At the Naval Postgraduate School there are several thesis' which research emerging financial technology with most highlighting Bitcoin in particular, such as Peter Denning's report titled *Bitcoins Maybe, Blockchains Likely*.[15] Most publications either connect threat finance to cryptocurrency and include various risk assessments or provide nuanced technical insight to the broader blockchain industry. For example, NPS's Systems Engineering Department offers a thesis paper detailing the protocols or security provenance for Ethereum's blockchain.[16] In general, the research framework is focused on methods to reduce undesired activity of cryptocurrency or ways to posture national security towards the disruptive nature of cryptocurrency and illicit applications such as the thesis titled *Cryptocurrency and State Sovereignty*.[17]

Another relevant NPS thesis discusses the social networks supporting Bitcoin and offers greater insight to Bitcoin utility for SOF, which directly impacted this thesis and inspired several operational concepts. The thesis titled, *Bitcoin: A Technology Influenced*

[13] Zachary S Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces* (Livermore, CA: Center for Global Security Research, 2021). Pg 269

[14] Hugh Harsono, "Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain," *The Cyber Defense Review* 5, no. 3 (2020): 153–60, https://www-jstor-org.libproxy.nps.edu/stable/26954878.

[15] Peter J. Denning and Ted G. Lewis, "Bitcoins Maybe; Blockchains Likely," *Sigma XI-The Scientific Research Society*, December 2017.

[16] Vikram K. Kanth, "Blockchain for Use in Collaborative Intrusion Detection Systems" (master's thesis, Monterey, CA, Naval Postgraduate School, 2019).

[17] Ryan L. Frebowitz, "Cryptocurrency and State Sovereignty" (Monterey, CA, Naval Postgraduate School, 2018), https://calhoun.nps.edu/handle/10945/59663.

Social Movement, by Green and Johnson presents cryptocurrency adoption in the context of global social movements and theory.[18] The thesis by Johnson and Green also provides a thought experiment which detailed a hypothetical use case incorporating a U.S. Army Civil Affairs team utilizing Bitcoin during key leader engagements and transactions.

The most recent NPS thesis, *Understanding Bitcoin and It's Utility for Special Operations Forces*, served as a starting point and helped steer this thesis approach.[19] The author, Michael Pero, focused on Bitcoin and offers a framework for continued research of Bitcoin in military operations. Pero's publication shares case studies on the history of money and Bitcoin's unique value proposition. The paper also references Bitcoin in resistance movements and posits that the U.S. could leverage the principles of cryptocurrency in future resistance movements which also inspired an expansion of that concept in Chapter III of this thesis.

Cryptocurrency presents many policy considerations, but these are beyond the scope of this thesis. It is difficult for anyone to fully grasp the complex nature of U.S. fiscal policy and regulation, but this paper recommends DOD leaders closely monitor publications or news releases from the U.S. Department of Treasury (DOT) and Commerce (DOC). Both departments are two key stakeholders leading the U.S. in responsible development of digital assets. The National Institute of Standards and Technology under the DOC published a blockchain technology overview. The Presidential executive order and whole-of-government framework charters the U.S. DOT and DOC to work across government to help drive innovation but maintain safeguards while advancing the frontier of digital assets. There are still outstanding legal questions, but the DOC's *Digital Asset Competitiveness Report* offers important background information with a balanced

[18] Jason D. Johnson, "Bitcoin: A Technology-Influenced Social Movement" (master's thesis, Monterey, CA, Naval Postgraduate School, 2019), https://calhoun.nps.edu/handle/10945/63988.

[19] Michael C. Pero, "Understanding Bitcoin and It's Utility for Special Operations Forces" (Monterey, CA, Naval Postgraduate School, 2022), https://calhoun.nps.edu/handle/10945/69701.

approach towards U.S. leadership in this emerging market while addressing a wide range of risks.[20]

The programmability of many cryptocurrency blockchains such as Ethereum and Bitcoin's Lightning Network may arguably reveal unforeseen opportunities in non-standard payment methods and communication capabilities. For the Ethereum blockchain in particular, one of the gold standard resources for developers is the book *Mastering Ethereum: Building Smart Contracts and DApps*.[21] This document was published in 2019 and offers methods to develop smart contracts on Ethereum blockchain, which helps expand the utility of the blockchain through computer programming and coding. As quoted in the first pages, the book is intended to "serve as both as a reference manual and as a cover-to-cover exploration of Ethereum."[22] Many of the arguments for the future utility of cryptocurrency lean heavily on the application development outlined in *Mastering Ethereum* with supporting evidence from the expanding cryptocurrency markets. The report titled *Weaponizing Blockchain* reveals how China, Russian, and the U.S. view military applications beyond explicit monetary transactions and the open-source nature of cryptography and distributed computing now levels the playing field for nation states and illicit networks.

It takes time to understand the array of digital asset threats and opportunities, which contributes to the United States reluctance to implement cryptocurrency into U.S. military operations. Sharing academic resources such as a technical summary for A *Taxonomy of Cryptocurrencies and Other Digital Assets* helps reduce the learning curve and establish a shared understanding of cryptocurrencies.[23] The number of academic resources continues to grow as mainstream adoption of certain digital assets increases, however there is still

[20] Department of Commerce, "Responsible Advancement of U.S. Competitiveness in Digital Assets," Digital Asset Competitiveness Report (Washington, D.C: U.S. Department of Commerce, September 2022), https://www.commerce.gov/files/digital-asset-competitiveness-report.

[21] Andreas M. Antonopoulos and Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, First edition (Sebastopol, CA: O'Reilly, 2019).

[22] Antonopoulos and Wood.

[23] Andria van der Merwe, "A Taxonomy of Cryptocurrencies and Other Digital Assets," *Review Business: St. Johns University*, no. 41 (2021): 30–43, https://www.stjohns.edu/sites/default/files/uploads/Review-of-Business-41%281%29-Jan-2021.pdf.

limited information published from a U.S. military perspective. An article published by *Strategy Bridge* in 2022 touches on the complicated nature of digital currency and policy hurdles for the United States when adapting regulations and standards to meet emerging digital currencies and how U.S. adversaries may leverage the technology.[24]

2. What Is Cryptocurrency?

The three main subsets of digital assets are cryptocurrencies, central bank digital currencies, and stablecoins with cryptocurrency holding the most volatility and speculation. Bitcoin became the first successful cryptocurrency after the whitepaper published in 2008 and remains the leader in global adoption compared to other alternative cryptocurrencies. The U.S. financial crisis in 2008 helped drive the early adopters of Bitcoin as many people lost trust for banks and centralized institutions. The introduction of Nakamoto's *Bitcoin Whitepaper* offers insight to the original intent of Bitcoin's protocol.

> …payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.[25]

This quote helps connect the relevance for special operations and Bitcoin if considering the mutual benefits to digital peer-to-peer connections. The ability to establish a private communications channel, without third-party intermediaries, transfer value, and trust through cryptography should pique the interest of special operations units.

The developers of Bitcoin are unknown, but the network protocol emerged as a novel way to conduct peer-to-peer transactions and remove third party entities to handle trust and accurate record keeping. Blockchain and cryptography underlie the technology

[24] Alyce Abdalla, "U.S. Strategy and the Future of Money: Advancing U.S. Interests During a Financial Transformation," The Strategy Bridge, August 2022, https://thestrategybridge.org/the-bridge/2022/8/29/us-strategy-and-the-future-of-money.

[25] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.Org*, October 2008, https://bitcoin.org/en/bitcoin-paper.

while advancements in computer processing power facilitated scaling through a global decentralized network. Individuals can download Bitcoin's open-source software, run a node on their home computer, and validate transactions, which codifies the information on the blockchain.[26] Bitcoin's innovative nature sparked organizational changes through a digitally native economy over the borderless internet without trusting a third party. The decentralized nature of Bitcoin helps the network avoid central points of failure or succumb to censorship from nation state firewalls. The resiliency and redundancy of the network is supported by distributed ledger technology (DLT) and people or "nodes" running the software which can update new or returning nodes with the transaction history.

A loose analogy is to imagine if individuals could run Visa's electronic payments network on their home computer, help validate every transaction occurring on the network, and also maintained a complete historical ledger. This analogy begins to reveal obstacles with Bitcoin's slow and cumbersome protocol as a medium of exchange which does hinder the ability to compete with cash payments as a means of currency. This factor, in combination with the open-source nature of Bitcoin and other cryptocurrency developer software, led to an emergence of alternative cryptocurrencies with a wide range of functionality. The viability of some cryptocurrencies is frequently debated as many are simply derivatives from other open-source documents and offer little value to customers.

In general, cryptocurrencies are categorized into different layers depending on which blockchain is used as the foundation and subsequent tokens to deliver new capabilities or applications. Typically, cryptocurrency blockchains offer specific tokens which are mined through various incentive structures to generate new coins and properly maintain network transactions.[27] Cryptocurrency is often used as the catch-all phrase but a more precise understanding places tokens as another category or layer, built on top of a cryptocurrency blockchain.[28] Developers even built a new layer, named the Lightning

[26] Kristen Busch, "Blockchain: Novel Provenance Applications" (Washington, D.C: Congressional Research Service, April 12, 2022), https://crsreports.congress.gov/product/pdf/R/R47064.

[27] Coinbase, "Crypto Basics - What Is Mining?," Coinbase Learn, 2022, https://www.coinbase.com/learn/crypto-basics/what-is-mining.

[28] "Cryptocurrencies vs. Tokens: Digital Assets," Gemini, accessed October 26, 2022, https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference.

Network, on top of Bitcoin's original protocol to help improve efficiency and promote application development for Bitcoin.

Many cryptocurrency companies offer helpful websites and free educational guides to increase understanding and confidence. For example, Chainalysis offers free online courses of instruction through their "Chainalysis Academy" website to choose specific areas to research.[29] The centralized exchange, Gemini, offers a particularly user friendly "cryptopedia" on their website which allows users read a concise summary for variety of digital asset terms.[30] Another trusted exchange, Coinbase, delivers a comprehensive guide to cryptocurrency basics, advanced terminology, and even Coinbase Institute which presents free reports to download and help increase awareness of the market.[31] Between both public and private research organizations, there is an abundance of resources on digital assets and are typically free to access online.

Centralized digital currencies and stablecoins are likely positioned as a critical bridge between the legacy financial system and emerging financial technology markets. Central bank digital currencies are a new form of digital money intended to supplement existing central bank reserves, according to The Federal Reserve Bank of Boston and Massachusetts Institute of Technology's digital currency initiative.[32] Stablecoins are like central bank digital currencies as the idea is to provide a stable value relative to a national currency. However, stablecoins have no leading authority or international standards for private stablecoin creation or oversight for assets in reserve which places added pressure for U.S. congressional action. Stablecoins and CBDC's help the digital currency markets manage volatility and diversify reserve pools if handled with proper oversight and regulation. It is reasonable to assume that future applications of digital assets by the DOD

[29] "Learn Cryptocurrency," Chainalysis Academy, accessed October 31, 2022, https://academy.chainalysis.com/page/learn-cryptocurrency.

[30] Gemini, "Crypto Glossary - Cryptopedia," Gemini Cryptopedia, 2022, https://www.gemini.com/learn/glossary.

[31] Coinbase Institute, "Coinbase Institute," accessed October 31, 2022, https://www.coinbase.com/institute.

[32] Federal Reserve Bank of Boston, "Project Hamilton Phase 1 Executive Summary," Federal Reserve Bank of Boston, February 3, 2022, https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx.

will require integration with approved stablecoins and potentially versions of a central bank digital currency.

3. Critiques of Cryptocurrency

The international community and the United States are struggling to catch up with cryptocurrency regulatory policy and standards. The global demand for digital assets is growing and government officials continue to push for varying levels of regulation.[33] Some concerns center around the official designation of digital assets to determine which cryptocurrencies are a security or commodity. Additional security minded concerns question how companies and governments can implement know-your-customer and anti-money laundering measures for cryptocurrency. These issues have been debated for years with dedicated research to help gauge the sensitivity and necessity to apply government clarity.[34] The alternative settlement layers of cryptocurrency offer methods outside of traditional financial systems and highlight concerns for the United States to enforce economic sanctions and project economic power.

Most cryptocurrencies have yet to be officially categorized or designated under specific U.S. regulatory offices or departments. Bitcoin, with no centralized company or owner is decentralized and considered a commodity with tax laws like gold, therefore falling under the U.S. commodities regulations. Many developing nations believe in the potential for a new asset class outside of national government issued currency and embraced Bitcoin as legal tender such as El Salvador in 2021.[35] Critics still argue El Salvador's decision to purchase large amounts of Bitcoin to hold in reserve is the wrong

[33] Tadas Limba, Andrius Stankevičius, and Antanas Andrulevičius, "Towards Sustainable Cryptocurrency: Risk Mitigations from a Perspective of National Security," *Journal of Security and Sustainability Issues*, December 19, 2019, https://repository.mruni.eu/handle/007/16063.

[34] Victor Dostov and Pavel Shust, "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?," *Journal of Financial Crime* 21, no. 3 (January 1, 2014): 249–63, https://doi.org/10.1108/JFC-06-2013-0043.

[35] International Trade Administration, "El Salvador Adopts Bitcoin as Legal Tender," U.S. Department of Commerce, International Trade Adminstration, June 2021, https://www.trade.gov/market-intelligence/el-salvador-adopts-bitcoin-legal-tender.

decision and the price volatility is supporting evidence against nation state ownership of Bitcoin.

There are growing concerns surrounding the cryptocurrency market as risks for investors and consumers are evident when major corporations in the ecosystem collapse and exploit customers in the emerging and unregulated global markets. 2022 revealed several failures within the digital asset ecosystem and the vulnerabilities when a venture capital, hedge funds, and centralized trading exchanges conduct reckless or criminal business practices. The collapse of a private stablecoin triggered a cascade effect which exposed multiple centralized digital asset investment companies and harmed both institutions and retail investors. The cryptocurrency market collapse in 2022 revealed that traditional business principles still apply for cryptocurrency and flaws in human nature will continue to be an enemy of innovation. The company FTX was the third largest cryptocurrency trading exchange in the world when details of potentially fraudulent financial management systems were revealed to the public. The subsequent collapse of FTX is a major reason for skepticism with digital assets and private cryptocurrencies. The hyper-financialization and speculative investing practices of digital asset markets often cloud the innovative potential for many observers and government organizations believe the risk is too high to consider cryptocurrency applications.

Cryptocurrency payments offer the path of least resistance for criminals and drives the exploitive nature in the ecosystem. Criminals find use from cryptocurrency's instant and borderless transactions while other open-source software helps to quickly move funds between wallets. Ransomware cyber-attacks are growing since 2020 and typically demand payment in Bitcoin or other cryptocurrencies.[36] This overshadows the positive utility of cryptocurrency for the U.S. military as the current objectives are focused on targeting threat actors who embrace digital assets.

The impact of cryptocurrency on climate change and the debate surrounding associated energy demands also hinder the adoption for the U.S. government. The Bitcoin

[36] Leandro Berg, "RTF Report: Combatting Ransomware," Institute for Security and Technology (IST), accessed August 13, 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.

protocol operates on a proof-of-work blockchain process which requires computers to solve a complex algorithm to create new digital coins. Bitcoin miners often employ hundreds of computers solely dedicated to the mining process and use tremendous amounts of energy. Some nations have banned the practice of cryptocurrency mining and other institutions have paused adoption of cryptocurrency until a more sustainable mining option is available.[37] The U.S. Department of Defense could anticipate tough questions from politicians and constituents concerned about the negative impacts of higher energy consumption with more adoption of proof-of-work cryptocurrency.

4. Current Gap in Research

The idea for operational use of cryptocurrency in SOF units is a critical gap in research and reveals a seam for financial technology applications in national defense. The private sector is far more advanced in their infrastructure and broad ecosystem which scaled rapidly to support growing international demand. Ukraine's rapid adoption of cryptocurrency supports the opportunity for USSOF personnel to apply a suite of value toolbox with cryptocurrency and help lean forward with building proficiency in cryptocurrency to support future moments of crisis and infrastructure collapse.[38]

Sara Dudley's article in Strategic Latency Unleashed offers a comprehensive synopsis of cryptocurrency implications for U.S. national security yet remains SOF-centric with a rare insight for harnessing the benefits. Dudley states, "SOF forces employing disruptive tactics offer commanders nonkinetic solutions and means to affect both the full spectrum of conflict and broad-ranging adversaries. Utilizing latent cryptocurrency capabilities in both a defensive and offensive way represents a viable disruptive, nonkinetic capability SOF might bring to the competitive gray space short of armed conflict."[39] After

[37] Harald Vranken, "Sustainability of Bitcoin and Blockchains," *Current Opinion in Environmental Sustainability*, Sustainability governance, 28 (October 1, 2017): 1–9, https://doi.org/10.1016/j.cosust.2017.04.011.

[38] Danny Nelson and Anna Baydakova, "Ukraine Leads Global Crypto Adoption, Chainalysis Says in New Report," September 8, 2020, https://www.coindesk.com/markets/2020/09/08/ukraine-leads-global-crypto-adoption-chainalysis-says-in-new-report/.

