The Proliferation of Decentralized Trust Technology

by Alexander G. Mullin

> ***We will use sophisticated investigative tools to disrupt the ability of criminals to use online marketplaces, crypto-currencies, and other tools or illicit activities.***
>
> ***— U.S. National Security Strategy, December 2017***

The inclusion of the quote referenced above on page 12 made the December 2017 National Security Strategy (NSS) the first United States strategic level document to acknowledge the powerful technology underpinning cryptocurrencies – blockchain. This excerpt from the NSS is particularly important because it acknowledges the illicit use of cryptocurrencies, like bitcoin, but it fails to mention anywhere else in the document the landscape altering potential of blockchain technology.[1] This shows a fundamental misunderstanding of blockchain technology at the strategic level, with a failure to grasp the potential applications and threats of the rapidly evolving *decentralized trust technologies* emerging throughout the world.

Decentralized trust technology (DTT) has characteristics utilizing cryptography and consensus algorithms across dispersed network participants to create verifiable relationships. DTT is a term coined in this paper to represent the current and future collection of ideas, applications, and protocols created using, or inspired by, blockchain technology. In this ecosystem there is currently much debate over terminology ranging from trust vs. trustless, what decentralized and distributed each really mean, and the varied use of "distributed ledger technology" (DLT), "shared ledger technology," "consensus ledger technology," and "mutual distributed ledger technology" as descriptions for blockchain technology.[2] The most popular, DLT, is conveniently used interchangeably with the term blockchain, but in reality blockchain is a subset of DLT, while DLT is an umbrella term to describe applications that distribute data in consensus.[3] Challengers to blockchain structure, such as Directed

Major Alexander G. Mullin is a U.S. Army officer currently assigned to the School of Advanced Military Studies. He holds a Master of Business Administration from Georgetown University, a B.S. in Economics from the United States Military Academy at West Point, and is a graduate with honors from the U.S. Army Command and General Staff College at Fort Leavenworth, Kansas.

Acyclic Graph (DAG), utilize “directed” nodes without loops to achieve superior characteristics, with which blockchain struggles, like scalability.[4] In this case, blockchain would be considered a chain-shape version of a DAG, and both blockchain and DAG receive a DLT classification.[5] This terminology can be very confusing, and the ecosystem is only going to continue to innovate at a blinding pace as user adoption increases, and huge sums of currency are invested into research and development for novel technology. These yet unknown novel technologies will continue to challenge the fundamental ideas of blockchain and DLT, as they attempt to push limits and improve upon weaknesses. It can be expected that new technology inspired by blockchain could move away from fundamental characteristics or create “hybrid” technologies. In this light, DTT, as a new term, descriptively represents blockchain, DLT, DAG, bitcoin, ethereum, cryptocurrency, and any other innovations in this space. DTT captures the essence of what this ecosystem represents, both now and in the future.

In this paper, I will explore how DTT presents significant opportunities and potential threats through the study of a current use case. I will apply a primary perspective, considering the United States National Security point of view, with a secondary lens for ethical considerations. This brief study will produce a set of recommendations for the United States to utilize when developing a strategy for the evolving DTT ecosystem.

Background

Satoshi Nakamoto altered the landscape of modern technology after introducing bitcoin in 2008. He described his new payment, in his own words, as “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.”[6] The idea that transactions do not require trust is the ground breaking technology behind bitcoin. Blockchain is a distributed ledger that records every transaction across a decentralized system. This system allows anyone to verify transactions that are unchangeable (immutable) and requires no central authority as a trusted actor. Blockchain allows market participants to execute costless verification, while largely eliminating the costs of auditing within a system.[7] Bitcoin, a cryptocurrency, is presently the center of attention, instead of blockchain as a whole, but it is just the beginning of a long line of industry disrupting uses.

Innovative use case: Syrian refugees in Jordan receive aid through a retina authenticated blockchain

As of January 2018, the World Food Programme has delivered aid using their ethereum-based blockchain application to more than 100,000 refugee camp residents.[8] Through a partnership with Irisguard, a biometrics technology company, refugees are able to access World Food Programme assistance in refugee grocery markets through a retina scan.[9] This use-case leverages many of the hallmark factors that make blockchain a disruptive technology. Most importantly, aid is tracked and verified until it reaches the hands of those in dire need of help.

