Design Considerations for Central Bank Digital Currencies (CBDCs)

by

William Peracchio

A Thesis
Presented to the Graduate Committee
of Lehigh University
in Candidacy for the Degree of
Master of Science
in
Computer Science

Lehigh University
May 2021

This thesis is accepted and approved in partial fulfillment of the requirements for the Master of Science.

William Peracchio

Design Considerations for Central Bank Digital Currencies (CBDCs)

____

Date

____

Thesis Advisor

____

Chairperson of Department

Contents

Design Considerations for Central Bank Digital Currencies

William Peracchio, Hank Korth

May 26, 2021

Abstract

Central Bank Digital Currencies (CBDCs) are one of the biggest potential use cases of blockchain technologies, whereby fiat currency transactions are put on a distributed ledger, creating at a minimum digital cash and opening the door for programmable logic in fiat currency. CBDCs have already begun to roll-out in different parts of the world, and large-scale projects look to bring CBDCs to millions, if not billions, of consumers in coming years. This work summarizes some common use cases and design considerations of CBDCs from existing literature, as well as discusses the potential technical and non-technical issues in a CBDC, particularly from the perspective of the US. Issues such as system decentralization, performance, and privacy are discussed and solutions proposed for mitigating the issues that may arise, including contributions regarding geographic segmentation of CBDC chains, the concept of international alloy CBDCs, and the use of zero-knowledge proofs as a privacy-compliant alternative to on-chain transaction data storage. Though the complexity of CBDCs likely lack a true one-size-fits-all solution for all nations, this work describes some common scenarios that would help guide engineering and policy choices for CBDCs.

1 Introduction

While blockchain technologies may have taken the public zeitgeist by storm in recent years, championed largely by cryptocurrencies such as Bitcoin, the large-scale public impact of blockchain technologies still remains brewing under the surface in the form of Central Bank Digital Currencies (CBDCs). CBDCs have gone from ideation to implementation in less than a decade and represent one of the biggest opportunities for central banks in recent decades to provide an augmented set of economic indicators and monetary policy tools [1]. The recent rollouts of CBDCs in many countries — most notably China with the Digital Yuan — has prompted many large Western economies such as the US Federal Reserve and the European Central Bank to look into and even begin developing their own CBDCs, but many questions remain as to specific implementation details [2] [3] [4]. CBDC design choices will be precipitated by a number of technical and political factors, which will likely prevent a one-size-fits-all solution.

CBDCs are defined by the R3 Consortium as a "digital payment instrument and store of value issued by and as a liability of a jurisdiction's central bank or other monetary authority" [5]. While cryptocurrencies have historically come from a libertarian ideological backing, promising decentralization away from governmental authorities, CBDCs flip this paradigm, with central banks (in the US the Federal Reserve System) playing the part of guaranteeing the chain's digital token as an equivalent to paper fiat currency.

These tokens, which represent digital versions of the local fiat currency, can therefore be thought of as "digital cash" at a minimum, and "programmable money" in a much more expanded sense [6]. In this regard, CBDCs can be seen as distant cousins to stablecoins such as Tether (USDT), but in CBDCs every token is precisely 1 of that currency because fiat is defined as what the Central Bank says it is, rather than an approximation as with stablecoins [7]. CBDCs would allow for a greatly expanded set of monetary policy tools for central banks, as is covered in **USE CASES AND REQUIREMENTS**. Despite their nascence, CBDCs are now being rolled out across the world.

2 Current Global Status

In a 2020 survey of more than 65 central banks, which represent 91% of global economic output, on the status of their CBDC considerations (if any), 86% of respondents said that they were looking into the possibility of a CBDC. Furthermore, nearly 60% of respondents said they were undergoing proof-of-concept trials with CBDCs, and 14% said they were undergoing pilot arrangements [8].

This past year also marked the first time a CBDC had gone live, with the Central Bank of the Bahamas launching the Sand Dollar, a digital cash equivalent of the Bahamian Dollar [9]. On a much larger scale, China has soft-launched the Digital Yuan in several cities in the early months of 2020, even utilizing the Lunar New Year celebrations to roll out the currency [2].

While technical details have remained scant on the Digital Yuan, it shows that CBDCs will not be relegated to a novelty for only small nationstates.

Recently, both the European Central Bank and the Federal Reserve have stated that CBDC projects are high-priority in nature over the coming years [4] [3]. Given the rollout of the Digital Yuan in China, increased political pressure may increase the focus of central banks into developing and launching CBDCs. Several other notable examples of CBDC developments include Canada, Jamaica, Japan, Singapore, and Sweden [8] [10] [11].