[39] Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. 278.

acknowledging the potential of cryptocurrency use in SOF, leaders in the SOF community should push for more research and development to make sense of the cryptocurrency ecosystem and prioritizes where to start for the tactical end-user.

At minimum SOF units should improve education and local training in the digital asset ecosystem to allow for greater awareness on the battlefield and be capable of supporting alternative transaction methods if requested by critical partners and allies in the future. SOF may embrace cryptocurrencies inherent characteristics and begin overt testing with the top two cryptocurrencies, Bitcoin and Ethereum. Many special operations units operate with the grassroots individuals knowledgeable with cryptocurrency such as in Eastern Europe, Southeast Asia, and Africa. This raises the prospect that Special Operations Forces may be a primary tool for research and development into how to leverage the cryptocurrency ecosystem both in training environments and during deployments.

II. SOF AS THE INCUBATOR

A. THE CULTURE OF SOF AND INNOVATION

The Russian invasion of Ukraine serves as a catalyst for exploring the implications of cryptocurrency on the battlefield. As Eliot Cohen articulated in *Commandos and Politicians*, historically commando units are directed to assist in innovation by testing new concepts which are then shared with the broader national security enterprise.[40] Special operations units continue to serve as a laboratory to inject new ideas and technology into the force by applying rapid prototyping techniques which combine professional military education and cognitively flexible members and incubators.[41] Case studies on innovation in the military are well documented but one trait commonly referenced for successful diffusion is driven by organizational and leadership culture toward innovation, specifically referenced by scholar Stephen Rosen. "Winning the Next War" by Rosen proposes that innovation is often best accomplished during peacetime but does face significant barriers of adoption from conventional incentive structures and timelines.[42] By comparison, special operations organizations offer the most flexibility for career progression, funding, and typically provide senior leader support for mavericks and small teams championing new concepts. SOFWERX is one available "maker-space" or incubator resource for SOF to help source solutions through research and development. The unique authorities and acquisitions processes required to maintain a competitive edge in emerging technologies is acknowledged by SOF leadership and supported through DOD and the National Security Innovation Network.

Elite cross functional teams are often granted the time and space to test, measure and educate the force on novel use cases and recommendations for adoption. Elite unit

[40] Eliot A. Cohen, *Commandos and Politicians: Elite Military Units in Modern Democracies*, Harvard Studies in International Affairs, no. 40 (Cambridge, Mass.: Center for International Affairs, Harvard University, 1978).

[41] Leo Blanken, "Special Operations Forces as a Rapid Prototyping Laboratory," ed. Philip Swintek, *Center for Global Security Research*, January 2021, http://hdl.handle.net/10945/67924.

[42] Stephen Peter Rosen, *Winning the next War: Innovation and the Modern Military*, Cornell Studies in Security Affairs (Ithaca, NY London: Cornell University Press, 1994).

support to cyber operations is increasingly important as the necessity to mitigate risk and improve tactical fidelity through cyber technology is too large to ignore. Many special operations security practitioners understand that expanding irregular warfare capabilities and authorities may present opportunities to update doctrine or tactics. Special operations forces can access their international footprint and partnerships to experiment while providing feedback regarding digital asset adoption to assist U.S. policymakers.

In *Strategic Latency Unleashed*, Blanken and Swintek describe the benefits to prototyping and offer that "SOF forces are the most capable of weaving research activities into their operations. Through their careful selection and training processes and lean organizational design, SOF possess the cognitive and operational flexibility to integrate prototyping nimbly and responsibly. Through thoughtful planning that leverages a dedicated network of PME-based researchers and "customers," the joint force could fruitfully utilize SOF units as a global laboratory for innovation."[43] SOF could benefit from rapid experimentation and connection to commercial company developers to test mobile applications that navigate the digital asset ecosystem and create custom solutions for each region or tactical element.

As the first steps are taken through education, units must show a willingness to collaborate across government agencies and departments, which has become standard practice for many special operations units. For the U.S. special operations community to experiment responsibly with cryptocurrency, it is imperative to collaborate with the U.S. Department of Commerce, Department of Treasury, and The Office of Science and Technology Policy to follow cutting edge guidance and regulation while sharing educational tools or training opportunities. Approving new cryptocurrency instruments in the operator's toolbox can help the United States remain agile and reinforce its position as a preferred partner around the globe. SOF units understand the importance of building relationships and establishing trust through working groups with interagency partners will

[43] Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. 322.

help illuminate adversary activity while ensuring SOF tactical end-users maintain awareness of shifting policy for cryptocurrency.

A formal mechanism will be required to ensure feedback is shared effectively. The Theater Special Operations Commands (TSOC) are forward deployed subordinate to each Geographic Combatant Command (GCC) and could facilitate intelligence reports and deployment summaries from tactical units. The TSOCs are positioned to serve as the interlocuter for real-time tactical insights and other U.S. government organizations impacted by financial technologies.

Beyond U.S. borders, developing nations lead global rankings for cryptocurrency adoption, which corresponds neatly with the extensive special operations footprint around the world.[44] USSOF should add a "fiscal preparation of the environment" component to deployment reports which includes analysis of digital asset activity to help capture broad economic variables inside their assigned region.[45] A real-time tactical perspective can offer indicators and warnings for adversary use of cryptocurrency or friendly forces sentiment and activity with cryptocurrency. SOF teams often serve as complimentary sensors on the ground to help gather human dynamics and strengthen information gathering capabilities.

B. A SHIFT IN STRATEGY FOR SOF

As competition on the world stage continues, the lines may continue to blur between legacy special operations and irregular warfare methods to keep pace in an era of strategic competition. The development of non-kinetic options for military practitioners are increasingly more valuable as operations to counter nation state adversaries generate extreme risk. The shift to strategic competition and integrated deterrence takes time and requires deliberate training validation processes prior to operational approval. SOCOM holds the largest percentage of financial management service members in the defense

[44] Chainalysis Chainalysis Team, "2022 Global Cryptocurrency Adoption Index," Chainalysis, September 14, 2022, https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/.

[45] Christian Breede, Kevin Stringer, and Sara Dudley, "A Counter-Threat Finance Approach to Competition," The Politics of Special Forces, n.d., https://podcasts.apple.com/us/podcast/episode-2-a-counter-threat-finance-approach-to-competition/id1553806860?i=1000557143750.

enterprise and demand for comptrollers' expertise may rise if financial technology integrates into pilot programs. As tactical teams observe more digital asset activity on the battlefield, comptrollers should be leveraged to improve battlefield forensics and analysis for cryptocurrency hardware and software. The integration of new occupational specialties with tactical teams is typically embraced by SOF and the shift in strategies demands a wider use of cross-functional teams and diverse expertise.[46] U.S. adversaries continue to apply dual-use technologies to disrupt traditional global order and influencers of power. China, as the pacing threat for the United States, may see digital assets as an offset technology to create overmatch during competition or crisis phase and help avoid direct military to military engagements.

China obtained first mover advantage by launching an active central bank digital currency, with plans to compete through the deployment of their digital yuan and leverage international one belt one road infrastructure to overlay new CBDC access points and continue expanding their influence.[47] Russia recently announced plans to launch a digital ruble and develop mutual settlements with China's digital yuan.[48] Time is of the essence for U.S. security strategies to account for current conditions where competitors and adversaries are actively employing dual purpose technologies such as Huawei for hardware and software development which comes outfitted to integrate digital asset tools.[49] It is difficult to anticipate the future intersection of global currencies, digital assets, and U.S. security strategies but expertise in all subsections of digital assets will likely be required to compete effectively.

[46] Davis Winkie, "New MOS and Formations Could Come to Army Spec Ops in Tech-Savvy Era," Army Times, July 2022, https://www.armytimes.com/news/your-army/2022/07/28/new-mos-and-formations-could-come-to-army-spec-ops-in-tech-savvy-era/.

[47] Darrell Duffie, "Can China Conquer Crypto?," *Foreign Affairs*, September 2, 2022, https://www.foreignaffairs.com/articles/china/2022-04-22/can-china-conquer-crypto.

[48] Reuters, "Russia Plans to Use Digital Rouble in Settlements with China, Says Lawmaker," *Reuters*, September 26, 2022, sec. Currencies, https://www.reuters.com/markets/currencies/russia-plans-use-digital-rouble-settlements-with-china-says-lawmaker-2022-09-26/.

[49] M Kimani, "China Leads Africa's Digital Currency Race," Yahoo, Michael, February 2021, https://finance.yahoo.com/news/china-leads-africa-digital-currency-202250648.html.

The U.S. should recommend more collaboration with tactical units to apply financial technology tools at the edge of conflict areas which will add non-kinetic options to better compete and strengthen alliances. Cryptocurrency may appear to serve a marginal role in security cooperation and partner building, however in developing regions with unstable national currencies, there is potential for higher rates of adoption than anticipated. The U.S. military could take a niche approach through special operations forces to help monitor adoptions rates and identify moments cryptocurrency or other digital assets serve U.S. security cooperation objectives.

Starling Labs is an academic research center that developed a new method to document Russian war crimes in Ukraine and prevent misinformation or entropy of evidence online. The lab was co-founded by Stanford University and University of Southern California's Shoah Foundation with collaboration from a global enterprise to include Hala Systems. Titled, Project Dokaz Alliance, the effort utilizes components of blockchain and cryptocurrency technologies to securely capture evidence of war crimes for use by the International Criminal Court.[50] The principles of transparency and immutability of blockchain technology allow for the data to be captured accurately and securely managed. "This process establishes the provenance of the data and allows prosecutors to prove it has not been tampered with from the field to the courtroom."[51] This example provides nonkinetic and irregular effects to hold U.S. adversaries accountable and support broader integrated deterrence strategies. Filecoin is the cryptocurrency used to support Project Dokaz by helping to incentivize users on the data storage and retrieval network. USSOF could apply research efforts to either expand upon Project Dokaz or build additional applications on Filecoin and IPFS replicating the secure processes Starling Labs developed for Project Dokaz.

[50] University of Southern California, "Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court," USC Shoah Foundation, June 10, 2022, https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes.

[51] University of Southern California.

C. A DRIVER OF CHANGE FOR POLICY IN DOD

As SOCOM continues to answer responsibilities for countering threat financing, a demand for education and training in cryptocurrency may emerge for tactical special operations units to compliment current processes and systems. SOCOM is chartered as DOD's lead and coordinating authority for counter threat finance. This requirement has allowed SOCOM to establish interagency relationships which could help tactical units maintain awareness of the latest U.S. guidance for digital assets. Former USSOCOM commander, General Raymond Thomas, in a 2017 posture statement to the U.S. Senate referenced the active support to interagency efforts and pointed to SOCOMs leading role for DOD in CTF.[52] U.S. DOD directive number 5205.14 *DOD Counter Threat Finance (CTF) Policy* originally released in 2010 and now incorporates changes from 2017 assigns responsibilities for countering terror financing, illicit trafficking, and other related adversary activities.[53] The policy window is opening for USSOCOM and tactical units to help illuminate threats and opportunities for financial technology and use existing relationships from the Global War on Terror's (GWOT) counter threat finance activities.

On U.S. SOCOM's website, the *SOCOM Vision and Strategy* report references the need to "innovate for future threats" and offers that "Over the next 10 years, we will modernize SOF, pioneer dynamic and unorthodox approaches (including the full toolkit associated with irregular warfare), leverage emerging technologies to mitigate adversarial activities by China, and create asymmetric advantages for current and future conflict."[54] One innovative step forward could be to leverage current counter threat financing expertise and programs of instruction to expand or adapt training pathways for tactical units to test and experiment with cryptocurrency.

[52] *Statement of General Raymond A. Thomas, U.S. Army Commander United States Special Operations Command Before the Senate Armed Services Committee*, 115th Cong. (2017) (statement of Raymond A. Thomas, USSOCOM Commander).

[53] Department of Defense, *DOD Counter Threat Finance (CTF) Policy*, DOD Directive 5205.14 (Washington, D.C: Department of Defense, 2017), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520514p.

[54] USSOCOM, "SOF Vision and Strategy" (Tampa, FL: U.S. Special Operations Command, April 11, 2022), https://www.socom.mil/sof-vision-and-strategy.

The overlap between cryptocurrency and SOCOM's CTF charter creates an opportunity space for SOF to take an important role in improving U.S. and partner nation education, testing, and application of cryptocurrency tools. Special operations units inherently offer the culture, capacity, and calculations to serve as the Department of Defense's driver of change for cryptocurrency technology and could help experiment with the costs and benefits for utility of cryptocurrency. This would allow the United States to shape global cryptocurrency adoption with the intent of countering nefarious activity and modernizing security strategies, while concurrently enabling economic development for our allies. Special operations forces, in particular, have a rich opportunity to embrace an irregular approach by leveraging key aspects of cryptocurrency that offer a menu of non-standard means of communication, digitized payments, and access to global communities, often with pseudonymity. By initiating the processes to test cryptocurrency, the SOF community can help identify what levels of adoption or curiosity are present in U.S. military formations and partner forces around the globe.

The bureaucracy and cumbersome defense enterprise is an issue for disruptive technology adoption, but there are signs of successful digital asset adoption in niche use cases and specialized military units. *Forging the Sword* by Benjamin Jensen highlights the importance of incubators and advocacy networks which USSOF has embraced through maker spaces down to the battalion level.[55] USSOF improved talent management and organized technical support formations to create environments conducive to successful innovation. Everett Rodgers wrote Diffusion of Innovation in 1995 but the five key factors are still useful: relative advantage, compatibility, complexity, trialability, and observability.[56] The relative advantage of cryptocurrency in developing regions may drive adoption the most among Rodgers' five factors, as populations face volatile national currency and limited access to U.S. dollars.

[55] Benjamin M. Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, California: Stanford Security Studies, an imprint of Stanford University Press, 2016). 17–19.

[56] Everett M. Rogers, *Diffusion of Innovations*, 4th ed (New York: Free Press, 1995).

THIS PAGE INTENTIONALLY LEFT BLANK

III. CONCEPTS FOR CRYPTOCURRENCY UTILITY

A. CRYPTOCURRENCY ON THE WORLD STAGE

U.S. citizens may struggle to see value beyond U.S. dollars (USD) however, individuals living in other countries may desire options outside of their nations denominated currency or even struggle to acquire USD. Cryptocurrency payment rails offer enticing cross-border transaction alternatives for remittances since fees over some blockchains can provide faster and cheaper means to reach family members' digital wallets.[57] The instability in Afghanistan and limited rights for women negatively impacted their access to financial infrastructure. Despite those challenges, some women in Afghanistan managed to build systems leveraging cryptocurrency combined with traditional hawala networks to receive donations or remittances and transition between fiat currency in Afghanistan.[58] The combination of a legacy hawala systems and cryptocurrency inside a nation with volatile infrastructure sheds light on the creativity for cryptocurrency opportunities compared to traditional finance systems.

Cryptocurrency and stablecoins offer developing regions access to global trade and have potential economic upsides in the future. National currencies in developing regions suffer from price volatility, often triggered by corruption or domestic conflicts, which can lead some communities searching for alternative stores of value. Many digitally native generations who were raised on mobile payment applications such as M-Pesa in East Africa, may continue to adopt emerging cryptocurrencies and other digital assets. If private stablecoins such as Circle's USDC and Tether's USDT, receive better oversight and possible global standards, digital natives may embrace more reliable alternate stores of value.

[57] Hugo Renaudin, "Remittance and Payments: Crypto's Big Opportunity in Latin America," accessed October 27, 2022, https://www.nasdaq.com/articles/remittance-and-payments%3A-cryptos-big-opportunity-in-latin-america-2020-08-06.

[58] Joshua Zitser, "Impoverished Afghan Women Are Receiving Emergency Aid in Crypto as the Taliban Limits Cash Withdrawals and Millions Go Hungry," Business Insider, accessed October 27, 2022, https://www.businessinsider.com/afghanistan-women-turn-to-cryptocurrency-to-feed-their-families-2022-1.

Bitcoin and other decentralized digital currencies can offer additional support to populations burdened under autocratic regimes. One example to emulate, during the COVID-19 health crisis, the United States approved support for oppressed health care workers and transferred humanitarian aid directly to Venezuelan citizens in the form of cryptocurrency to avoid a tightly controlled domestic financial system.[59] This example reveals how the alternative financial ecosystem of cryptocurrency allowed access to populations when traditional payment mechanisms were constrained or unable to complete the transaction.

Ultimately, cryptocurrencies inherent nation agnostic origins may provide an irregular option for the U.S. to deliver military aid for resistance elements while partially reducing signature and the associated risk with physical U.S. dollars. In regions with compromised smart city technology or robust digital firewalls, cryptocurrency communities with censorship resistance and privacy conscious culture offer unique ways to mitigate risk for oppressed populations and better circumvent adversary cyber controls.