The pilot application, Building Blocks, was launched in May 2017 at the Azraq Refugee Camp for Syrian refugees.[10] The World Food Programme estimates that the ability to eliminate bank transactions through their blockchain application will save in excess of $150,000 monthly in bank fees.[11] In the humanitarian aid sector, questions about how much aid is lost to corruption, and verifying if aid is actually applied to a desired outcome, are constant concerns. In addition, humanitarian aid organizations often lack the personnel to have oversight over aid distribution. The Building Blocks application abruptly ends these concerns with straight-to-refugee disbursement of aid, eliminating corruption and providing a costless verification of the aid delivery. There are psychological benefits as well. Refugees are empowered through their own utilization of aid in the refugee grocery stores, rather than lining up for food handouts in the traditional distribution model.[12] This example also provides a window into the future of digital identity applications, since The World Bank estimates that more than one billion people are unable to prove their identity, which means biometric authenticated blockchain technology provides a way for un-verified people to create a digital identity.[13]

United States National Security Perspective

From a United States National Security perspective, there are vast opportunities for this use-case. The United States' efforts in Afghanistan, over a fourteen-year period, funded $68 billion for Afghan security forces.[14]

> "Corruption undermined the U.S. mission in Afghanistan by fueling grievances against the Afghan government and channeling material support to the insurgency."
>
> – Special Inspector General for Afghanistan Reconstruction[15]

A report by the Special Inspector General for Afghanistan Reconstruction (SIGAR) highlighted deeply troubling concerns over the complete lack of information the United States had about the Afghan National Security Forces, despite the billions of dollars in funding they received.[16] Inconsistent self reporting of Afghan National Security Forces introduced the possibility that the United States funded "ghost soldiers."[17] An April 2015, the SIGAR report found that the Department of Defense (DoD) could only provide financial documents for 40 percent of the $2.2 billion dollars of distributed Commander's Emergency Response Program funds.[18] Another SIGAR report found that over $154 million worth of fuel had been stolen in Afghanistan, and was likely fueling Taliban efforts.[19] This fuel theft was easily conducted through a mixture of corruption and poor record keeping.[20] All of these facts present a struggle between competing cultures in a war zone, and failing to reliably create accurate transactions with massive amounts of resources.

Beneficial DTT applications can help to solve these types of reoccurring problems the United States faced in Afghanistan. Afghanistan presents a unique opportunity for implementation of technology unrestricted by a low-technology economy. The issue for a potential DTT solution would be overcoming the adoption and education phases.

Applying a similar blockchain solution to the Building Blocks application in the Azraq Refugee Camp, the Afghan National Security Forces could eradicate accountability issues and erroneous personnel information. On a daily basis, simple biometric authentication at the troop level would instantly provide accurate data on each soldier, squad, company, and battalion. The leadership of the Afghan National Security Forces could know, in great detail, their true troop strength. This immutable and biometrically authenticated data trail would eliminate the ability for bad actors in the system to exercise corruptive tactics, like reporting "ghost soldiers."

The path to increasing the functionality of a blockchain solution for the Afghan National Security Forces is clear, with the assumption that adoption and education are successful, and that technology becomes part of everyday processes. The benefits of creating digital identities for each soldier is an opportunity to obtain accurate training data that senior leadership have previously desired. The preceding question, of how the $68 billion dollars of funding was truly utilized, becomes a simple review of accurate budgeting data stored within the blockchain. Individual soldier training, medical, equipment, and accountability records on an immutable data trail become a force multiplier.

A blockchain solution achieves accountability for the 60 percent of funds missing from the $2.2 billion Commander's Emergency Response Projects fund, while altering how funds can be utilized. Currently, many contracting entities achieve "middlemen" roles in the process for issuance of project funds, and they act as trusted intermediaries to ensure funds are utilized to complete projects. This system rewards those that receive a cut, while fund accountability is lost down the line, and end states remain potentially unknown. As previously explained, a core function of blockchain is the costless verification of two parties executing a transaction. In this case, only required "middlemen" in the project funding process would be allowed to continue their services, and each transaction for every project, down to the cent, could be easily audited. This accountability would fundamentally change the behavior of actors within the projects system. The review of how project funds meet desired end-states and affect the local economy would no longer be an abstract exercise.