While not specifically a CBDC, Diem (formerly Libra) by the Diem Association led by Facebook represents an interesting tangent to CBDCs, with the promise of international payments made up of a collection of stablecoins of various global currencies [12]. While scrutiny from regulators has delayed the intended launch of Diem, it still represents a potential use case for interoperability between CBDCs, considering the Diem Association is already expected to act as a "de facto central bank," which in turn might be used to issue Libra tokens akin to a CBDC [13].

3 Use Cases and Requirements

CBDCs have become a hot topic for central banks because of what they can potentially do for improving economic policy control and for improving economic efficiency. Most obviously, CBDCs serving purely as a digital substitute for physical fiat currency would improve efficiency [14] [15]. In addition, CBDCs would serve as a way to reach the potentially millions of unbanked individuals within a central bank's jurisdiction, with the central bank serving as a rudimentary commercial bank for individuals who would otherwise lack access to basic financial services [14] [15]. CBDCs could also be used to help identify and minimize cases of fraud and tax evasion in areas that are prone to money laundering and minimize "off-the-books" transactions [14] [15]. Not only do CBDCs have the potential to provide finer grain control for existing central bank policy prescriptions, but they also would allow for a new array of potential economic policy tools for central banks that are well beyond the current scope of possibility.

As a means of augmenting existing central bank functions, CBDCs would, at a minimum, provide central banks with a far deeper and finer degree of macroeconomic data to work with. The Federal Reserve's *Summary of Commentary on Current Economic Conditions* publication ("Beige Book") of economic activity could be hypothetically transformed into a live dashboard with instantly-updating data, summarizing up from the transaction to the national level [16]. But beyond expanding data, policy knobs such as interest rates could be managed at a finer level of detail, such as allowing the central bank to increase *and decrease* the money supply via a process similar to coin mining/coin burning in the cryptocurrency space, potentially making open market operations by central banks obsolete. In this sense, the colloquial "turning on the printer" would be replaced by an effective "copy-cut-paste" paradigm.

These possibilities are extensions of existing central bank powers, but CBDCs also have the potential to open an entirely new array of policy tools. For example, CBDCs could effectively program currency, adding in positive and negative rights of use. Economic stimulus payments were a hot-button issue during the course of the COVID-19 pandemic, with policy questions if the money would effectively circulate around the economy [17]. A CBDC-enabled central bank could have the power to send stimulus checks with preconditions, such as requiring the money to be spent within a specified period of time or preventing the digital cash from being deposited in a financial institution, an effective "use it or lose it" memorandum to ensure that the money is being used to stimulate the economy. Even beyond the irregularity of stimulus payments, regular forms of welfare could also be augmented to come with strings attached, ranging from universal basic income to food stamps (this is not an endorsement of those strings, just that it *is* possible) [1]. In this sense, CBDCs allow the possibility of altering the fungible nature of currency: a dollar with no restrictions is practically worth marginally more than a dollar with restrictions (though these restrictions could be ephemeral, and are not necessarily permanent).

Depending on political leanings, the above possibilities may either seem incredible, horrifying, or both. CBDCs will come in many different forms, and will ultimately be heavily influenced by cultural and political norms. The focuses of these potential design differences are discussed in the **DESIGN CHOICES** section, but all CBDCs will have a baseline set of requirements

- engineering logic such as"2+2=4" and resistance to security penetrations are universal. These baseline requirements for CBDCs are well documented and will not be delved into extensive detail here [1]. At a high level, CBDCs will need to be a comparable substitute to traditional fiat for end users in terms of convenience and acceptability, at least initially. CBDC payments will need to be highly available and near instant, where payments are able to be made at any time, anywhere (including offline for short periods), with almost no settlement time. System security and resiliency to cyberattacks will be of paramount importance, given the risk of financial loss if programmed incorrectly [1].

4 Design Choices

Central banks will be faced with numerous design choices for their CBDCs, which will be influenced heavily by political objectives and technical requirements in their respective nations. And as there is no one-size-fits-all policy objective for something as large and as varied as a national economy, so too will there not be a single CBDC design that works for all central banks. Some design choices that are relevant in the discussion of CBDC design include level of centralization in the system, performance, and privacy and transparency.