In late 2022, Taiwan's Ministry of Digital Affairs adopted a decentralized protocol to help improve cybersecurity defenses and infrastructure resiliency in the face of Chinese aggression.[60] The public protocol is called the InterPlanetary File System (IPFS) which stores data across and wide network of nodes which removes centralized points of failure or expensive file storage servers. Decentralized file sharing systems are not new, however IPFS is unique by building a system intended to be interoperable with blockchains. Protocol Labs is the open-source research and development laboratory maintaining IPFS to facilitate growth. Filecoin which is a cryptocurrency built to incentivize peer-to-peer file storage and retrieval with IPFS helps the network maintain active users and nodes.[61]

[59] Gideon Long, "Digital Scheme Pays Venezuela Health Workers from Frozen Funds," Financial Times, December 10, 2021, https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18.

[60] Jason Nelson, "Taiwan Turns to Ethereum IPFS Tech to Thwart Chinese Cyberattacks," Decrypt, August 11, 2022, https://decrypt.co/107293/taiwan-turns-to-ipfs-tech-to-thwart-cyberattacks-from-china.

[61] "About Protocol Labs," Protocol Labs, accessed November 20, 2022, https://protocol.ai/about/.

B. MODERNIZE PARTNERSHIPS

The value proposition for cryptocurrency in special operations lies beyond the basic financial transaction component. In certain conditions, service members may find payments in virtual currencies help reduce both digital and physical signatures by removing transactions in U.S. dollars. This characteristic is undoubtedly helpful, but the potential to customize applications with cryptocurrency "software" for smart contracts or peer to peer communication highlights the underlying human dynamic where SOF units should build capability. SOF has an opportunity to monitor a pulse on shifting trends in financial technology and identify exquisite capabilities using cryptocurrency specific DApps tailor made for SOF operations which could prove valuable in future irregular warfare concepts.

The network effect of cryptocurrencies may be an underappreciated aspect however, not in the traditional finance sense, but for increasing access to new communities and populations.[62] The internet-based economy of cryptocurrency encourages network growth beyond borders and may help incentivize niche information gathering opportunities through surveys, fundraising for war efforts, or remote education and training concepts with foreign allies. "Over-the-horizon" or remote advise and assist operations are now more common with the proliferation of digital tools and applications to share information. The commercial sector is beginning to merge communication, financial, and social platforms together which stimulates the network growth of cryptocurrency as they become interoperable on everyday social platforms.

Foreign policy experts and military professionals should heed the advice on networks from John Arquilla who writes extensively on the topic; "leveling networks as actors of equal importance to nation-states" and highlights that networks often serve as counterweights to nation-state hegemon.[63] The emerging decentralized communications market connected to cryptocurrency may allow alternative methods for USSOF and partner

[62] Daniel Roberts, "How Crypto Adoption by Companies like Visa, PayPal, and Tesla Is Creating a Network Effect," Yahoo, February 2021, https://finance.yahoo.com/news/how-crypto-adoption-by-companies-like-visa-pay-pal-and-tesla-is-creating-a-network-effect-214639389.html.

[63] John Arquilla, "Of Networks and Nations," *The Brown Journal of World Affairs*, no. 14.1 (2007): 199–208, http://bjwa.brown.edu/14-1/of-networks-and-nations/. Pg 208.

forces to communicate over the internet. For example, the Bitcoin Lightning Network sparked a new company named, Impervious.ai which created an entirely new communication protocol and browser which uses the lightning network for secure peer-to-peer interaction.[64] There is potential for cryptocurrency to drive partner force preferences for communication platforms interacting remotely or over-the-horizon and USSOF members should be prepared to connect and interact appropriately.

1. Assist in Targeting and Network Analysis

The U.S. could leverage special operators experience and expertise for targeting methodologies in both steady state and conflict by combining blockchain network analysis with human dynamics in the operational environment. Comptroller's in SOCOM could supplement tactical targeting and analysis efforts for SOF units and the wider interagency working groups for digital assets. The transparency of cryptocurrency blockchains offers a unique ability to analyze and control sanctions but also create risk by publicly identifying individual transaction history.[65] This capability provides a double-edged sword as adversaries can observe the same transaction activity.[66] However, this does not dismiss the potential for effective pseudonymous transactions or communication but does require an increased level of training and knowledge with the cryptocurrency ecosystem. If training and education in the digital currency environment improves, U.S. military advisors can recommend best practices for targeting adversaries and managing the risks from cryptocurrency's transparent and immutable ledgers.

The United States improved techniques to counter terror financing and illicit drug finance networks over the last 20 years however, a plethora of laundering opportunities

[64] Impervious, "Impervious Project," Your Portal to the P2P Internet, accessed October 31, 2022, https://www.impervious.ai/.

[65] Adam Myers et al., "Crypto-Controls: Harnessing Cryptocurrency to Strengthen Sanctions," War on the Rocks, December 9, 2020, https://warontherocks.com/2020/12/crypto-controls-harnessing-cryptocurrency-to-strengthen-sanctions/.

[66] Chainalysis Team, "Transparency in Blockchains Senate Hearing," Chainalysis, March 22, 2022, https://blog.chainalysis.com/reports/senate-hearing-underscores-value-of-blockchain-transparency/.

still exist globally, and cryptocurrency has only added to the menu.[67] Contrary to popular opinion, many financial task force experts focused on disrupting terror finance will argue cryptocurrency laundering is overstated and offers a valuable forensic tool.[68] In order for SOF to work safely and effectively with cryptocurrency and blockchains, units will need to incorporate these techniques into "hands on" training where U.S. comptroller's monitor USSOF and partner activity of the blockchain to mitigate risk prior to operational use.

In 2018 ISIL support networks were using steganography techniques to embed messages in images sent over messaging applications and transparent blockchain ledgers while leveraging open-source coding tools to encrypt the communication in plain sight.[69] This level of expertise is not difficult to attain but it must start with basic, overt employment of cryptocurrencies to build proficiency. U.S. military units should begin experimenting with cryptocurrency software and hardware tools in training scenarios to establish a low-risk baseline before attempting complex methods to obfuscate transactions or recommend options to allies. A training event which incorporates cryptocurrency could benefit from dual-purpose education by allowing tactical teams to experiment and simultaneously integrate blockchain forensics from intelligence or comptroller analysts as "red-hat" counterparties.

Comparable to financial intelligence tools which search networks for illicit activity, the transparent ledgers of most digital currencies can help improve accountability of foreign military aid. The digital breadcrumbs from blockchain transactions may lead to better oversight and management of rapidly procured funds or at minimum share insight to the level of digital currency adoption. Immediately after Russia invaded Ukraine in 2022, cryptocurrency donations flooded to Ukrainian government cryptocurrency wallet addresses. However, a more organized and pre-planned distribution system may have

[67] Laura Jones and Shawna Sinnott, "Money Talks: How Nonstate Armed Groups Finance Their Operations and Organizations," Modern War Institute, July 15, 2022, https://mwi.usma.edu/money-talks-how-nonstate-armed-groups-finance-their-operations-and-organizations/.

[68] Michael Morell, Josh Kirshner, and Thomas Schoenberger, "Report: An Analysis of Bitcoin's Use in Illicit Finance," The Cipher Brief, April 13, 2021, https://www.thecipherbrief.com/report-an-analysis-of-bitcoins-use-in-illicit-finance.

[69] Lily Hay Newman, "Mysterious 'MuslimCrypt' App Helps Jihadists Send Covert Messages," *Wired*, accessed October 27, 2022, https://www.wired.com/story/muslimcrypt-steganography/.

allowed more time and space for the United Nations to vote and structure support efforts. Additionally, an immediate and deliberate U.S.-led blockchain network analysis system may have offered better insight to Russian digital breadcrumbs over cryptocurrency networks to evade sanctions and help fund the invasion. USSOF should work towards building a structured cryptocurrency and blockchain targeting standard operating procedure with NATO and other allies before the next crisis occurs.

2. Cyber Partnerships and Information Gathering

Ukraine continues to provide a relative roadmap for cryptocurrency utility in support to allies and partners as the threats and opportunities are displayed for the world to take note.[70] As cryptocurrency donations to Ukraine surpassed 50 million U.S. dollars, the Ukrainian government realized the grassroots appeal for many foreigners around the world who are now able to provide modest support through micro-payments and avoid traditional banking fees and limitations.

The Ukrainian government's decision to include cryptocurrency donations and crowdsource military support after an invasion, is a great example of the potential utility of cryptocurrency in conflict areas and offer transparency with blockchain data.[71] The cryptocurrency broker in Ukraine, Kuna Exchange, revealed how the modernized hybrid banking system helps to finance a resistance movement or government during conflict and maneuver between the fiat currency market and cryptocurrency to meet the needs of customers.[72] Ukraine's banking system collapse during the Russian invasion revealed another example for the benefits to self-custody of digital currencies for emergencies, especially in unstable regions.

[70] Ananya Kumar and Nikhil Raghuveera, "Can Crypto Deliver Aid amid War? Ukraine Holds the Answer.," *Atlantic Council* (blog), April 4, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-answer/.

[71] United 24, "Aid For Ukraine – Donate Crypto to Ukraine," United 24: The initiative of the President of Ukraine, accessed October 27, 2022, https://u24.gov.ua/.

[72] Romain Dillet, "How Ukraine Is Spending Crypto Donations," *TechCrunch* (blog), March 2, 2022, https://techcrunch.com/2022/03/02/how-ukraine-is-spending-crypto-donations/.

In Eastern Europe "hunt forward" operations by allies with assistance from U.S. units help disrupt nefarious cyber activity. Cyber partnership training and execution complimented with special operations units is long overdue and will strengthen alliances and increase the value proposition for U.S. tactical forces.[73] Cryptocurrency expertise can be an important component of cyber security operations, and the U.S. defense enterprise will improve partnered cyber capability after innovating in the cryptocurrency ecosystem.

Some emerging technologies apply in all aspects of special operations and quickly scale to become unavoidable in conflict such as drones and mobile phones. One commonality among technological innovations are the vulnerabilities at the human layer either through faulty developer code or human end user errors. This analogy exists with cryptocurrency and typically dominate the headlines as speculative traders or greedy business owners will exploit cryptocurrency development and underlying software. An Article in the Cyber Defense Review outlines a value proposition for SOF personnel working in the cyber domain. The authors touch on the human vulnerabilities, often connected to social engineering, that erode cyber security measures. They present the idea SOF should be requested to apply human domain skill sets to defend or disrupt efforts in the cyber domain.[74] USSOF's diverse footprint offers a unique ability to interact with local populations and partner forces to illuminate cryptocurrency sentiment and potentially apply in supplemental security cooperation incentives or better compete with adversary strategies.

The U.S. military community is working to build a closer relationship between U.S. special operations forces, space, and cyber. A recent article published in the *Army Times* outlines the debate for adding more technical skills in operational detachments or tactical units of action.[75] The article references a growing partnership between SOF, cyber, and space departments to support strategic competition and demands for specialized tech-based

[73] Mark Montgomery, "Equipping U.S. Partners in Cyberspace Is a Must," The Cipher Brief, July 2022, https://www.thecipherbrief.com/column_article/equipping-u-s-partners-in-cyberspace-is-a-must.

[74] Patrick M. Duggan and Elizabeth Oren, "U.S. Special Operations Forces in Cyberspace," *The Cyber Defense Review* 1, no. 2 (2016): 73–80, http://www.jstor.org.libproxy.nps.edu:2048/stable/26267360.

[75] Winkie, "New MOS and Formations Could Come to Army Spec Ops in Tech-Savvy Era."

skills. Many blockchain based applications which utilize cryptocurrency transactions to manage costs and incentive structures are not simple to use. If additional skillsets are delivered to SOF units, it will support practical applications for cryptocurrency in offensive operations. Cryptocurrency may grow to become one of the preferred currencies in cyber domains or the information environment and SOF could begin understanding the atmospherics through surveys in USSOF formations then expand to partner forces and foreign populations in areas of operation.

Emerging peer to peer communication and transaction tools like cryptocurrency may offer a vital bridge between the digital and human domain where elite units excel at building partner capabilities or gathering ground-truth information to help identify adversary vulnerabilities. As the SOF, cyber, space triade continues to build and integrate into training and operations, the diverse backgrounds and expertise in these formations could build creative and region-specific solutions on blockchain and cryptocurrency technology.

3. Include in Resistance Operating Concepts

Digital assets can help concepts in support resistance modernize by offering methods that reduce signature, embrace decentralization, resist censorship, leverage the cyber domain, and serve units with agility and speed. A pragmatic perspective of cryptocurrency will see the innovation simply as software that is programmable for specific decentralized applications. This view helps to determine use cases outside of standard digital financial transactions and check if a solution exists using a cryptocurrency protocol to build a smart contract or DApps. *The Resistance Operating Concept* released by the Joint Special Operations University was developed in conjunction with Baltic and NATO partners.[76] Despite offering immense information for both military and civilian roles in a resistance, the document does not include details for financial technology techniques or capabilities.

[76] Otto C. Fiala, *Resistance Operating Concept (ROC)* (MacDill Air Force Base, Florida: The Joint Special Operations University Press, 2020).

Many of the Baltic nations are applying the resistance operating concept and U.S. Special Operations Command Europe increased assistance to Baltic allies after Russia's annexation of Crimea in 2014.[77] The alternative digital payment rails embraced by Russia, are now leveraged against them by cryptocurrency savvy resistance leaders who understand the processes to procure physical goods and services using in-expensive and commercially available cryptocurrency with satellite internet.

In the *Resistance Operating Concept*, several key networks are necessary to be successful and the underground component is referenced to have "the greatest and most varied responsibilities. Each function should be established and organized prior to a crisis."[78] Financing is outlined as one of the seven key functions of the underground component of a resistance. The financing section of the book further drives home the importance or pre-planning, "Resistance organizations are often aided by allied or partner nations. In fact, we have stressed, these relationships are best begun prior to a crisis through joint training, information exchanges, agreements, and planning coordination."[79] If cryptocurrency was incorporated into resistance planning concepts prior to the Russian invasion in 2022, Ukrainian partners may have seized an opportunity to swap fait currency held in local banks to stablecoins or Bitcoin and remain agile pre-crisis. A cache of emergency funds stored on a cryptocurrency hardware wallet could help purchase both humanitarian and military aid but also allow for resistance leadership access to liquidity or alternative currency to expedite transactions locally. The traditional banks surrounded by a crisis or conflict, who are not prepared to handle instant crowdsourcing funds through digital assets may find support through resistance planning and preparation with digital assets. Substitute currency is briefly mentioned in the *Resistance Operating Concept*, but it does not reference cryptocurrency or expand upon the nuanced ways to properly handle cryptocurrency.

[77] Oren Liebermann, "How Ukraine Is Using Resistance Warfare Developed by the U.S. to Fight Back against Russia | CNN Politics," CNN, August 27, 2022, https://www.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html.

[78] Fiala, *Resistance Operating Concept (ROC)*. 39.

[79] Fiala. 51.

A central component to survivability in resistance operations is proper organizational structure, specifically decentralization, compartmentalization, and redundancy. Those traits overlap with cryptocurrency principles and begs for continued exploration to ensure consistent funding to complicated resistance operations. Figure 2 from the *Resistance Operating Concept* manual offers a cell structure template for an underground organization in a resistance movement.

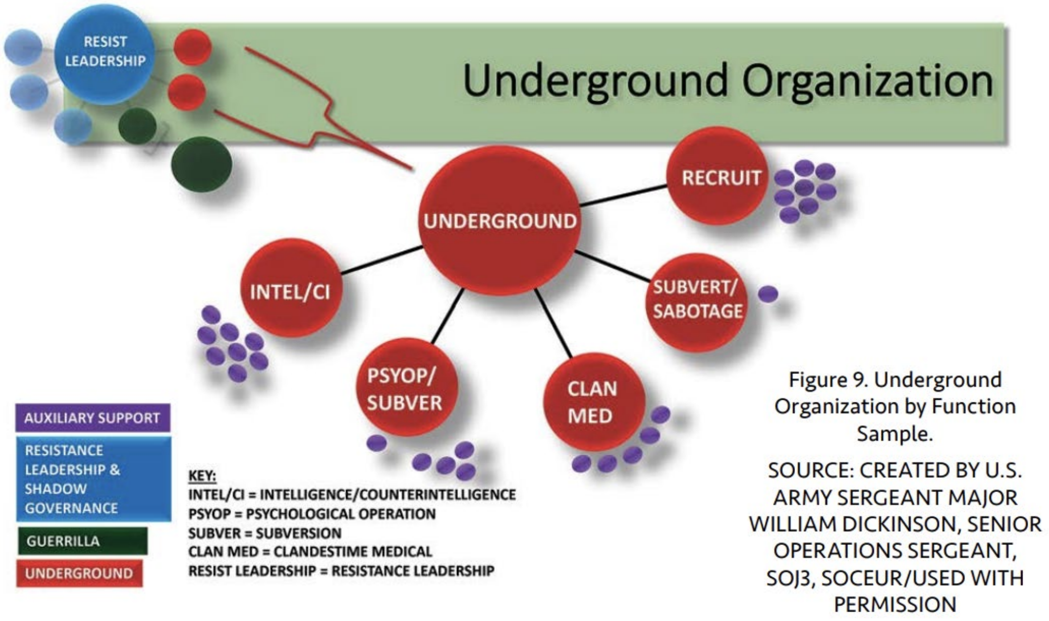

Underground Organization
RESIST LEADERSHIP
UNDERGROUND
RECRUIT
INTEL/CI
SUBVERT/ SABOTAGE
PSYOP/ SUBVER
CLAN MED
AUXILIARY SUPPORT
RESISTANCE LEADERSHIP & SHADOW GOVERNANCE
GUERRILLA
UNDERGROUND
KEY:
INTEL/CI = INTELLIGENCE/COUNTERINTELLIGENCE
PSYOP = PSYCHOLOGICAL OPERATION
SUBVER = SUBVERSION
CLAN MED = CLANDESTIME MEDICAL
RESIST LEADERSHIP = RESISTANCE LEADERSHIP

Figure 9. Underground Organization by Function Sample.