Ethical Considerations

Significant ethical dilemmas should be considered when implementing DTT for innovative solutions. The dramatic results of the successful blockchain application in Jordan masks potential ethical issues. Similarly, ethical dilemmas are present in the theoretical case for blockchain use by the Afghan National Security Forces. Each case creates an immutable trail of personal data that increasingly promotes adding additional services for end-user functionality. This thought process eventually leads to a desire to create a full suite of services for end users.

An example of this grand vision is currently being utilized by the Estonian government, which has pioneered the country-as-a-service model with blockchain. Some experts believe that this has made it the world's most digitally advanced society.[21] Estonia began implementing operational blockchain solutions in 2012 for national health, judicial, legislative, security and commercial code systems.[22] Their e-Residency program is a transnational digital identity that allows anyone on earth to apply for a government issued ID with full access to Estonia's public e-services.[23] All of these pioneering efforts are supported by Guardtime's keyless signature infrastructure blockchain technology, which ensures stored data is immutable and 100 percent private.[24]

This example of a full suite of services utilizing blockchain seems like a natural continuation of the successful use-cases we see in Jordan and, theoretically, in Afghanistan. An ethical dilemma arises in the collection of an immutable trail of personal data within a digital identity. The temptation to analyze user financial data or health records is an exposure of private information. Further, private blockchains, similar to the one utilized in Jordan, are more exposed to cyber attacks than public, permissionless blockchains, like bitcoin. While this exposure is no different, in a sense, than data exposed from a conventional database, the immutability and verified nature of data on a private blockchain provides attackers a much higher degree of accuracy with stolen data.

United States Strategy Recommendations

Section 1646 in the National Defense Authorization Act for Fiscal Year 2018, outlines the current plan for a required briefing on blockchain technology. H.R.2810 was initially introduced on June 7, 2017, and became public law on December 12, 2017. The excerpt of Section 1646 is in Figure 1.

Recommendation #1

The United States must construct a strategy to ensure the domestic development of public and private sector innovation in the global DTT

H.R. 2810 – National Defense Authorization Act for Fiscal Year 2018

Subtitle C – Cyberspace-Related Matters

PART I – GENERAL CYBER MATTERS

Sec. 1646. Briefing on cyber applications of blockchain technology.

(a) Briefing Required – Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the heads of such other departments and agencies of the Federal Government as the Secretary considers appropriate, shall provide to the appropriate committees of Congress a briefing on the cyber applications of blockchain technology.

(b) Elements. – The briefing under subsection (a) shall include:

(1) a description of potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies;

(2) as assessment of efforts by foreign powers, extremist organizations, and criminal networks to utilize such technologies;

(3) an assessment of the use or planned use of such technologies by the Federal Government and critical infrastructure networks; and

(4) an assessment of the vulnerabilities of critical infrastructure networks to cyber attacks.

(c) Form of Briefing – The briefing under subsection (a) shall be provided in unclassified form, but may include a classified supplement.

(d) Appropriate Committees of Congress Defined – In this section, the term “appropriate committees of Congress” means –

(1) the Committee on Armed Services, the Select Committee on Intelligence, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Financial Services, and the Committee on Homeland Security of the House of Representatives.

Figure 1. Excerpt of Section 1646 of H.R. 2810.

ecosystem. Domestic innovation development ensures that learning and idea creation from new research and development flows through the public and private sectors in unison. This flow of information places the United States in a position of strategic initiative within the DTT ecosystem.

This should be the first priority in any required briefings and discussions on strategy development. The present priority in required briefings is a description of potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies. This fails to promote a true understanding of the implications of blockchain technology. This also leans on a common dualistic perspective on anything cyber security, which is an immediate emphasis to adversaries and bad actors.

Cyber solutions are created through a deep understanding of advanced technology, with a focus on proactive actions guided by regimented frameworks. Adversaries and bad actors will always identify cyber vulnerabilities. Outside of the most complex threats, many of the cyber solutions available are open source fixes to identified vulnerabilities, which implies the vulnerability is already exposed. This logic will always keep adversaries and bad actors in a positive position with the initiative. This is why a focus on deep understanding of advanced technology is imperative. This knowledge base is the foundation for providing clarity on why domestic development of innovative DTT is essential.