4.1 Centralization vs. Decentralization

In a traditional database, or even general information system, data is stored in a centralized manner. When a search request is made to Google, information is stored on and retrieved from some of Google's data centers, with the entity of Google.com serving as the central arbiter in the system. Even if there are multiple physical data centers, the illusion of one singular Google is given to the user, representing a central system. The appeal of blockchain technology is that the need for centralization is no longer a requirement. Cryptocurrencies, which are largely powered by blockchain, generally keep this promise of decentralization a core tenet of the system - Bitcoin, for example, is stored on millions of nodes. But, this decentralization comes at a cost in regards to performance - whereas Visa is able to process tens of thousands of transactions per second at peak performance, a transaction in Bitcoin could take about an hour to completely settle [18] [19]. Generally speaking, increased centralization leads to faster settlement and consistency times, across all forms of distributed systems. While there have been performance improvements in this area of nearly pure decentralized systems such as Stellar, decentralization is a hard selling point for a central bank from a political perspective [20]. A central bank is unlikely to design a system where it does not have authority over the members of that system, which makes the performance of decentralized systems a moot point for CBDCs.

Rather than a purely decentralized architecture, one can imagine a state of semi-centralization, where governmental entities, such as the Federal Reserve and its member banks, are given additional power within the system to serve as arbiters in the network. Semi-decentralization opens the door for increased performance as covered in the **PERFORMANCE** section, but also allows for a more politically palpable sell. Semi-centralization could also include putting a requirement on financial institutions to do heavy lifting in monitoring network health, including letting commercial banks serve as validator nodes on the system. End users would not be able to store full copies of the CBDC history from a storage perspective, but could be implemented in a structure similar to light nodes on a traditional blockchain system [21].

In addition to just the level of centralization with regard to node dispersal, the level of tiers in the system must also be selected. In existing CBDC literature, there is the general consensus of two types of vertical architectures for CBDCs: one-tier and two-tier systems [15]. In one-tier systems, the central bank interacts directly with end users, and in the two-tier system, the central bank interacts with commercial banks, which in turn interface with end users [5].

The two-tier system is much closer to what currently exists in most Western democracies, and it seems unlikely that central banks would want the additional overhead of dealing with end users via the one-tier system (at least initially), let alone considering the significant potential for push back from commercial banks on this move. The importance that the familiarity of a two-tier structure provides also cannot be understated from a consumer perspective: privacy concerns likely become mollified if a new system has participants directly transacting with the same parties as the old system. The two-tier system also allows the current set of segregation of duties that exist between commercial banks and the central bank to still largely be left in place. Consumers are at least marginally aware that their transactions are visible to a bank or credit card company for transactions with a check or credit card and would be in a situation where their transactions are still being processed by these institutions. In conjunction with this, roll-out for a two-tier system may be done in phases by each individual tier. A phased roll-out would likely start at the central bank-commercial bank tier as it is easier to coordinate among a relatively small number of financial institutions and the central bank on requirements rather than coordinating a large-scale public roll-out to the general public. The infrastructure for the first tier could be quietly built out, with no potential change to the individual consumer until the roll-out of the second tier.

4.2 Performance

Performance considerations, like most design considerations with CB-DCs, will be heavily country specific. For reasons that should be apparent, The Bahamas will need a very different performance benchmark on transactions per second compared to the United States, based on differences in population magnitudes alone. While literature is scarce at estimating exactly how many transactions involve USD occur per second, Visa alone performs about 1,700 transactions per second with the ability to scale up to 65,000 transactions per second [18]. This benchmark would serve as an absolute floor for what a US CBDC system would need to effectively operate at when one considers that Visa is only one single credit card provider, and that only approximately one quarter of all consumer transactions in the US utilize credit cards [22].

For this reason, larger economies such as the US, may need to explore some form of segmentation when considering how to effectively scale to these large transaction rates. Currently, semi-centralized distributed ledger technology (DLT) systems such as Hyperledger Fabric are able to scale to 10,000-20,000 transactions per second, with the goal of eventually hitting 100,000 transactions per second [23]. Perhaps most obvious method of segmentation to alleviate the performance issue bottleneck is geographic, considering that most consumer transactions exist within a given geographic area and that commercial transaction laws would already need to consider geographical boundaries for taxation and regulatory purposes.