SOURCE: CREATED BY U.S. ARMY SERGEANT MAJOR WILLIAM DICKINSON, SENIOR OPERATIONS SERGEANT, SOJ3, SOCEUR/USED WITH PERMISSION

Figure 2. Example of ROC Compartmentalized Structure[80]

The compartmentalized nature of resistance organizations is necessary but difficult to match perfectly in real-world situations. Financial support cells often violate the principles of cell structure since diverse payment rails and alternative currencies are difficult to establish post-crisis or without deliberate planning. Additionally, internet connectivity is typically degraded or destroyed in regions. The Bitcoin network specifically, is built to sustain and continue in the face of catastrophic events as several

[80] Source: Fiala. 35.

companies maintain Bitcoin Lightning Network nodes through private satellites. Blockstream and GoTenna are two private companies who developed open-source software and hardware to complete transactions for individuals with no connectivity.[81] Their products utilize mesh networks and TxTenna devices, a subsidiary of GoTenna, to hop service from one node with internet backhaul along a relay of devices to reach the "last mile" or a device with no service and conduct a Bitcoin transaction.[82] The data from the transaction is later published to the blockchain with the help of the mesh network relaying the confirmation details.

Figure 3 is sourced from a research paper directed by the Bank of International Settlements in 2017. This graphic helps emphasize the opportunity to add variance in currency choices for resistance components or functions and helps planners consider the dynamic value or monetary systems around the world. Financial technologies will likely continue to expand in digital global markets which also offer new methods to communicate privately with one another. Peer-to-peer digital payment tools could be incorporated in resistance concepts to create air gaps between highly sensitive cells or build redundancy in attempts to avoid central points of failure.

[81] Daniel Williams, "GoTenna with Blockstream Satellite," Blockstream, May 11, 2019, https://blog.blockstream.com/en-gotenna-satellite-api-integration/.

[82] TxTenna, "TxTenna: Route Around Censorship," November 28, 2022, http://txtenna.com/.

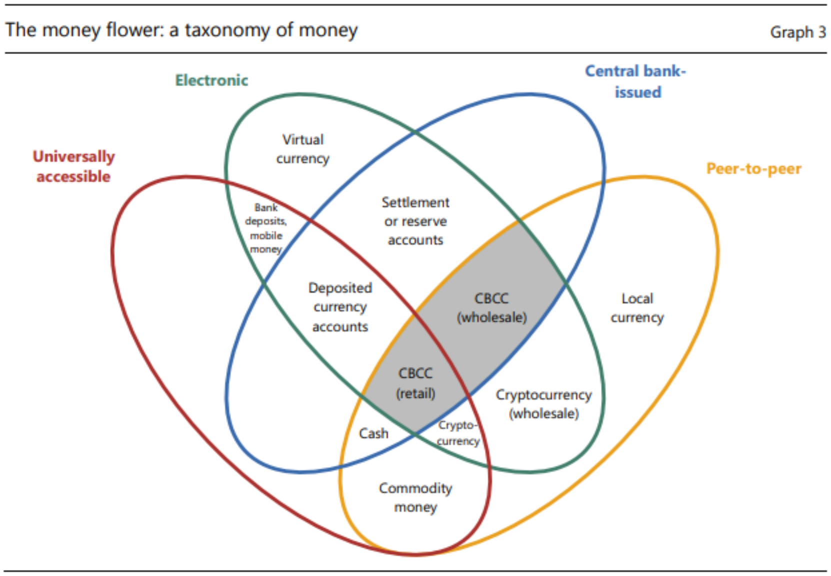


Figure 3. A Diagram Revealing Types of Money and Organizational Overlap[83]

The special operations community would benefit from a proactive discussion with foreign partners to gauge the sentiment toward cryptocurrency and highlight utility for certain special operations use cases for U.S. and allies. As the demographic in many developing regions are dominated by generations under the age of 30, security forces should embrace digitally native communities and prepare to apply cryptocurrency incentives or non-standard techniques and to break reactionary innovation cycles.

U.S. irregular warfare strategies could weaponize the cryptocurrency ecosystem and strengthen a network for integrated deterrence to supplement current contingency plans and offer alternative mediums of exchange if legacy systems are compromised. As military planners continue to refine and develop irregular warfare campaign plans; leaders should be reminded that not all irregular techniques need to be completely covert or clandestine. Some non-standard tools such as cryptocurrencies and emerging financial technologies can assist irregular warfare options by simply reducing the blatant fingerprints of physical U.S.

[83] Morten L. Bech and Rodney Garratt, “Central Bank Cryptocurrencies,” SSRN Scholarly Paper (Rochester, NY, September 17, 2017), https://papers.ssrn.com/abstract=3041906. Pg 60

dollars or wire transfers between centralized banks. Sara Dudley in *Strategic Latency Unleashed* articulates the indirect and asymmetric approach cryptocurrency offers by "harnessing this technology to address underlying causes of illicit-actor penetration into vulnerable communities might finally allow SOF forces the ability not only to fight symptoms of bad acting and terror through direct action but also to employ the will of the underlying populations effectively to effect influence on their governance."[84] The learning curve for effective and responsible employment of cryptocurrency is steep and requires iterations of training and testing. The shifting roles of U.S. special operations units and allies in strategic competition requires more flexible options to remain under the threshold of conflict while still supporting resistance campaigns like in Ukraine.

[84] Davis et al., *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. 280.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE CURRENT STATE OF BLOCKCHAIN AND CRYPTOCURRENCY

This chapter will start with a brief introduction to national defense innovation characteristics and trends cited as reasons for successful adoption. The chapter concludes with a summary and lessons learned from a NPS Blockchain Research Symposium: National Security Implications held on campus and virtually on 12–13 September 2022. The decision to organize a symposium focused on blockchain technology allowed for a larger group of participants and willingness from government organizations to consider dialogue that heavily included the contentious topic of cryptocurrencies. LTC Michael "Kelly" McCoy was the faculty lead and co-author for the symposium executive summary referenced below and the panel concepts referenced in the subsequent annexes.

A. INNOVATION ADOPTION TRAITS CRITICAL FOR SUCCESS

The reasons for successful diffusion of emerging technology vary depending on what publication and scholar but largely associate with organization culture, incubators, mavericks, leaders to champion ideas, and influence from policymakers. Benjamin Jensen's book, *Forging the Sword*, highlights the value of advocacy networks and the impact a profession has on innovation. When discussing doctrinal change in the military, Jensen offers that "cultural heuristics often bound potential solutions for battlefield challenges."[85] The idea of cultural heuristics arguably connects the debate for cryptocurrency utility and appropriateness in U.S. DOD. As referenced earlier, many U.S. citizens struggle to see value in alternative currencies, which may partially feed the heuristics to national security practitioners when conceptualizing the positive benefits to cryptocurrency. This research intends to offer a new lens to observe possible solutions to strategic competition arenas for USSOF and the broader security enterprise.

The research symposium at NPS delivered reason for optimism for responsible innovation of financial technology in DOD by connecting public and private advocacy

[85] Jensen, *Forging the Sword*. Pg 13.

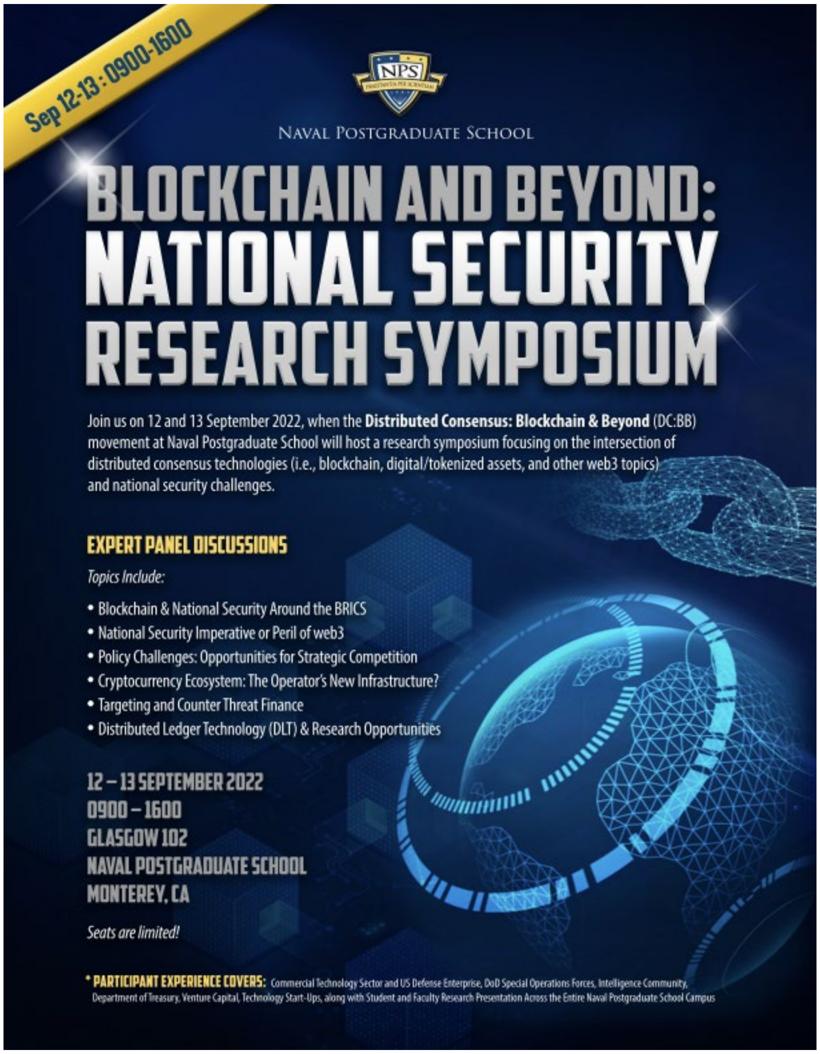
networks to incubators and mavericks. When considering Rodgers' five factors, proving relative advantage, overcoming complexity, and compatibility rise to the top as factors for slowing adoption of cryptocurrency in special operations. The headwinds facing cryptocurrency lean heavily toward those three factors and relate back to the larger narrative surrounding cryptocurrency. The connection to illicit activity slows diffusion for U.S. security practitioners and the perception that cryptocurrency is mainly used for sanctions evasions or criminal activity must shift slightly for broader application. The natural heuristics referenced by Jensen also impact the perceptions of Rodger five factors and through deliberate training and education, cryptocurrency utility may expand beyond countering threat finance.

Professional comptrollers in the CTF teams understand cryptocurrency capabilities more than most SOF personnel and will help promote the narrative for cryptocurrency and assist in the innovative approach to transfer knowledge from one sector to another. Digital assets and cryptocurrency undoubtedly face early adoption phase hurdles, but the disruptive financial technology created new opportunities to quickly move money, pay for services, reduce signature, and improve transparency at a global scale which all provides value to SOF. As leaders in DOD advocate for more capabilities in financial technology, the established base of incubators and results-based formation of special operators will likely lead to productive research and development.

B. BLOCKCHAIN AND BEYOND: NATIONAL SECURITY SYMPOSIUM

1. Background and Context

In the Spring of 2022, NPS students and faculty established the Distributed Consensus: Blockchain & Beyond (DC:BB) movement to address the general misperceptions around blockchain technologies. When it comes to present geopolitical dynamics, especially with China, the knowledge gap in these innovations come at a significant opportunity cost to the United States. Specifically, for the U.S. military, blockchain technologies offer potential advantages from supply chain management to decentralized operations. To help counter this problem, DC:BB held a research symposium to initiate a conversation on the role and impact of blockchain technologies in a national security context – with the intent to build awareness, knowledge, and connections that can propel relevant research opportunities for students and faculty at the Naval Postgraduate School (NPS). The following synopsis was written by the author and NPS faculty member LTC Michael "Kelly" McCoy and include interpretations of expert panel discussions. Figure 4 is the formal Naval Postgraduate School flyer utilized for the symposium and distributed publicly prior to the event. NPS's graphic design department designed the flyer artwork, provided materials, and conducted the printing all in house.



Sep 12-13 : 0900-1600

NPS

PRAESTANTIA PER SCIENTIAM

NAVAL POSTGRADUATE SCHOOL

BLOCKCHAIN AND BEYOND: NATIONAL SECURITY RESEARCH SYMPOSIUM

Join us on 12 and 13 September 2022, when the **Distributed Consensus: Blockchain & Beyond** (DC:BB) movement at Naval Postgraduate School will host a research symposium focusing on the intersection of distributed consensus technologies (i.e., blockchain, digital/tokenized assets, and other web3 topics) and national security challenges.

EXPERT PANEL DISCUSSIONS

Topics Include:

- Blockchain & National Security Around the BRICS
- National Security Imperative or Peril of web3
- Policy Challenges: Opportunities for Strategic Competition
- Cryptocurrency Ecosystem: The Operator's New Infrastructure?
- Targeting and Counter Threat Finance
- Distributed Ledger Technology (DLT) & Research Opportunities

12 – 13 SEPTEMBER 2022
0900 – 1600
GLASGOW 102
NAVAL POSTGRADUATE SCHOOL
MONTEREY, CA

Seats are limited!

* **PARTICIPANT EXPERIENCE COVERS:** Commercial Technology Sector and US Defense Enterprise, DoD Special Operations Forces, Intelligence Community, Department of Treasury, Venture Capital, Technology Start-Ups, along with Student and Faculty Research Presentation Across the Entire Naval Postgraduate School Campus

Figure 4. NPS Poster for Blockchain and Beyond: National Security Research Symposium

2. Notable Participants

NPS students and faculty largely represented Defense Analysis, National Security Affairs, and Computer Science departments. Industry leaders who participated included PayPal, Coinbase, Trail of Bits, Espresso Systems, Impervious, improbable.io, and many others. Outside academics and researchers include MIT, Stanford, Congressional Research Services, Starling Labs, Atlantic Council, Center for New American Security, and Lincoln Network.

3. Overview

Over the course of two days, the research symposium covered a wide range of topics ranging from comparative international perspectives on the use and role of blockchain technologies, the potential impact of blockchain technologies on U.S. national security, key policy considerations, operational utility of cryptocurrencies for special operations, use of blockchain technology for targeting, and research opportunities to explore with blockchain. The conference ended with four research presentations, which focused on use of cryptocurrency for SOF, use of blockchain for clandestine communications, contract management, and improving data resiliency through peer-to-peer data security leveraging blockchain technology.

C. TOP THREE POINTS FROM THE SYMPOSIUM

1. Blockchain Resiliency

Civilians impacted by conflict and/or political upheaval may benefit from blockchain technologies by offering immutable records such as digital identities for refugees and an alternative means to transact with digital assets when markets and economies are disrupted. Specific to the U.S. national security audience, global and borderless blockchains offer a new communication mechanism to reach populations and resist censorship or manipulation.

2. United States' Strategic Opportunity

The United States is positioned to assist allies who are looking for regulatory clarity and policy guidance to establish global norms in line with U.S. values for blockchain and digital assets. Panelists and participants noted the importance on the emergent demand for public/private partnerships to quickly improve awareness, capacity, and competency in the complex blockchain ecosystem. The DOD is too often overlooked in key stakeholder positions in U.S. government publications. Experts also routinely coalesced around the need for a whole-of-nation U.S. strategy for blockchain development.

3. Possible Geo-Political Split

Blockchain's diverse technology solutions reveal higher adoption rates with communities in developing regions, typically intended to help improve accountability in fragmented bureaucratic ecosystems (medical records, financial inclusion, federated licensing, and credentials) especially when applied through zero knowledge proofs. There is potential for a divergence in blockchain development and adoption between authoritarian regimes and democratic nations, underscoring the need to understand the implications of blockchain technology in U.S. national security strategies.

D. RECOMMENDED NEXT STEPS

1. Develop Partnerships between Industry, Researchers, and NWSI

Naval Postgraduate School (NPS), with their technical focus and expertise, undercurrent of strategic art and policy proficiency, and intent to support the warfighter in all that they do, is uniquely situated to lead in the exploration of building out research opportunities for blockchain technologies. As highlighted in the key findings, partnerships within this space are the key to moving forward and NWSI is specifically designed for this intent. Developing partnerships with industry leaders like Coinbase, PayPal, and others will be critical to successful adoption of blockchain technologies.