Within the National Security Strategy to "Promote American Prosperity" is the guideline to "lead in research, technology, invention, and innovation."[25] A strategy to develop innovative DTT accomplishes the prioritization of "emerging technologies critical to economic growth and security."[26] This is more important than ever as nations like Venezuela are creating initial country offerings as a means to access liquidity to bypass United States' sanctions. DTT applications are already testing the effectiveness of economic levers we have long relied on as a policy tool.

Recommendation #2

Streamline the implementation of public and private partnerships in the DTT ecosystem. There are two key priority actions outlined in the National Security Strategy to implement this recommendation: First, leverage private capital and expertise to build and innovate; and second, rapidly field inventions and innovations.[27]

Leveraging private sector expertise is paramount. This must be a true partnership with real alignment of resources and incentives. Currently, the U.S. government is organizationally encumbered with layers of stacked and outdated technology. This is a symptom of a culture attempting to utilize innovative technology while still resisting change. This is not an easy dilemma to solve, but a step in the right direction is true partnerships with the private sector. Government agencies will gain a far-sighted vision for emerging technologies from true public-private partnerships. This long-term vision can initiate the planning and resources necessary to adopt innovative technology at tempo, while shedding older technology layers. The current known use cases for blockchain are enough to disrupt processes within agencies across the government. However, it is the true public-private partnerships that will dismiss hype and ineffective blockchain use ideas so real innovation can be implemented.

Rapidly fielding inventions and innovation is a known weakness for interagency government organizations. Processes designed to ensure proper fielding are now encumbrances on emerging technology ready for government utilization. The DTT ecosystem presents a unique dilemma in that most of the innovation is happening with extremely low barriers to entry. This means that rapid fielding is necessary to even begin to match the pace of current innovations. Reliance on crypto-exchanges as the point of contact for government regulation is a pertinent example of how quickly the environment is evolving. In a recent conference, a crypto-exchange expert commented on a question that non-state actors or terrorist organizations do not have the ability to properly launch or list an initial coin offering because exchanges would never list such an endeavor knowing government interference could follow. However, in a short period of time, this comment may be viewed as irrelevant if decentralized exchanges operating as decentralized autonomous organizations become operable. These exchanges can act free of any ethical standards and could allow any currency or medium of value to be exchanged free of interference. This would allow terrorist organizations to move from illicit cryptocurrency transactions, that the government is currently concerned with, into their own initial coin offerings. Coupling this with a blockchain application that produces true anonymity would open avenues for unethical behavior without consequences. The key here is that public-private partnerships with rapid fielding of innovative technology provides the environment for strategic initiative.

Recommendation #3

In unison with recommendations one and two, the United States must embrace DTT and take global leadership in the promotion of legal, regulatory, compliance, and standards advancement. At present, there is a general lack of guidance or clear legal standards in the DTT ecosystem.[28] There have certainly been intensive, domestic efforts in the financial sector to provide guidance and standards. Europe is by-and-large taking a progressive stance towards DTTs and small pockets like the "crypto valley" in Switzerland are taking leadership on the development of guidance and standards.[29]

Perhaps the most important aspect of the United States taking leadership in the legal, regulatory, compliance, and standards environment is the application of ethics. Many DTT applications and ideas have discussion points surrounding ethical implications. Interesting systems and protocols are designed in different DTTs to promote good user behavior. However, these actions do not ensure users will always act in accordance with encouraged norms. There is no question that clear guidance and standards promote ethical behavior. Future technology in this space will create ideas that have yet be conceived. The United States can have a positive ethical effect on these future technologies by providing fair and clear guidance that embraces innovation. ***IAJ***

NOTES

[1] Jordan Daniell, "Cryptocurrency mention buried in US National Security Strategy" *Ethnews* (blog), ethnews.com, December 28, 2017, https://www.ethnews.com/cryptocurrency-mention-buried-in-us-national-security-strategy.

[2] Angela Walch, "The Path of the Blockchain Lexicon (And the Law)," *Review of Banking & Financial Law*, Vol. 36 (2016-2017): 719.