One could imagine different segmentations of a CBDC network at the state level or local level in the US, with jurisdiction-specific laws programmed into the network to reflect regulations and overarching federal networks for transactions that cross these boundaries, similar to existing regulations in the realm of the Commerce Clause [24]. With periodic reconciliation between these networks, the performance thresholds needed can potentially become orders of magnitude less than the national requirements. This segmentation could allow for increased parallelism in a system and take load off of particular bottlenecks in a system. In addition, operating under the assumption of a two-tier architecture, multiple tiers of transactions and multiple intermediaries at the commercial bank level would further help to reduce stress points in the system (e.g., a commercial bank would only need to worry about the consumer transactions that directly involve an account from that bank). While multiple chains add in a layer of complexity regarding cross-chain transactions, recent developments in the space of semi-centralized blockchain assets such as Ripple could be used a reference for making this technically feasible [25] [26].

In the case of particularly "global" currencies such as the US Dollar, considerations will also need to be made to consider the significant amount of transactions that may occur outside the true jurisdiction of the central bank issuing the digital currency. Not only does the USD serve as the world's reserve currency, but there are also several countries that officially utilize the US dollar, and many dozen more that either peg their currency to the dollar and/or utilize the dollar for sufficiently large/important transactions [27]. In fact, the Federal Reserve Bank of St. Louis even estimates that 60%, or the outright majority of US dollars are in circulation outside the US [28]. The global power-play for international reserve currencies has been well-documented, and it is not unlikely that major economic players will utilize CBDCs as a chance to grow their currency's power globally [29].

This geopolitical consideration may require some level of network segmentation away from the main network that is technically outside the jurisdiction of the central bank. As discussed earlier, CBDCs allow for the possibility of removing true fungibility in currency and could theoretically be used to segment currencies at almost a "flavor" level: the Republic of Palau, which has the USD as the official currency, could program a set of restrictions to create a Palaun-flavored USD [30]. This alloyed CBDC could theoretically still be interoperable with the regular USD CBDC, and the Palaun restrictions could be ignored if used in the US. The politics that would be involved with negotiating what restrictions, if any, would be permissible between nationstates is well-beyond the scope of this paper, but the possibility exists nonetheless.

4.3 Privacy and Transparency

Perhaps the aspect of CBDC design that will vary the most among countries based on cultural norms, rather than purely technical requirements, will be that of designing between privacy and transparency. The general trade-off that exists between privacy and transparency is well-documented, and is not specific to CBDC design.

Due to the ever-evolving nature of privacy regulations such as GDPR or the CCPA, CBDCs will need to be flexible when considering the possibility of storing sensitive user information on the network [31] [32]. Even if personal data is sufficiently encrypted, the immutability of a blockchain-based CBDC would render complexities when considering privacy regulations such as "the right to be forgotten," considering that blockchain histories cannot be truly forgotten. In addition, different privacy regulations in different jurisdictions would dramatically increase the required customization that would need to exist in a CBDC if data were to be stored on chain. For example, if the US faces 50 different privacy regulations for 50 different states, a set of possible transactional relationships needs to consider all possible combinations of these subdivisions, which would balloon to '$C(50, 2) = 1225$' transactional relationships even when only considering two party transactions.

Rather than storing personal information on the network in transactions, the use of third-party verifiers for personal information, such as Sovrin, could be utilized to help avoid this issue of data sovereignty in combination with zero-knowledge proofs [33]. Zero-knowledge proofs are well-documented in their ability to provide verification of facts without revealing what the underlying facts are [34] [35]. In the context of a CBDC, this form of transacting could even be able to enhance privacy for consumer transactions. In a modern scenario, a situation where a consumer attempts to buy an alcoholic beverage would currently require the showing of an ID card, with name, drivers license, and other personal information only to convey the required field of birthdate to the bartender. A zero-knowledge verification scheme could send the result of the question "is this customer at least 21 years old?" to the bartender, with no other fields revealed. While zero-knowledge verification would not require a CBDC for implementation, a CBDC could likely build out the social infrastructure needed to make identity verification systems mainstream, as a byproduct of *not* storing information on the CBDC itself.

5 Conclusion

Central bank digital currencies represent the likely future (and in some limited cases, present) of currency as we know it today. CBDCs will be subject to a rapid phase of expansion and maturity in the coming years and will be influenced in a dynamic environment of changing technology and political pressures. The design choices faced by central banks in the areas of centralization, privacy, performance, and regulatory security will be highly variable based on a number of country-specific factors.

6 References

[1] S. Allen, S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, E. Prasad, K. Wüst, and F. Zhang, "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," The Brookings Institution, Jul. 2020. [Online]. Available: `https://www.brookings.edu/research/design-choices-for-central-bank-digital-currency-policy-and-technical-considerations/`.