The Post-Conference Actions Taken: One introductory meeting has been completed between NWSI and Coinbase, with follow-on intent to develop education, training, and internship opportunities focused on understanding how to conduct blockchain intelligence analysis.

2. National Security and Blockchain Coalition of the Willing

Establish a decentralized open community of national security professionals, academics, researchers, and industry leaders. The initial intent of the Coalition of the willing (CoW) is to provide a space where information and opportunities focused on distributed ledger technologies and national security can be shared. As the CoW takes shape, we will respond to member demand and create additional opportunities for ideas, research, and opportunities to be shared amongst the group.

The Post-Conference Action Taken: Symposium attendees have been invited to join the Blockchain CoW channel on Signal.

3. Identify Sponsorship for Blockchain Technology Experimentation

As a general-purpose technology, blockchain provides a wide breadth of opportunities. However, given its nascent status in DOD there is little to no understanding how best to employ it. DC:BB recommends identifying either an institutional (U.S. Army Futures Command) or operational (USASOC) command who could serve as an intended sponsor for research and experimentation on blockchain technologies.

Post-Conference Actions Taken: This current thesis work, sponsored by USASOC, explores the utility of cryptocurrency in supporting special operations. This thesis is best situated to demonstrate value and grow opportunity for an enduring sponsorship.

E. PANEL 1: COMPARATIVE PERSPECTIVES FROM AROUND THE WORLD ON BLOCKCHAIN ADAPTATION

1. Objective

The goal of this panel was to focus on a geo-political level and offer a stratospheric view for the audience. The discussion was intended to help articulate how emerging technology is influencing the changing dynamics for the BRICS nations and set the tone for following topics nesting closer to U.S. policy or strategy. Present the question how do other countries, cultures, and region's view, use, and adopt these technologies? Intent is also to challenge American bias that we know best and have the right answer.

2. Key Findings

Panelists brought perspectives from across Asia (China and India), Africa, and Europe, specifically Russia and Ukraine. The panel was able to draw on examples from Ukraine and Africa, offering that blockchain provides immediate benefits in a conflict zone or where political upheaval brings discontinuous change:

Self-sovereign identification methods can help secure identities for refugees, as is the case in Ukraine. The technically advanced population in Ukraine built on this opportunity by leveraging the digital asset ecosystem during the invasion. Through this effort, Ukrainians effectively crowdsourced and stored value outside of the collapsed banking system. Subsequently, adoption across Ukraine and other unstable regions accelerated. Some nations pride themselves on resisting physical U.S. dollar transactions internally, presenting possible problems for national security practitioners in tactical environments.

Blockchain / digital assets can be viewed as either revolutionary or evolutionary – noting how some populations and generations quickly adopted smartphones and mobile payments over traditional centralized banking systems (no SWIFT or credit system).

China recognizes the decentralized and trustless nature of blockchain technology as a threat to their centralized approach to governance. China reached first mover advantage by creating a PRC issued Central Bank Digital Currency (CBDC). This new digital currency was released during the latest Olympics in China with additional plans to scale globally with the help of China's One Belt One Road infrastructure and global saturation in the mobile phone markets.

The high cost of currency conversion/exchange and loss of value for fiat currency helps adoption rates of digital assets and decentralized blockchain technologies.

India has the broadest adoption of blockchain technologies, which should be reassuring given it is the largest democracy in the world.

In observing how quickly sanctions tore down Russia's economy after their invasion of Ukraine, India expressed interest in finding a way to futureproof their economy through blockchain technologies and prevent such economic loss from possible sanctions.

F. PANEL 2: NATIONAL SECURITY IMPLICATIONS OF WEB3

1. Objective

This panel's intent was to discuss the value-side argument behind web3, with the focus on decentralization, autonomy, removing intermediaries, and read-write-create ownership. The discussion attempted to provide varying perspectives capturing whether web3 has national security implications for the United States because it is reshaping the world or if it is all hype and the world, along with its societies within it, are not evolving to a decentralized network state. Additionally, the panelists could offer opinions on how the U.S. could responsibly on-ramp institutions to the ecosystem and mitigate risk of AML/CTF/Sanctions/Diminished Fiat currency influence?

2. Key Findings

Panelists discussed blockchain technologies in context of the web3 movement, which centers on decentralization, autonomy, and removing state and non-state intermediaries ranging from technology companies, like Google and Meta, to nation-states.

The strategic culture of the United States, with a focus on individual freedoms and penchant towards decentralization is a natural match for web3 – and should be embraced as a soft power advantage against other authoritarian regimes.

The United States is at risk if it fails to lead the adoption of web3 – as it opens the door for other actors (nation-state or network-state) to fill that void with their own special interests that may not align to liberal world order.

G. PANEL 3: POLICY CONSIDERATIONS AND CHALLENGES FOR BLOCKCHAIN TECHNOLOGIES

1. Objective

The objective for this panel was to discuss the evolution of blockchain technologies and their current state, with a focus on how they are perceived by the larger public. Some of the general questions posed: Where are the present opportunities and real-use applications? How do we help move from thinking Ponzi scheme to general purpose technology and enabler? Take a broader strategic outlook toward U.S. Security Cooperation leveraging Web3 technologies, how can the U.S. generate more competency in Web3? How might the U.S. take on a leadership role in global adoption and how would this influence foreign policy? What does it look like to scale in Web3 and is it possible for the U.S. to be a net exporter of Web3 expertise? The intent is to cover where web3/ blockchain technologies have evolved from and where they currently are in terms of capabilities and providing services. Ideally, audience members will leave discussion with key points and considerations about web3/blockchain technology that will help them breakdown barriers to adoption by understanding areas of potential vice unsubstantiated hype.

2. Key Findings

Panelists discussed the evolution of blockchain technologies (web3) and their current state, potential uses, and the policy challenges surrounding them.

When it comes to digital assets, most U.S. policymakers focus their attention on the digital dollar development and analysis of a U.S. approved central bank digital currency (CBDC).

Any blockchain/web3 idea should be evaluated for the business, legal, and distributed ledger technology (DLT) cases that define it. At present, at least one element of the DLT is left vague and undefined.

Most U.S. leaders and policymakers are briefed only on extreme examples or issues, which inhibits responsible development and innovation in both public/private organizations. A quote by Leslie Lamport in 1987 was highlighted to emphasize the trials of distributed consensus; "A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable."[86]

Overarching consensus on the key limitation of public blockchain technologies: Given the immutable chain is public, without zero knowledge proofs, privacy is impossible—as all transactions are public. Given the identification of an individual and their wallet address, their entire financial history (on that wallet) and who they associate with can be quickly discovered.

H. PANEL 4: CRYPTOCURRENCY FOR SPECIAL OPERATIONS

1. Objective

The objective for this panel framework was to discuss the tangible threats and opportunities of specially selected U.S. DOD units experimenting with digital assets and the broader Web3 ecosystem. The goal is to be as concrete as possible with real world tools which may provide value to security practitioners. Offer ideas for how the Web3 community can best articulate the potential without immediately losing non-technically savvy people. State the relative advantage cryptocurrency or blockchain offers compared to legacy systems.

2. Key Findings

Blockchain and digital assets (to include cryptocurrency) offer lesser-known positive use cases like censorship resistant peer to peer payments, better economic inclusion, cheaper global payment system, and a new medium for information and distribution.

Cryptocurrency has already displayed relevance on the battlefield and in moments of crisis by supporting fast payments and crowdfunding a resistance element. Blockchain and cryptocurrency is a social movement, often happening in frontier environments

[86] Leslie Lamport, "Distribution," May 1987, https://www.microsoft.com/en-us/research/publication/distribution/.

overlapping with SOF footprints. Blockchain payment rails can provide creative opportunities for SOF operators to influence and shape an environment with allies and partners.

Synthetic and metaverse environments have both a training and operational role in the military. These environments help transfer real world experiences into virtual environments at scale and enable the testing of modeling concepts. Blockchain technologies, to include digital assets, can help unify different commercial metaverses and transfer value through underlying cryptocurrency settlement protocols. Decentralized information collection, with the help of blockchain and the digital asset ecosystems, can feed into synthetic environments to update data for U.S. and partner force training and employment.

The U.S. military is still exploring where to place blockchain training and expertise within the DOD organizational structures and prefers to match incumbent tools or training with emerging blockchain and financial technology capabilities. SOF is an ideal place to start with research and development to offer recommendations for blockchain or digital asset integration into DOD manning, training, organization, and equipment requirements.

I. PANEL 6: USE OF BLOCKCHAIN THREAT FINANCING AND TARGETING

1. Objective

The objectives for this panel were to discuss threats and opportunities for end users applying blockchain technology and the general targeting methodologies it provides for the U.S. National Security enterprise. Additionally, to help the audience understand the pros and cons of blockchain technology, threat finance role in competition, and the need to educate and build proficiency for security practitioners utilizing cryptocurrency. Highlight some of the current (unclassified) successes but share insight into current gaps in capabilities that stand to benefit from additional research. Discuss the value of threat financing connected to irregular strategies and nested under the concepts for strategic competition / integrated deterrence.

2. Key Findings

There is a need for U.S. national security practitioners to understand the connection of blockchain technology and threat finance, specifically allied targeting approaches and adversary techniques utilizing blockchain.

U.S. personnel and allied end users who are employing blockchain (or digital assets) must understand the strengths and weaknesses of the technology to mitigate and account for risk. The private sector is generally more advanced in monitoring illicit activity on blockchains. Mutual interests exist in building stronger relationships between industry leaders and government agencies, for the purpose of targeting adversary activities, such as ransomware, theft, and laundering.

DOD could establish information sharing programs with the Department of Treasury and Justice to align emerging financial technology with on-going and future irregular warfare security strategies for competition and integrated deterrence.

J. PANEL 7: RESEARCH OPPORTUNITIES AT NPS AND BEYOND

1. Objective

The main objectives for this panel were to share emergent topics and requirements for DLT research; discuss sponsorship opportunities for DLT focused research such as CRADA's; highlight possible opportunities derived from the 2023 NDAA SEC 5913 and other relevant R&D sections. The discussion should help the audience identify future opportunities for research and sponsorship to include specific processes to establish contact and legally develop research agreements or learn from on-going partnerships.

2. Key Findings

The Naval Postgraduate School could serve as a unique hub of technical and conceptual resources by connecting students and faculty with commercial leaders and DOD sponsored research initiatives.

There are many siloed blockchain research programs (Stanford, MIT, DARPA) that support current U.S. national security objectives but there is no coherent campaign, designated organization, or aggregate research and development.

The Biden Administration released a call to action for digital asset development recommendations in March 2022 and a subsequent Digital Asset Framework in September 2022, proving a need to increase collaboration and research.

The 2023 NDAA includes SEC 5913 "National Research and Development Strategy for Distributed Ledger Technology." This guidance will continue to build momentum for fiscal and operational support to blockchain research broader U.S. public/ private collaboration.

K. RESEARCH PRESENTATIONS

The utility of cryptocurrency for Special Operations Forces extends broadly across the whole digital asset ecosystem and directly supports methods to modernize partnerships while simultaneously allowing SOF units to share lessons learned with U.S. decision-makers. Cryptocurrency has positive use cases in the resistance operating concept, improving the SOF-Cyber-Space Triade, offering non-standard information collection techniques, provide opportunities to mitigate risk to personnel, and reduce costs from physical cash. Overall, the perceived utility of cryptocurrency in SOF goes beyond techniques to disrupt threat finance processes, however clear regulation and policy will be required to scale beyond niche pilot programs.[87] For the complete recording of the 30-minute presentation from the research symposium on 13 September 2022, see https://nps.edu/web/nps-video-portal/-/cryptocurrency-utility-for-special-operations.

Covert communications over the Ethereum blockchain is possible and relatively simple if a modest amount of training is dedicated to the process. The transparency of the Ethereum blockchain allows for the immediate publication and distribution of financial transactions, which helps prevent manipulation by third parties. However, prior planning

[87] Michael Rowen, "Cryptocurrency Utility for Special Operations - Video Portal - Naval Postgraduate School," September 13, 2022, https://nps.edu/web/nps-video-portal/-/cryptocurrency-utility-for-special-operations.

is essential and required between the two communicating entities to ensure covert communications are effectively exchanged. Transparent blockchains are pseudonymous, which means public wallet addresses are observable while personal identity behind the transaction is not apparent. By utilizing open-source encryption tools, it's possible to send a transaction from a pre-planned wallet address to a random (unaffiliated) address which holds the encryption hash intended to be decrypted into the covert message.[88]

CSE Engineering presented their blockchain product leveraging the benefits of smart contracts (customizable programs/applications on blockchain) to automate enforcement of spending controls, dictate payment rules, check for sanctioned wallets, and simplify reporting. Smart contracts offer unavailable solutions to some of biggest challenges facing government financial management—specifically for supply chain traceability and internal controls.[89]

Constellation Network shared research for their product currently in SBIR contract USTRANSCOM to create an end-to-end data security solution using blockchain and distributed data management. "The goal is to further develop the solution as a standard for use in securely exchanging mission data with commercial partners across the Defense Transportation System (DTS)".[90]

[88] "Framework for Anonymized Covert Communications: Ethereum Blockchain-Based Concept - Video Portal - Naval Postgraduate School," accessed October 31, 2022, https://nps.edu/web/nps-video-portal/-/framework-for-anonymized-covert-communications-ethereum-blockchain-based-concept.

[89] "CSEngineering – Engineering Freedom through Digital Transformation," CSEngineering, accessed October 31, 2022, https://cse-corp.com/.

[90] "Constellation Network: Trusted in Federal Cybersecurity," Constellation Network website, accessed October 31, 2022, https://constellationnetwork.io/.

V. CONCLUSION

The cryptocurrency ecosystem does offer utility for special operations as a complimentary tool for tactical concepts and as a component to financial intelligence assessments. Beyond financial settlements, cryptocurrency offers the ability to build private and secure applications on public blockchain infrastructure to deliver valuable non-standard communication or data management tools for military operations. International use cases for cryptocurrency offer a framework for USSOF during research and development to deliver exquisite capabilities in support of resistance movements and supplement U.S. security strategies in the financial battlespace.

The DOD should not sit idly by and watch financial technology outpace USSOF capabilities or allow China and Russia to manipulate digital currency markets to proliferate invasive CBDC's and diminish U.S. influence. The DOD and more specifically, SOCOM should push operational leaders to identify ways to operationalize cryptocurrency through tailored non-standard applications to support special operations concepts. The public-private innovative cluster for cryptocurrency can help inject new thinking for gray-zone operations and SOF's role in strategic competition. The disruptive nature of "internet money" demands an open mind to account for the relative advantage in both offensive and defensive postures.

Tactical units should start to view cryptocurrency as software or nuanced pieces of equipment to handle carefully but remain willing to use for training purposes. Military leaders should work towards a standard validation pathway comparable to current pay agent and field ordering officer programs of instruction to normalize digital asset use in training and operations. SOCOM's comptroller community will be invaluable by providing connective tissue to interagency partners and sharing legal boundaries as changes or updates to regulation occurs. Ultimately, a hybrid version of digital asset employment may be the logical direction for scaling digital asset and cryptocurrency utility in military operations.

A Harvard Business Review article in 2014 titled, *Understanding "New Power,"* offers a framework of old and new power models for business. The authors state, "new power operates differently, like a current. It is made by many. It is open, participatory, and peer-driven. It uploads, and it distributes. Like water or electricity, it's most forceful when it surges. The goal with new power is not to hoard it but to channel it."[91] The elements of new power according to the authors accurately depict both extremes of cryptocurrency markets today such as intoxicating hype and influential networks disrupting entrenched old power. Cryptocurrency warrants attention from SOF units since the communities and conditions with high levels of adoption correlate to SOF areas of operation. Special operations units are well suited to channel the new power of cryptocurrency and proactively support national security objectives.

A. RECOMMENDED WAY FORWARD

One hypothetical pilot program for tactical forces would be granting approval to store stablecoins and cryptocurrency with electronic wallets on designated mobile phones. If a U.S. special operations team identifies high adoption rates in their assigned partner force and region, they should have an opportunity to request access to digital currency during the deployment. A future where tactical teams utilize smart phone applications and digital wallets to store stablecoins will offer the advantage of immediately accessing the cryptocurrency market by swapping stablecoins for cryptocurrency tokens. This concept can be replicated in the United States during training events and refined over time to incorporate recommendations from the U.S. national security enterprise.