[3] Anthony Stevens, "Gaining clarity on key terminology: Bitcoin versus blockchain versus distributed ledger technology," *Hackernoon* (blog), Medium.com, April 23, 2018, https://hackernoon.com/gaining-clarity-on-key-terminology-bitcoin-versus-blockchain-versus-distributed-ledger-technology-7b43978a64f2.

[4] KC Tam, "Blockchain and the Challengers," *Good Audience* (blog), Medium.com, April 2, 2018, https://blog.goodaudience.com/blockchain-and-the-challengers-74e22cf0cf4e.

[5] Ibid.

[6] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org. Accessed September 28, 2017. https://bitcoin.org/bitcoin.pdf.

[7] Christian Catalini & Joshua Gans "Some Simple Economics of the Blockchain" (Working Paper, MIT, 2016), 0.

[8] "Building Blocks" accessed April 15, 2018. http://innovation.wfp.org/project/building-blocks.

[9] Ibid.

[10] "An Ethereum Blockchain is Restoring the Identity of Syrian Refugees" last modified April 15, 2018, accessed April 15, 2018. https://www.ccn.com/an-ethereum-blockchain-is-restoring-the-identity-of-syrian-refugees.

[11] "How Refugees are Helping Create Blockchains Brand New World" last modified March 14, 2018, last accessed April 15, 2018. https://www.wired.com/story/refugees-but-on-the-blockchain.

[12] "An Ethereum Blockchain."

[13] "How Refugees are Helping."

[14] Tim Craig, "Despite billions in U.S. funding Afghan forces have a problem with boots" *Washington Post*, May 5, 2016 https://www.washingtonpost.com/world/asia_pacific/despite-billions-in-us-funding-afghan-forces-have-a-problem-with-boots/2016/05/04/5d0b0e34-1062-11e6-8967-7ac733c56f12_story.html?utm_term=.756874a763ad.

[15] Special Inspector General for Afghanistan Reconstruction, *SIGAR-16-58-LL Corruption in Conflict: Lessons from the U.S. Experience in Afghanistan* (Arlington, VA, 2016), i.

[16] Special Inspector General for Afghanistan Reconstruction, *Supplement to SIGAR's January 2015 Quarterly Report to the United States Congress* (Arlington, VA, 2015).

[17] Brianna Ehley, April 30, 2015 "The U.S. could be Paying $2.3 Billion a Year for Afghan Ghost Soldiers" *The Fiscal Times* April 30, 2015. http://www.thefiscaltimes.com/2015/05/13/65-Billion-Effort-Train-Afghan-Army-Failing.

[18] Special Inspector General for Afghanistan Reconstruction, *SIGAR-15-49-SP Department of Defense Commander's Emergency Response Program (CERP): Priorities and Spending in Afghanistan for Fiscal Years 2004-2014* (Arlington, VA, 2015), 13.

[19] Special Inspector General for Afghanistan Reconstruction, *SIGAR-18-41-SP Management and Oversight of Fuel in Afghanistan: DOD is Taking Steps to Improve Accountability, but Additional Actions are Needed*. (Arlington, VA, 2018).

[20] Special Inspector General for Afghanistan Reconstruction, *SIGAR-18-41-SP Management and Oversight of Fuel in Afghanistan: DOD is Taking Steps to Improve Accountability, but Additional Actions are Needed*. (Arlington, VA, 2018).

[21] "Lessons From the Most Digitally Advanced Country in the World," last modified January 15, 2018, accessed April 15, 2018. https://www.forbes.com/sites/peterhigh/2018/01/15/lessons-from-the-most-digitally-advanced-country-in-the-world/#1db9fd6221ac.

[22] "2008 Blockchain" accessed April 15, 2018, https://e-estonia.com.

[23] "2014 e-Residency" accessed April 15, 2018, https://e-estonia.com.

[24] "KSI Blockchain" accessed April 15, 2018, https://e-estonia.com/solutions/security-and-safety/ksi-blockchain.

[25] National Security Strategy of the United States of America (Washington D.C., 2017), 20.

[26] Ibid.

[27] Ibid., 21.

[28] David Henderson, "Why Cryptocurrency Regulation Moves Faster in Smaller Jurisdictions" *Payments Journal* (blog), *paymentsjournal.com* October 10, 2017, http://paymentsjournal.com/cryptocurrency-regulation-moves-faster-smaller-jurisdictions.

[29] Ibid.