[2] E. Cheng, "CHINA ECONOMY China plans to hand out $1.5 million in a digital currency test during the Lunar New Year," Feb. 2021. [Online]. Available: `https://www.cnbc.com/2021/02/08/china-`

to-hand-out-1point5-million-in-lunar-new-year-digital-currency-test.html.

[3] S. Hansen, "Fed Chair Powell Says Digital Dollar Is A 'High Priority Project'," Feb. 2020. [Online]. Available: https://www.forbes.com/sites/sarahhansen/2021/02/23/fed-chair-powell-says-digital-dollar-is-a-high-priority-project/?sh=6464097f7e4c.

[4] "A digital euro," 2021. [Online]. Available: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html.

[5] G. Calle, R. Coassin, and L. Douglas, "CBDC Taxonomy Design Choices," R3, Mar. 2021. [Online]. Available: https://www.r3.com/cbdc-research/taxonomy-design-choices/.

[6] H. Arslanian, W. Gee, L. Gazmararian, J. Tao, D. Diemers, T. Campione, J. Park, C. Suzuki, F. Axisa, P. Yeo, D. Fitzgerald, C. Y. Cheung, L. Wang, G. Law-Kun, A. Keller, G. Dobrauz, P. Adam-Kalfon, J. Amos, M. J. Kashyap, and S. N. Lim, "The Rise of Central Bank Digital Currencies (CBDCs)," PricewaterhouseCoopers, Nov. 2019. [Online]. Available: https://www.pwc.com/gx/en/financial-services/pdf/the-rise-of-central-bank-digital-currencies.pdf.

[7] (2021), Tether Operations, [Online]. Available: https://tether.to/.

[8] C. Boar and A. Wehrli, "Read, steady, go? - Results of the third BIS survey on central bank digital currency," Bank for International Settle-

ments, Jan. 2021. [Online]. Available: https://www.bis.org/publ/bppdf/bispap114.pdf.

[9] "Mastercard and Island Pay Launch World's First Central Bank Digital Currency-Linked Card," Feb. 2021. [Online]. Available: https://www.mastercard.com/news/press/2021/february/mastercard-and-island-pay-launch-world-s-first-central-bank-digital-currency-linked-card/.

[10] T. Akhtar, "Jamaica's Central Bank to Pilot CBDC Beginning in May," Mar. 2021. [Online]. Available: https://www.coindesk.com/jamaica-central-bank-pilot-cbdc-may.

[11] O. Ummelas and R. Lindeberg, "Swedish Central Bank Reveals First Study of Digital Currency," Apr. 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2021-04-07/sweden-s-central-bank-reveals-first-study-of-digital-currency.

[12] R. Browne, "Facebook-backed Diem aims to launch digital currency pilot later this year," Apr. 2021. [Online]. Available: https://www.cnbc.com/2021/04/20/facebook-backed-diem-aims-to-launch-digital-currency-pilot-in-2021.html.

[13] R. Brandom, "Facebook's cryptocurrency has a trust problem," Jun. 2019. [Online]. Available: https://www.theverge.com/2019/6/18/18683867/facebook-cryptocurrency-libra-calibra-trust-banking.

[14] U. Bindsell, “Tiered CBDC and the financial system,” European Central Bank, Jan. 2020. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf.

[15] B. Coeuré, S. J. Cunliffe, T. Lane, F. Panetta, S. Uchida, C. Skingsley, F. Zurbrügg, L. Brainard, and H. S. Shin, “Central Bank Digital Currencies: Foundational Principles and Core Features Report No. 1 in a Series of Collaborations from a Group of Central Banks.,” Bank for International Settlements, 2020. [Online]. Available: https://www.bis.org/publ/othp33.pdf.

[16] *Beige Book, Summary of Commentary on Current Economic Conditions by Federal Reserve District*, Board of Governors of the Federal Reserve System. [Online]. Available: https://www.federalreserve.gov/monetarypolicy/beige-book-default.htm.

[17] B. Holzhauer, “Stimulus Packages Throw Money At Financial Crises. But Do They Actually Help The Economy?,” Sep. 2020. [Online]. Available: https://www.forbes.com/advisor/personal-finance/stimulus-packages-throw-money-at-financial-crises-but-do-they-actually-help-the-economy/.