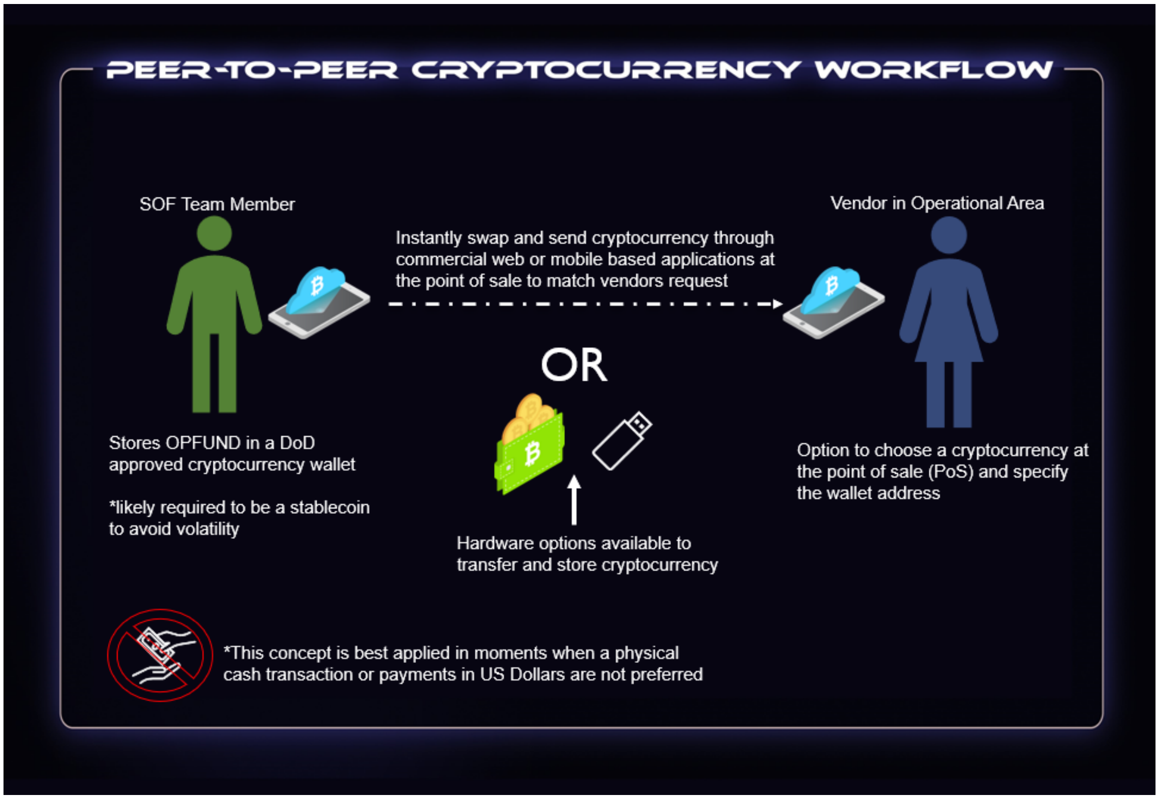
A modernized digital future would help prevent moments when the only currency option for service members is to withdraw in person and carry physical bundles of cash, often in dangerous environments and elevating risk to military members and customers. The cryptocurrency peer to peer ecosystem, known as decentralized exchanges, and certain cryptocurrency mobile application tools allows end users to immediately swap their

[91] Jeremy Heimans and Henry Timms, "Understanding 'New Power,'" *Harvard Business Review*, December 1, 2014, https://hbr.org/2014/12/understanding-new-power.

stablecoin token with another alternative cryptocurrencies within seconds.[92] If a foreign merchant prefers to receive a specific cryptocurrency, the service member or customer can rapidly swap digital currencies and send payments to the merchant's wallet address. This payment agility at the point of sale would help many special operations units deployed and at the edge of conflict, choose the best currency for every unique circumstance. Funds for each operational deployment are requested well in advance and require multiple levels of accountability. Tactical cryptocurrency pilot programs may also reveal streamlined accountability with the help of transparent blockchain ledgers and reduce overall expenses from travel and currency conversion fees.

Figure 5 presents a synopsis of the pilot program concept and was developed for this thesis with the help of NPS's media fusion office. The concept presents a basic step in cryptocurrency capability for tactical SOF members for peer-to-peer transaction options. This workflow example is intended to show an overt process for financial settlements using cryptocurrency and currently available commercial products and services.

[92] Arcane Research, "The State of Crypto - The P2P Market" (Norway: Arcane Research, October 1, 2020), https://arcane.no/research/reports/the-state-of-crypto-the-p2p-market.



PEER-TO-PEER CRYPTOCURRENCY WORKFLOW

SOF Team Member

Instantly swap and send cryptocurrency through commercial web or mobile based applications at the point of sale to match vendors request

Vendor in Operational Area

OR

Stores OPFUND in a DoD approved cryptocurrency wallet

*likely required to be a stablecoin to avoid volatility

Hardware options available to transfer and store cryptocurrency

Option to choose a cryptocurrency at the point of sale (PoS) and specify the wallet address

*This concept is best applied in moments when a physical cash transaction or payments in US Dollars are not preferred

Figure 5. Pilot Program Workflow

Figure 6, also created for this thesis with NPS's media fusion office, is intended to show a workflow with commercial business logos to further emphasize the range of products available to assist in pilot program development and experimentation. The logos represent steps that may be used along a peer-to-peer transfer process but this is not all encompassing or depicting the mandatory process for all transactions. Circle's stablecoin, USDC, and Bitcoin were the focus for this particular example, but many comparable companies exist for other cryptocurrency blockchains. The intent with this graphic is to reveal the diverse ecosystem which includes decentralized identity, stablecoin options, electronic wallets, mesh network devices, and private internet browsers. Figure 7 provides a legend for the company logos depicted in Figure 6 workflow.

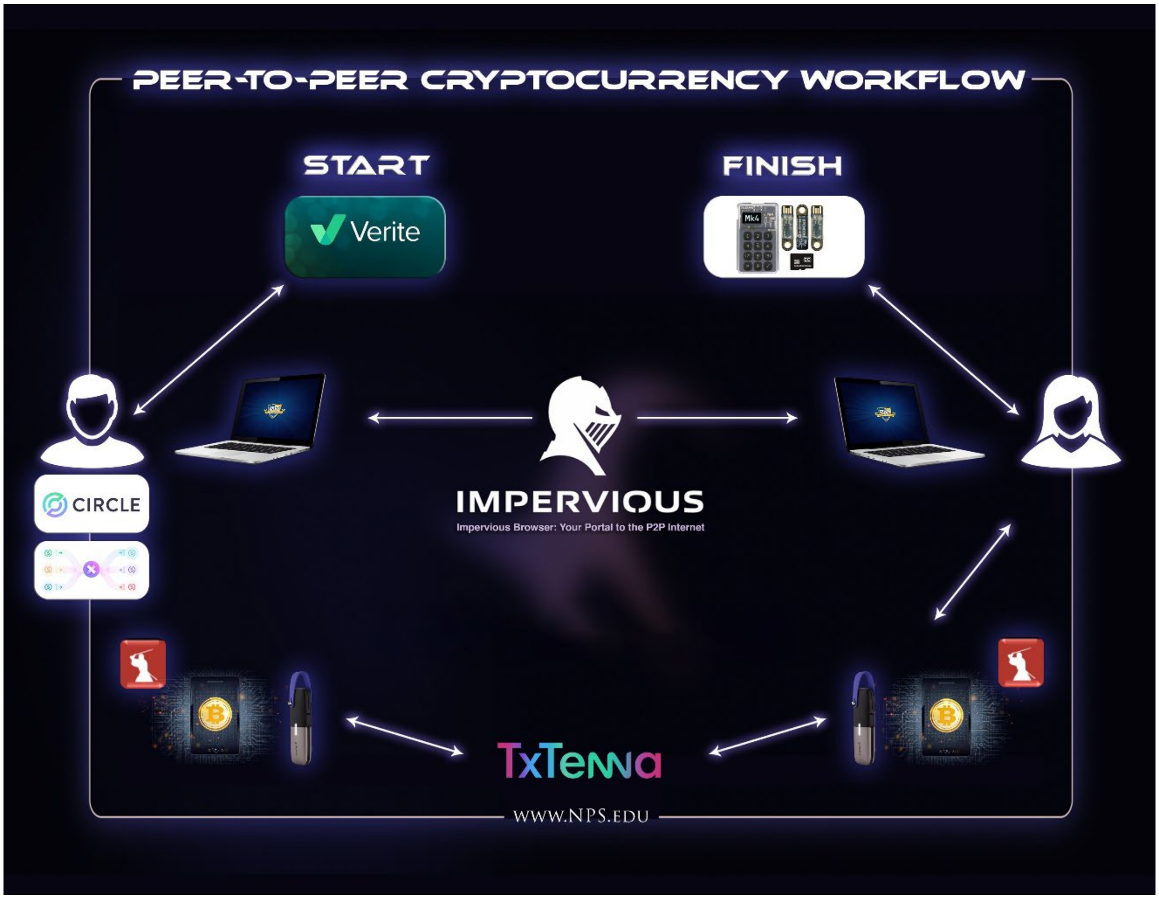
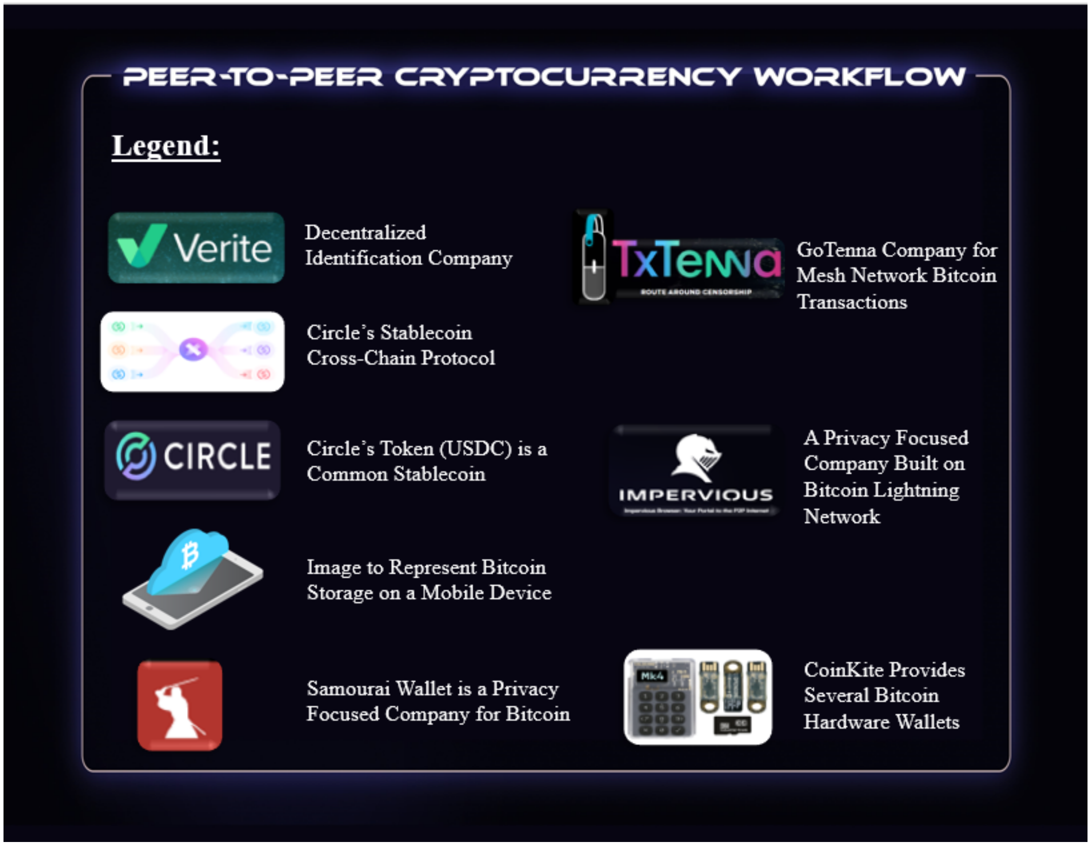

PEER-TO-PEER CRYPTOCURRENCY WORKFLOW
START
Verite
FINISH
Mk4
CIRCLE
IMPERVIOUS
Impervious Browser: Your Portal to the P2P Internet
TxTenna
WWW.NPS.EDU

Figure 6. Commercial Workflow Example



PEER-TO-PEER CRYPTOCURRENCY WORKFLOW

Legend:

Decentralized Identification Company

Circle's Stablecoin Cross-Chain Protocol

Circle's Token (USDC) is a Common Stablecoin

Image to Represent Bitcoin Storage on a Mobile Device

Samourai Wallet is a Privacy Focused Company for Bitcoin

GoTenna Company for Mesh Network Bitcoin Transactions

A Privacy Focused Company Built on Bitcoin Lightning Network

CoinKite Provides Several Bitcoin Hardware Wallets

Figure 7. Legend for Commercial Company Workflow

The workflow examples attempt to provide a starting point for additional research and development for end-users or tactical teams. The example presented is not frictionless and does require additional steps to complete depending on the point of origin for funds. The general framework helps to set the baseline for including a proof-of-concept training exercise for USSOF. Additionally, cybersecurity testing and assessments should be implemented prior to operational use of these services. However, SOF should begin education and local training with this type of basic pilot program or workflow.

Overall, a cryptocurrency pilot program is an attractive way of developing a niche tool to supplement legacy processes and one that encourages creative problem-solving, accountability, and novel risk mitigation when applied correctly. As proficiency increases for building smart contracts and DApps with cryptocurrency, SOF formations will likely find additional use cases or offer better training and solutions to partner forces.

As U.S. special operations forces continue to build organic cyber talent, the barrier for entry into the cryptocurrency ecosystem will become more manageable. The initial steps for experimentation should be developed now to account for administrative hurdles prior to testing various overt concepts and develop a baseline proficiency to mitigate risk beyond benign operational use cases.

A survey or poll among the USSOF formation is a reasonable option to start developing awareness of cryptocurrency literacy or curiosity. Additionally, a proactive discussion between operational units and partner forces globally can help gauge interest and adjust future research accordingly. Civilian and military research facilities may serve as a valuable hub to connect commercial projects with battlefield challenges or the military incubators attempting to harness digital asset concepts. The DOD innovation network can help matchmaking between tactical end-users who bring real-world use cases and commercial companies with expertise to tailor software applications or deliver unique hardware. The disruptive nature of financial technologies is forcing SOF to consider financial lines of communication as legitimate options for nonkinetic effects from friendly and enemy forces.[93]

B. RECOMMENDED AREAS FOR ADDITIONAL RESEARCH

The 2023 NDAA SEC 5913 highlights research for distributed ledger technology and this could assist with cryptocurrency education and broader understanding of the threats and opportunities. The consensus around blockchain or DLT research allows for exploration of cryptocurrency testing and localized training to deliberately build understanding and capability in SOF. Research institutions connected to the innovation network can enable project teams of researchers for quantitative analysis and cybersecurity assessments of the open-source software which also helps reduce the burden on operational DOD cyber organizations.

[93] Smith, “Applying Financial Capabilities to Achieve Multi-Domain Effects: Using Financial Capabilities Operationally Rather Than Transactionally.” 55.

The transparency of public cryptocurrency blockchains allows access to new types of data sets for operational research faculty and students. Academic institutions could develop more cooperative research agreements with commercial blockchain analytics companies to maintain a steady stream of information to merge network analysis and social sciences depending on the accuracy of region-specific data. This type of research would benefit the DOD and many other stakeholders working to responsibly develop digital asset regulation in the United States.

Climate security research with cryptocurrency, and specifically "proof of work" processes such as Bitcoin, may identify beneficial steps to improve prototyping, testing, and operating green energy devices in austere environments. The thought to include Bitcoin mining hardware next to green energy generation like wind, solar, and thermal has been discussed but little has been lobbied for government sanction testing in austere locations or when energy transfer infrastructure is expensive or non-existent. Bitcoin mining devices connected to sustainable energy prototypes may seem inappropriate but the potential to offset the fiscal burden for research and development through Bitcoin rewards may help in incentivize future experimentation. Since SOF units are typically deployed to austere locations and could benefit from sustainable energy equipment, additional research to assist interagency, academic partners, or allies in testing prototypes may be mutually beneficial.

Perhaps the most intriguing area for continued research between cryptocurrency and special operations is from non-standard communications concepts. Specifically, mesh networks incentivized through cryptocurrency may offer unique ways to approach security strategies. Companies like Helium and Pollen Mobile revealed grassroots models to help scale a mobile 5G network with a local population by offering rewards for "proof of coverage."[94] The benefits of inherent encryption standards on blockchain and smaller form factor routers or antennas may lead to reliable peer to peer communication protocols and mesh networks to cover regions with limited service. Additionally, the opportunity to circumvent Chinese owned 5G infrastructure with the help of local communities

[94] Decrypt / Andrew Hayward, "Samsung, Qualcomm Back FreedomFi, Helium's 5G Crypto Network Partner," Decrypt, March 15, 2022, https://decrypt.co/95153/samsung-qualcomm-back-freedomfi-heliums-5g-crypto-network-partner.

maintaining decentralized networks may prove invaluable in the future. However, more research is required to help determine feasibility, security concerns in both hardware and software, and country specific obstacles for spectrum ownership among many other variables.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. PANEL CONCEPT SHEET 1

Panel 1 (12 September 2022)

Title: Blockchain & National Security Around the BRICS

Objective: This panel should focus on a geo-political level and offer a stratospheric view for the audience. Help to articulate how emerging technology is influencing the changing dynamics for the BRICS nations and set the tone for following topics nesting closer to U.S. policy or strategy. How do other countries, cultures, and region's view, use, and adopt these technologies? The intent is also to challenge traditional American bias that we know what is best and have the right answer.

Panel Members:
Moderator: Dr. Leo Blanken: NPS Faculty Lead/ Co-Founder for Applied Design for Innovation Curriculum

Panelist 1 – Mark Gabriele: USG Senior Advisor, Lead Author of 2018 DHS Report on Blockchain Technologies, (Russia)

Panelist 2 – Jonathan Bench: International Business Attorney, Harris-Bricken, (China)

Panelist 3 – Founder bc13o Technology Group, (Ukraine)

Panelist 4 – Selina Hayes: Founder / CEO of Hayes Group, (Africa)

Panelist 5 – John Medel: International Policy Team, Coinbase, (India)

Framing Questions:

Mark – In developing the 2018 DHS report on blockchain technologies, what was your take-away on how blockchain has been adopted around the world? Specifically, can you share any examples of what Russia was or has been doing?

Jonathan – China is a highly centralized nation, how does the decentralized nature of blockchain fit into China's vision of the future? Is there a disconnect between the people and the government of China? What are the challenges and opportunities Facing China with the emergence of web3?

bc13o Technology Group – Being on the ground in Ukraine for a few months now, can you tell us about the role you have seen crypto and blockchain take on? Is there a use for blockchain on the battlefield? In the conflict space? What does that look like?

Selina – Adoption of cryptocurrency in Africa is rather high compared to the rest of the world. Why is that? Where do you think the U.S. fits into Africa's FinTech growth comparatively to China, Russia, India? With the ongoing winter for crypto, hasn't that placed those who trusted their use at a greater disadvantage and loss than if they stuck to their country's fiat?

John Medel – India has the highest adoption rate of web3 and crypto. Why is that? What is it that drives adoption in India and is it unique to their culture or something we'll see across the globe as adoption scales? Looking out a decade, what are the potential outcomes of India being a leader adopter of web3?

General Questions for Conversation:

1. On a scale of importance, where would you rate blockchain technologies? What would you equate blockchain technology too – especially in the context of your countries? Is this really a revolution or is it hype? To the point of this event – does your respective countries governments view any elements as a national security threat or maybe a soft or hard power opportunity?

2. How have blockchain technologies shaped the elements of national power in your country? Has there been impacts in your country's ability to flex power diplomatically, via information, militarily, or economically? Or is blockchain and the associated web3 movement purely a private sector impact?

3. The United States is at a critical point in the history of blockchain regulations. From your perspectives, what are the larger impacts if the United States seeks to clamp down on innovation in this sector? What are the impacts for the U.S.? What are the impacts in your respective countries? Would there be any?
    a. Follow-on Question – What should the United States learn from your respective countries experience in dealing with blockchain technologies and crypto?

4. How has the use of blockchain technologies, like cryptocurrencies changed over the years in your respective countries? How has government control or regulation shaped it?

5. Let’s talk about other elements of blockchain technologies – Decentralized Autonomous Organizations – or DAOs. DAOs are easily global in nature. Has there been adoption of DAOs or explicit prohibition of participating in them in your respective countries? How might the strategic culture of your country shape or influence the DAO movement? Or will the DAO movement potential shape some countries?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PANEL CONCEPT SHEET 2

Panel 2 (12 September 2022)

Title: National Security Imperative or Peril of web3

Objective: Discuss the value-side argument behind web3 – the focus on decentralization, autonomy, removing intermediaries, and read-write-create ownership. Provide varying perspectives capturing whether web3 has national security implications for the United States. Is web3 reshaping the world or is it all hype?

Panel Members:
Moderator – CPT Jay Long: Innovation Officer

Panelist 1 – August Cole: Renowned author exploring the future of conflict through Fictional Intelligence storytelling, non-resident senior fellow at Atlantic Council among several others

Panelist 2 – Antonio Garcia Martinez (AGM): Author, internet native, early ad-tech developer, and "research scientist"

Panelist 3 – Spencer MacDonald: Building and enabling talent, supported by mutual understanding, to drive effective technological innovation within DOD

Framing Questions:

August – Can you walk the audience from web 1.0 to web3 and what possible implications you see on the horizon? What do you see life, and more specifically, our national security challenges and opportunities looking like in the future?
Antonio – The Network State is an emerging idea born out of web3, can you help the audience understand what a Network State is and how it could be part of our future? What are the key elements that are unique from web3 that make it possible?
Spencer – The U.S. Government, especially DOD, has had their challenges in working with the tech industry. Are we doomed to repeat our mistakes? What does success look like for the United States national security apparatus to leverage the opportunities afforded by web3?

General Questions for Conversation:

1. Is web3 a natural match for America and the liberal world order born out of World War 2? How might web3 be a destabilizing impact on our current systems? How might they be co-opted against us by China or Russia?
2. I can't mention blockchain in my professional circles without having to be apologetic…how do we move beyond the hype and speculation? How do we get towards achieving greater adoption? And maybe more important…greater adoption of what?
3. To the title of this panel, is web3 an enabler, a threat, or a distraction for national security? How so?
4. Focusing on decentralization and trustlessness, how might we see that play out in future warfare? Is the U.S. going to sponsor bounties to go after our adversaries?

APPENDIX C. PANEL CONCEPT SHEET 3

Panel 3 (12 September 2022)

Title: Policy Challenges: Opportunities for Strategic Competition

Objective: Discuss the evolution of blockchain technologies (web3) and their current state – with a focus on how they are perceived by the larger public. Where are the present opportunities and real-use applications? How do we help move from thinking ponzi scheme to general purpose technology and enabler? Take a broader strategic outlook toward U.S. Security Cooperation leveraging Web3 technologies, how can the U.S. generate more competency in Web3? How might the U.S. take on a leadership role in global adoption and how would this influence foreign policy? What does it look like to scale in Web3 and is it possible for the U.S. to be a net exporter of Web3 expertise? The intent is to cover where web3/blockchain technologies have evolved from and where they currently are in terms of capabilities and providing services. Ideally, audience members will leave discussion with key points and considerations about web3/blockchain technology that will help them breakdown barriers to adoption by understanding areas of potential vice unsubstantiated hype.

Panel Members:
Moderator – Tom Dixon: Senior Account Executive, Lukka. Former DIA Chief of Operations

Panelist 1 – Michael Mosier: General Counsel, Espresso Systems. DoJ; White House NSC; Treasury; adj_prof. Georgetown Law

Panelist 2 – Alex McLeod: Parlay Protocol, Blockchain uses for businesses

Panelist 3 – Evan Sultanik: Computer Security Researcher, Trail of Bits

Panelist 4 – Chris Jaikaran: Policy perspectives, Congressional Research Service

Panelist 5 – Jesse Spiro: Header of PayPal cryptocurrency wing to work on regulatory policy

Framing Questions:

Framing of Blockchain Technologies – Hype vs Reality:

Chris – Let’s talk about the inherent limitations of blockchain technologies and the web3 movement…there are some serious hurdles to the hype. Can you break that down for us?

Evan – You wrote a piece covering whether or not your problem needs a blockchain solution. Can you break down the space in which blockchain is best designed to function within?

Alex – Given your experience, what innovative successes have you seen from using blockchain technologies? Given what Chris and Evan laid out, where do you see the opportunities?

Policy Challenges for Blockchain – What are the policy discussions around this technology? Why do they matter?

Michael – You’ve been on the frontlines of the executive branch in looking at the darker problems and illicit activities people point to as to why blockchain is bad. Can you give us an inside look of how blockchain technologies like crypto are being viewed inside the executive branch? What are the concerns and problems shaping those discussions?

Chris – With your work and research, what have you consistently seen to be the most pressing policy issues generated by blockchain associated technologies?

Jesse – From the private sector perspective, what are the essential policy problems you see that need to be solved? Is regulation a good thing or a bad thing? How big of an impact can these discussion cause?

General Questions for Conversation:

1. Is web3 and its associated blockchain technologies an important sector for the United State to take lead in? Is it a public problem or a private sector issue?

2. Blockchain is a bit of a dirty word within the government and largely to anyone who isn’t an early adopter. Can blockchain move from being considered a ponzi scheme to general purpose technology and enabler? How do we do this?

3. Taking a broader strategic outlook toward U.S. Security Cooperation and leveraging Web3 technologies, how might the U.S. generate more competency in Web3, to take a leadership role in global adoption and how does this influence foreign policy?

4. What does it look like to scale in Web3 and is it possible for the U.S. to be a net exporter of Web3 expertise?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. PANEL CONCEPT SHEET 4

Panel 4 (12 September 2022)

Title: Cryptocurrency Ecosystem: The Operator's New Infrastructure?

Objective: Discuss the tangible threats and opportunities of specially selected U.S. DOD units experimenting with digital assets and the broader Web3 ecosystem. The goal is to be as concrete as possible with real world tools which may provide value to security practitioners. Offer ideas for how the Web3 community can best articulate the potential without immediately losing non-technically savvy people. State the relative advantage cryptocurrency or blockchain offers compared to legacy systems.

*Discuss questions posed by operational members of the military such as***:** how does the global adoption rates of the cryptocurrency ecosystem potentially impact the broad U.S. military footprint? What is the future direction of NFTs and where are areas of potential research to push NFTs to the next level? Will novel decentralized identification methods overtake some of the utility functions from NFTs? What is the process to merge physical assets or processes to help build logical NFT functionality and will it diffuse into the national security or defense sector? How can synthetic environments improve U.S. military training and operations? How will the metaverse or other synthetic environments integrate with digital assets and is there a role for the military?

Panel Members:
<u>Moderator</u> – <u>MAJ Scott Rowen</u>: NPS Student, U.S. Army, 3rd Special Forces Group

<u>Panelist 1</u> – <u>George LeMeur</u>: Head of business operations at Impervious.ai, fmr 1st Special Forces Group

<u>Panelist 2</u> – <u>Cameron Armstrong</u>: Founder VF Protocol, eCommerce Start-up and financial modeling, former U.S. Army Infantry Officer

<u>Panelist 3</u> – <u>Michael Pavek</u>: Senior technical product manager at Improbable.io, former U.S. Army Officer

<u>Panelist 4</u> – <u>LTC Chris Robinette</u>: Battalion Commander 5th BN SWCS, PWC Finance and Acquisition, former 10th Special Forces Group

Framing Questions:

George – Impervious uses the term Peer-to-Peer to discuss the tools and infrastructure it builds. Why do you make this distinction and how is p2p relevant to operators?

Cameron – Where do you see the future direction of NFTs and what is the relevance for national security? Will novel decentralized identification methods overtake some of the utility functions from NFTs?

Michael – How can synthetic environments improve U.S. military training and operations? How will the metaverse or other synthetic environments integrate with digital assets and is there a role for the military? Can you touch on the question if blockchain is truly helpful and/or a practical tool for metaverse development and scaling?

Chris – How do you see leaders shifting their mindset towards emerging technologies and including methods to integrate these concepts into doctrine, manning, training, and equipping? Does the idea for creating a new and more technical military occupational specialty into SOF units have weight and is it needed?

General Questions for Conversation:

1. What are your opinions regarding the learning curve or the barrier of entry at some traditional tactical units for incorporating Web3 technologies?

2. How do you approach the opinion many of these Web3 technologies are not important to military operations or digital assets are outside of the scope of DOD operations?

3. Can emerging decentralized identification technology help mitigate the risks for service members if granted approval to use more blockchain, digital assets, metaverses in military operations? How does the transparency of public blockchains create a double-edged sword for military units?

4. Any recommendations for the U.S. Defense enterprise to responsibly integrating advanced Web3 commercial company products with cumbersome but motivated DOD/SOF units, for example the potential branding or marketing issues when associated with governments?

APPENDIX E. PANEL CONCEPT SHEET 6

Panel 6 (13 September 2022)

Title: Targeting and Counter Threat Finance

Objective: Discuss threats and opportunities for end users applying blockchain technology and the general targeting methodologies it provides for the U.S. National Security enterprise. Help the audience understand the pros and cons of blockchain technology, threat finance role in competition, and the need to educate and build proficiency for security practitioners utilizing cryptocurrency. Highlight some of the current (unclassified) successes but share insight into current gaps in capabilities that stand to benefit from additional research. Discuss the value of threat financing connected to irregular strategies and nested under the concepts for strategic competition / integrated deterrence.

Panel Members:

Moderator – MAJ Aaron Heaviland: NPS Student, Foreign Area Officer, previously in 75th Ranger Regiment

Panelist 1 – COL Brian Smith: USASOC Counter Threat Finance, SOF centric Targeting and Finance approach in Irregular Warfare

Panelist 2 – Alex Zerden: Lawyer, fmr White House Advisor, U.S. Treasury CTF in Kabul

Panelist 3 – Mike Aleman: Senior Director at PayPal's global financial crime and blockchain innovation development

Framing Questions:

> **Alex and Brian** – Can you help the audience understand the pros and cons of blockchain technology and the connection it has with threat finance? How does it play a role in competition with other nations or organizations, and touch on the need to educate and build proficiency for security practitioners utilizing cryptocurrency.
>
> **Brian** – Can you discuss threats and opportunities for end users applying blockchain technology and the general targeting methodologies it provides for the U.S. National Security enterprise.

Alex – Can you discuss civilian lines of effort focusing on the Department of Treasury and Justice that covers strategies for combating terrorism financing, laundering and illicit finance and then operational methods such as sanctions designations and criminal prosecutions?

Michael – Can you help some of the DOD population contextualize how PayPal or generally how private industry frame illicit finance and counter terrorism financing?

General Questions for Conversation:

1. Can you share insight to the role of the darknet to include negative impacts from the proliferation of ransomware and cyber intrusions/hacking? How does the transparency of blockchain factor into the analysis for CTF and anti-money laundering compliance?

2. What is the black swan event that keeps you up at night or generates the most cause for concern?

3. In relation to CTF, does the U.S. need to clarify the legal framework for digital assets and blockchain technology or are the current legal boundaries adequate and effective? If changes are needed, will minor adjustments to definitions and policy help fill the legal gap or is a drastic shift in guidance and regulation required?

4. Is there a need for U.S. SOCOM to better leverage public-private engagements to understand new business models, identify and address development obstacles, threat identification, attribution, or techniques?

APPENDIX F. PANEL CONCEPT SHEET 7

Panel 7 (13 September 2022)

Title: Distributed Ledger Technology (DLT) & Research Opportunities

Objective: (1) Discuss emergent topics/requirements for DLT research; (2) Discuss sponsorship opportunities for DLT focused research (i.e. CRADA); (3) Highlight possible opportunities derived from the draft 2023 NDAA SEC 5804 and other relevant R&D sections. The discussion should help the audience identify future opportunities for research and sponsorship to include specific processes to establish contact and legally develop research agreements or learn from on-going partnerships.

Panel Members:
Moderator – Sheila Vaidya: Emerging Technology Portfolio Lead, NWSI, NPS

Panelist 1 – Dr. Evan Sultanik: Computer Security Researcher at Trail of Bits
(Topic: DARPA sponsored research)

Panelist 2 – Jonathan Dotan: Director of Starling Lab, Stanford University
(Topic: Opportunities for innovative use of blockchain solutions at the tactical level)

Panelist 3 – Gene Keselman: Executive Director of MIT Innovation Initiative
(Topic: Opportunities for applied research and innovation from MIT perspective)

Panelist 4 – Will Schweitzer: Protocol Labs
(Topic: Emerging areas for DLTs that coincide with national security applications)

Panelist 5 – John Kothanek: Vice President Global Intelligence Cryptocurrency, Coinbase, Blockchain Analytics (Topic: Blockchain analytics as an emergent research method)

Framing Questions:

Evan – What has been your experience in developing research for DARPA sponsored research? Do you see both demand and room for growth for more in depth research?

Gene and **Jonathan** – How have you seen academic research into blockchain technologies evolve over the year or years? What has worked? What failed?

John – How do you see blockchain changing research methods today or in the near future? What kind of opportunities does that open?

Will – Drawing on your tactical special operations experience, and current perch with Protocol Labs – how would you want to focus emerging research to generate opportunities at the tactical level?

General Questions for Conversation:

1. Let's talk relevance, timeline, and research opportunities. Why are blockchain technologies relevant to the Navy or the U.S. military more broadly? How would you assess the technological readiness of these technologies? Are we talking adoption within the next 10 years, or is it further out? What are the research opportunities you see for NPS students and faculty?

2. For someone who doesn't know blockchain, explain to me where the research opportunities are in this space? What type of academic research would be useful, especially from an applied research perspective?

3. On the TRL scale, what are the emergent topics researchers should focus on from your perspective?

SUPPLEMENTAL. DIGITAL ASSET AND CRYPTOCURRENCY RESOURCE GUIDE

A link is available to this Supplemental file with the main thesis's catalog entry in the NPS Institutional Archive, Calhoun, or by contacting the NPS library.

These resources are intended to provide a starting point to discover more knowledge in the digital asset ecosystem and increase understanding in cryptocurrency terminology.