[18] (2018). “Visa Fact Sheet, What you need to know about one of the world’s largest payments companies,” Visa, [Online]. Available: https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf.

[19] D. Dog, “How Long Does a Bitcoin Transaction Take?,” Sep. 2020. [Online]. Available: https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take.

[20] (2021), Stellar Development Foundation, [Online]. Available: https://www.stellar.org/.

[21] (Aug. 2020). “Classification and importance of nodes in a blockchain network,” SEBA Bank, [Online]. Available: https://www.seba.swiss/research/Classification-and-importance-of-nodes-in-a-blockchain-network.

[22] R. Kumar and S. O’Brian. (2019). “2019 Findings from the Diary of Consumer Payment Choice,” Federal Reserve Bank of San Francisco: Cash Product Office, [Online]. Available: https://www.frbsf.org/cash/files/2019-Findings-from-the-Diary-of-Consumer-Payment-Choice-June2019.pdf.

[23] *Hyperledger Fabric Documentation*, IBM Corp, 2016. [Online]. Available: https://openblockchain.readthedocs.io/en/latest/FAQ/usage_FAQ/.

[24] *Commerce Clause*, Legal Information Institute. [Online]. Available: https://www.law.cornell.edu/wex/commerce_clause.

[25] (2021), Ripple, [Online]. Available: https://ripple.com/.

[26] T. Louie, "Introducing decentralised XRP cross-chain bridges," Apr. 2021. [Online]. Available: https://medium.com/wanchain-foundation/ushering-in-xrps-defi-era-introducing-decentralised-xrp-cross-chain-bridges-d80a97e18f5f.

[27] T. Adkins, "Countries That Use The U.S. Dollar," Apr. 2020. [Online]. Available: https://www.investopedia.com/articles/forex/040915/countries-use-us-dollar.asp.

[28] R. G. Anderson, "How U.S. Currency Stacks Up—at Home and Abroad," Apr. 2007. [Online]. Available: https://www.stlouisfed.org/publications/central-banker/spring-2007/how-us-currency-stacks-upat-home-and-abroad.

[29] T. Elyashiv, "Op-ed: A new global arms race in digital finance is heating up," Jan. 2021. [Online]. Available: https://www.cnbc.com/2021/01/21/op-ed-a-new-global-arms-race-in-digital-finance-is-heating-up.html.

[30] *Flags, Symbols Currency Of Palau*, worldatlas.com. [Online]. Available: https://www.worldatlas.com/flags/palau.

[31] *Data protection*, European Commission. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en.

[32] *California Consumer Privacy Act (CCPA)*, State of California Department of Justice. [Online]. Available: https://oag.ca.gov/privacy/ccpa.

[33] (2021), Sovrin Foundation, [Online]. Available: https://sovrin.org.

[34] B. Lynn. (). "Zero-Knowledge Proofs," [Online]. Available: https://crypto.stanford.edu/pbc/notes/crypto/zk.html.

[35] (Dec. 2018). "What is a Zero Knowledge Proof?" Sovrin Foundation, [Online]. Available: https://sovrin.org/faq/what-is-a-zero-knowledge-proof/.

7 Vita

William Peracchio is from Manasquan, New Jersey and born to parents David and Anne-Marie Peracchio. William Peracchio graduated with a Bachelor of Science in Computer Science and Business and triple minors in Data Science, Economics, and Entrepreneurship in January 2021 from Lehigh University with Highest Honors and as a member of Phi Beta Kappa Honor Society, Beta Gamma Sigma Honor Society, Tau Beta Pi Honor Society, and Upsilon Pi Epsilon Honor Society. Immediately following the conclusion of his undergraduate degree, William enrolled in the Master of Science in Computer Science program at Lehigh University as a Presidential Scholar, and graduated from the program in May 2021 following a single semester as a full graduate student. While at Lehigh University, William served the Computer Science and Engineering Department and the P.C. Rossin College of Engineering and Applied Sciences as the President of the Computer Science and Business Student Association, the President of the Rossin Junior Fellows Honor Society, a Teaching Assistant for CSE 340 - Analysis of Algorithms and CSE 298 - Modern Software Development Methodologies, and helped to found the Upsilon Pi Epsilon Computing and Information Sciences Honor Society chapter at Lehigh University. Following graduation, William is attending Schwarzman College at Tsinghua University in Beijing, China as a Schwarzman Scholar, studying for a Master of Global Affairs. William hopes to work at the intersection of technology, business, and policy in the future.