Many of the resources are cited in the thesis however, this product may help reduce the burden when searching for reading material or clarity.

The reports or websites recommended below are only a snapshot of the ecosystem and cover several years of innovation for the digital asset markets or analysis in national security affairs.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abdalla, Alyce. “U.S. Strategy and the Future of Money: Advancing U.S. Interests During a Financial Transformation.” The Strategy Bridge, August 2022. https://thestrategybridge.org/the-bridge/2022/8/29/us-strategy-and-the-future-of-money.

Antonopoulos, Andreas M., and Gavin Wood. *Mastering Ethereum: Building Smart Contracts and DApps*. First edition. Sebastopol, CA: O’Reilly, 2019.

Arcane Research. “The State of Crypto - The P2P Market.” Norway: Arcane Research, October 1, 2020. https://arcane.no/research/reports/the-state-of-crypto-the-p2p-market.

Arquilla, John. “Of Networks and Nations.” *The Brown Journal of World Affairs*, no. 14.1 (2007): 199–208. http://bjwa.brown.edu/14-1/of-networks-and-nations/.

Bech, Morten L., and Rodney Garratt. “Central Bank Cryptocurrencies.” SSRN Scholarly Paper. Rochester, NY, September 17, 2017. https://papers.ssrn.com/abstract=3041906.

Berg, Leandro. “RTF Report: Combatting Ransomware.” Institute for Security and Technology (IST). Accessed August 13, 2021. https://securityandtechnology.org/ransomwaretaskforce/report/.

Blanken, Leo. “Special Operations Forces as a Rapid Prototyping Laboratory.” Edited by Philip Swintek. *Center for Global Security Research*, January 2021. http://hdl.handle.net/10945/67924.

Boston, Federal Reserve Bank of. “Project Hamilton Phase 1 Executive Summary.” Federal Reserve Bank of Boston, February 3, 2022. https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx.

Brady, Rich, and Bill Arnold. “Data Analytics: From Raw Data to Informed Decisions.” *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022). https://asmconline.org/armed-forces-comptroller/.

Breede, Christian, Kevin Stringer, and Sara Dudley. “A Counter-Threat Finance Approach to Competition.” The Politics of Special Forces, n.d. https://podcasts.apple.com/us/podcast/episode-2-a-counter-threat-finance-approach-to-competition/id1553806860?i=1000557143750.

Busch, Kristen. “Blockchain: Novel Provenance Applications.” Washington, D.C: Congressional Research Service, April 12, 2022. https://crsreports.congress.gov/product/pdf/R/R47064.

Chainalysis Team, Chainalysis. “2022 Global Cryptocurrency Adoption Index.” Chainalysis, September 14, 2022. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/.

Cohen, Eliot A. *Commandos and Politicians: Elite Military Units in Modern Democracies*. Harvard Studies in International Affairs, no. 40. Cambridge, Mass.: Center for International Affairs, Harvard University, 1978.

Coinbase. “Crypto Basics - What Is Mining?” Coinbase Learn, 2022. https://www.coinbase.com/learn/crypto-basics/what-is-mining.

Coinbase Institute. “Coinbase Institute.” Accessed October 31, 2022. https://www.coinbase.com/institute.

Constellation Network website. “Constellation Network: Trusted in Federal Cybersecurity.” Accessed October 31, 2022. https://constellationnetwork.io/.

Gemini. “Cryptocurrencies vs. Tokens: Digital Assets.” Accessed October 26, 2022. https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference.

CSEngineering. “CSEngineering – Engineering Freedom through Digital Transformation.” Accessed October 31, 2022. https://cse-corp.com/.

Davis, Zachary S, Frank Gac, Christopher Rager, and Jennifer Snow. *Strategic Latency Unleashed: The Role of Technology in a Revisionist Global Order and the Implications for Special Operations Forces*. Livermore, CA: Center for Global Security Research, 2021.

Denning, Peter J., and Ted G. Lewis. “Bitcoins Maybe; Blockchains Likely.” *Sigma XI-The Scientific Research Society*, December 2017.

Department of Commerce. “Responsible Advancement of U.S. Competitiveness in Digital Assets.” Digital Asset Competitiveness Report. Washington, D.C: U.S. Department of Commerce, September 2022. https://www.commerce.gov/files/digital-asset-competitiveness-report.

Department of Defense. *DOD Counter Threat Finance (CTF) Policy*. DOD Directive 5205.14. Washington, D.C: Department of Defense, 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520514p.

Dillet, Romain. “How Ukraine Is Spending Crypto Donations.” *TechCrunch* (blog), March 2, 2022. https://techcrunch.com/2022/03/02/how-ukraine-is-spending-crypto-donations/.

Dostov, Victor, and Pavel Shust. "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?" *Journal of Financial Crime* 21, no. 3 (January 1, 2014): 249–63. https://doi.org/10.1108/JFC-06-2013-0043.

Dudley, Sara, Travis Pond, Ryan Roseberry, and Shawn Carden. "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency." *Joint Force Quarterly*, no. 92 (2019): 58–64.

Duffie, Darrell. "Can China Conquer Crypto?" *Foreign Affairs*, September 2, 2022. https://www.foreignaffairs.com/articles/china/2022-04-22/can-china-conquer-crypto.

Duffie, Darrell, and Elizabeth Economy. "Digital Currencies: The U.S., China, And The World At A Crossroads." Working Group. Hoover Institute, 2022. https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads.

Duggan, Patrick M., and Elizabeth Oren. "U.S. Special Operations Forces in Cyberspace." *The Cyber Defense Review* 1, no. 2 (2016): 73–80. http://www.jstor.org.libproxy.nps.edu:2048/stable/26267360.

Exec. Order No. 14067. Executive Order on Ensuring Responsible Development of Digital Assets (2022). https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

Fiala, Otto C. *Resistance Operating Concept (ROC)*. MacDill Air Force Base, Florida: The Joint Special Operations University Press, 2020.

"Framework for Anonymized Covert Communications: Ethereum Blockchain-Based Concept - Video Portal - Naval Postgraduate School." Accessed October 31, 2022. https://nps.edu/web/nps-video-portal/-/framework-for-anonymized-covert-communications-ethereum-blockchain-based-concept.

Frebowitz, Ryan L. "Cryptocurrency and State Sovereignty." Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/59663.

Gemini. "Crypto Glossary - Cryptopedia." Gemini Cryptopedia, 2022. https://www.gemini.com/learn/glossary.

Harsono, Hugh. "Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain." *The Cyber Defense Review* 5, no. 3 (2020): 153–60. https://www-jstor-org.libproxy.nps.edu/stable/26954878.

Hayward, Decrypt / Andrew. "Samsung, Qualcomm Back FreedomFi, Helium's 5G Crypto Network Partner." Decrypt, March 15, 2022. https://decrypt.co/95153/samsung-qualcomm-back-freedomfi-heliums-5g-crypto-network-partner.

Heimans, Jeremy, and Henry Timms. "Understanding 'New Power.'" *Harvard Business Review*, December 1, 2014. https://hbr.org/2014/12/understanding-new-power.

House, The White. "FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets." The White House, September 16, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.

Impervious. "Impervious Project." Your Portal to the P2P Internet. Accessed October 31, 2022. https://www.impervious.ai/.

International Trade Administration. "El Salvador Adopts Bitcoin as Legal Tender." U.S. Department of Commerce. International Trade Adminstration, June 2021. https://www.trade.gov/market-intelligence/el-salvador-adopts-bitcoin-legal-tender.

Jensen, Benjamin M. *Forging the Sword: Doctrinal Change in the U.S. Army*. Stanford, California: Stanford Security Studies, an imprint of Stanford University Press, 2016.

Johnson, Jason D. "Bitcoin: A Technology-Influenced Social Movement." Master's thesis, Naval Postgraduate School, 2019. https://calhoun.nps.edu/handle/10945/63988.

Joint Knowledge Online. "New USSOCOM J35 Counter Threat Finance (CTF) Curriculum." Joint Chiefs of Staff, August 4, 2022. https://www.jcs.mil/JKO/Latest-News/JKO-Customer-Spotlights/Article/3115355/new-ussocom-j35-counter-threat-finance-ctf-curriculum/.

Jones, Laura, and Shawna Sinnott. "Money Talks: How Nonstate Armed Groups Finance Their Operations and Organizations." Modern War Institute, July 15, 2022. https://mwi.usma.edu/money-talks-how-nonstate-armed-groups-finance-their-operations-and-organizations/.

Kanth, Vikram K. "Blockchain for Use in Collaborative Intrusion Detection Systems." Master's thesis, Naval Postgraduate School, 2019.

Kimani, M. "China Leads Africa's Digital Currency Race." Yahoo. Michael, February 2021. https://finance.yahoo.com/news/china-leads-africa-digital-currency-202250648.html.

Kumar, Ananya, and Nikhil Raghuveera. "Can Crypto Deliver Aid amid War? Ukraine Holds the Answer." *Atlantic Council* (blog), April 4, 2022. https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-answer/.

Lamport, Leslie. “Distribution,” May 1987. https://www.microsoft.com/en-us/research/publication/distribution/.

Chainalysis Academy. “Learn Cryptocurrency.” Accessed October 31, 2022. https://academy.chainalysis.com/page/learn-cryptocurrency.

Liebermann, Oren. “How Ukraine Is Using Resistance Warfare Developed by the U.S. to Fight Back against Russia | CNN Politics.” CNN, August 27, 2022. https://www.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html.

Limba, Tadas, Andrius Stankevičius, and Antanas Andrulevičius. “Towards Sustainable Cryptocurrency: Risk Mitigations from a Perspective of National Security.” *Journal of Security and Sustainability Issues*, December 19, 2019. https://repository.mruni.eu/handle/007/16063.

Long, Gideon. “Digital Scheme Pays Venezuela Health Workers from Frozen Funds.” Financial Times, December 10, 2021. https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18.

McBride, Megan, and Zack Gold. “Cryptocurrency: A Primer for Policy-Makers.” Arlington, VA: Center for Naval Analyses: Analysis and Solutions. Accessed October 26, 2022. https://www.cna.org/reports/2019/08/cryptocurrency-primer-for-policymakers.

———. “Cryptocurrency: Implications for Special Operations Forces.” Arlington, VA: Center for Naval Analyses: Analysis and Solutions, August 2019. https://www.cna.org/reports/2019/08/cryptocurrency-implications.

Merwe, Andria van der. “A Taxonomy of Cryptocurrencies and Other Digital Assets.” *Review Business: St. Johns University*, no. 41 (2021): 30–43. https://www.stjohns.edu/sites/default/files/uploads/Review-of-Business-41%281%29-Jan-2021.pdf.

Montgomery, Mark. “Equipping U.S. Partners in Cyberspace Is a Must.” The Cipher Brief, July 2022. https://www.thecipherbrief.com/column_article/equipping-u-s-partners-in-cyberspace-is-a-must.

Morell, Michael, Josh Kirshner, and Thomas Schoenberger. “Report: An Analysis of Bitcoin’s Use in Illicit Finance.” The Cipher Brief, April 13, 2021. https://www.thecipherbrief.com/report-an-analysis-of-bitcoins-use-in-illicit-finance.

Myers, Adam, William Szymanski, Daniel Jackson, Ellen Wynkoop, Pete Heine, Tyler Hoffman, and Bri Mostoller. “Crypto-Controls: Harnessing Cryptocurrency to Strengthen Sanctions.” War on the Rocks, December 9, 2020. https://warontherocks.com/2020/12/crypto-controls-harnessing-cryptocurrency-to-strengthen-sanctions/.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin.Org*, October 2008. https://bitcoin.org/en/bitcoin-paper.

Nelson, Danny, and Anna Baydakova. “Ukraine Leads Global Crypto Adoption, Chainalysis Says in New Report,” September 8, 2020. https://www.coindesk.com/markets/2020/09/08/ukraine-leads-global-crypto-adoption-chainalysis-says-in-new-report/.

Nelson, Jason. “Taiwan Turns to Ethereum IPFS Tech to Thwart Chinese Cyberattacks.” Decrypt, August 11, 2022. https://decrypt.co/107293/taiwan-turns-to-ipfs-tech-to-thwart-cyberattacks-from-china.

Newman, Lily Hay. “Mysterious ‘MuslimCrypt’ App Helps Jihadists Send Covert Messages.” *Wired*. Accessed October 27, 2022. https://www.wired.com/story/muslimcrypt-steganography/.

Newmyer, Tory. “Pentagon Launches Effort to Assess Crypto’s Threat to National Security.” *Washington Post*, September 23, 2022. https://www.washingtonpost.com/business/2022/09/23/darpa-crypto-national-security/.

Pero, Michael C. “Understanding Bitcoin and It’s Utility for Special Operations Forces.” Naval Postgraduate School, 2022. https://calhoun.nps.edu/handle/10945/69701.

Protocol Labs. “About Protocol Labs.” Protocol Labs. Accessed November 20, 2022. https://protocol.ai/about/.

Renaudin, Hugo. “Remittance and Payments: Crypto’s Big Opportunity in Latin America.” Accessed October 27, 2022. https://www.nasdaq.com/articles/remittance-and-payments%3A-cryptos-big-opportunity-in-latin-america-2020-08-06.

Reuters. “Russia Plans to Use Digital Rouble in Settlements with China, Says Lawmaker.” *Reuters*, September 26, 2022, sec. Currencies. https://www.reuters.com/markets/currencies/russia-plans-use-digital-rouble-settlements-with-china-says-lawmaker-2022-09-26/.

Rivers, Martin Leo. “Got Bitcoin, Will Buy Intel: U.S. Government Offers Cryptocurrency Bounty In Radical New Approach To Fighting Cybercrime.” Forbes. Accessed October 27, 2022. https://www.forbes.com/sites/martinrivers/2021/07/18/got-bitcoin-will-buy-intel-us-government-offers-cryptocurrency-bounty-in-radical-new-approach-to-fighting-cybercrime/.

Roberts, Daniel. “How Crypto Adoption by Companies like Visa, PayPal, and Tesla Is Creating a Network Effect.” Yahoo, February 2021. https://finance.yahoo.com/news/how-crypto-adoption-by-companies-like-visa-pay-pal-and-tesla-is-creating-a-network-effect-214639389.html.

Rogers, Everett M. *Diffusion of Innovations*. 4th ed. New York: Free Press, 1995.

Rosen, Stephen Peter. *Winning the next War: Innovation and the Modern Military*. Cornell Studies in Security Affairs. Ithaca, NY London: Cornell University Press, 1994.

Rowen, Michael. “Cryptocurrency Utility for Special Operations - Video Portal - Naval Postgraduate School,” September 13, 2022. https://nps.edu/web/nps-video-portal/-/cryptocurrency-utility-for-special-operations.

Smith, Brian A. “Applying Financial Capabilities to Achieve Multi-Domain Effects: Using Financial Capabilities Operationally Rather Than Transactionally.” *The Journal of the American Society of Military Comtrollers*, Armed Forces Comptroller, 67, no. 4 (Fall 2022): 54. https://asmconline.org/armed-forces-comptroller/.

Team, Chainalysis. “Transparency in Blockchains Senate Hearing.” Chainalysis, March 22, 2022. https://blog.chainalysis.com/reports/senate-hearing-underscores-value-of-blockchain-transparency/.

Thomas. *Statement of General Raymond A. Thomas, U.S. Army Commander United States Special Operations Command Before the Senate Armed Services Committee*, 115th Cong. (2017) (statement of Raymond A. Thomas, USSOCOM Commander), May 4, 2017.

TxTenna. “TxTenna: Route Around Censorship,” November 28, 2022. http://txtenna.com/.

United 24. “Aid For Ukraine – Donate Crypto to Ukraine.” United 24: The initiative of the President of Ukraine. Accessed October 27, 2022. https://u24.gov.ua/.

University of Southern California. “Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court.” USC Shoah Foundation, June 10, 2022. https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes.

USSOCOM. “SOF Vision and Strategy.” Tampa, FL: U.S. Special Operations Command, April 11, 2022. https://www.socom.mil/sof-vision-and-strategy.

Vranken, Harald. “Sustainability of Bitcoin and Blockchains.” *Current Opinion in Environmental Sustainability*, Sustainability governance, 28 (October 1, 2017): 1–9. https://doi.org/10.1016/j.cosust.2017.04.011.

Williams, Daniel. “GoTenna with Blockstream Satellite.” Blockstream, May 11, 2019. https://blog.blockstream.com/en-gotenna-satellite-api-integration/.

Winkie, Davis. “New MOS and Formations Could Come to Army Spec Ops in Tech-Savvy Era.” Army Times, July 2022. https://www.armytimes.com/news/your-army/2022/07/28/new-mos-and-formations-could-come-to-army-spec-ops-in-tech-savvy-era/.

Zitser, Joshua. “Impoverished Afghan Women Are Receiving Emergency Aid in Crypto as the Taliban Limits Cash Withdrawals and Millions Go Hungry.” Business Insider. Accessed October 27, 2022. https://www.businessinsider.com/afghanistan-women-turn-to-cryptocurrency-to-feed-their-families-2022-1.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California