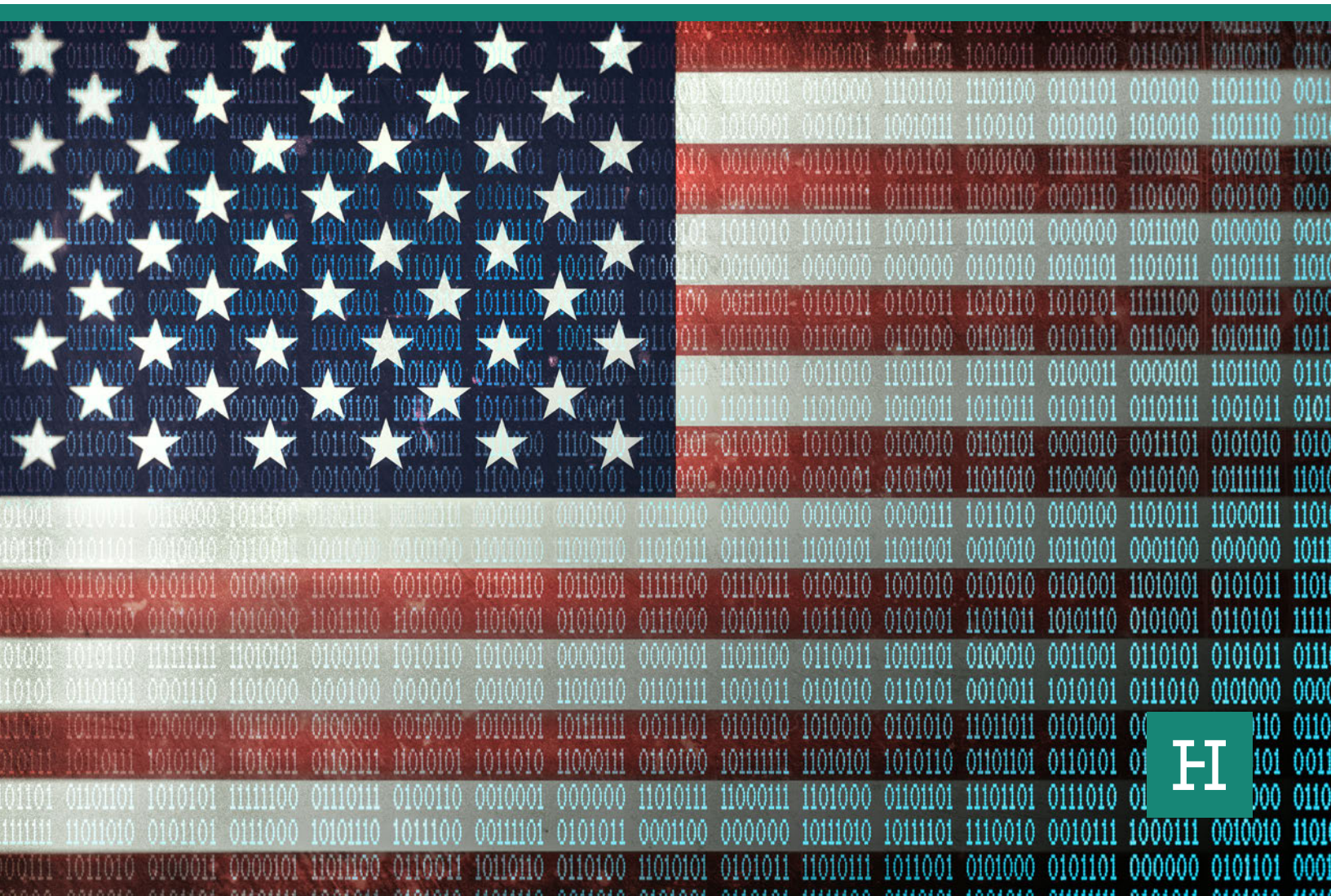
Hudson Institute

APRIL 2023

Prosperity at Risk: The Quantum Computer Threat to the US Financial System

BY ALEXANDER W. BUTLER AND ARTHUR HERMAN
QUANTUM ALLIANCE INITIATIVE



ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, energy, technology, culture, and law.

Hudson seeks to guide policymakers and global leaders in government and business through a robust program of publications, conferences, policy briefings, and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Fourth Floor
Washington, D.C. 20004

+1.202.974.2400
info@hudson.org
www.hudson.org

Cover: (Getty Images)

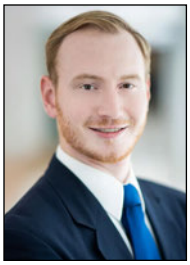
Hudson Institute

APRIL 2023

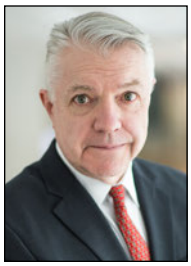
Prosperity at Risk: The Quantum Computer Threat to the US Financial System

BY ALEXANDER W. BUTLER AND ARTHUR HERMAN
QUANTUM ALLIANCE INITIATIVE

ABOUT THE AUTHORS



Alexander W. Butler is a research associate and project manager at Hudson Institute, supporting the work of Senior Fellow Arthur Herman and serving as associate director of the Quantum Alliance Initiative. He is the author of the anthology chapter "Quantum Tuesday: How the US Economy will Fall, and How to Stop It" in *Convergence: Artificial Intelligence and Quantum Computing* (Wiley, 2023). Before joining Hudson, Alexander worked at the American Society of Naval Engineers and the Navy League of the United States. Alexander holds a BS in economics from James Madison University's Zane Showker College of Business, where he focused on macroeconomics and applied econometrics.



Arthur Herman, PhD, is a senior fellow and director of the Quantum Alliance Initiative at Hudson Institute. His research programs analyze defense, energy, and technology issues. Dr. Herman is the author of ten books, including *The Viking Heart: How Scandinavians Conquered the World* (Mariner Books, 2021), *How the Scots Invented the Modern World* (Crown, 2002), *Gandhi and Churchill: The Epic Rivalry That Destroyed an Empire and Forged Our Age* (Bantam, 2008), *Freedom's Forge: How American Business Produced Victory in World War II* (Random House, 2012), *To Rule the Waves: How the British Navy Shaped the Modern World* (Harper Perennial, 2005), *Douglas MacArthur: American Warrior* (Random House, 2016), and *1917: Lenin, Wilson, and the Birth of the New World Disorder* (HarperCollins, 2017).

Dr. Herman served on the National Security Council as senior advisor to the national security advisor from 2020 to 2021. He comments frequently on technology and strategy at the *Wall Street Journal* and *The Hill*, and his column on quantum, AI, and other advanced technologies appears regularly at *Forbes*.

The authors would like to thank Daley Pagano, Andrew Pluemer, and Michael Tarino for their outstanding qualitative and quantitative research assistance. Past supporters of the Quantum Alliance Initiative include ID Quantique, QRCrypto, QRC Americas SA, Qubitekk Inc., Quintessence Labs, QuNu Labs Pvt. Ltd., Rivada Networks, and SK Telecom. Additional thanks go to the Smith Richardson Foundation for their support for this report, and other work conducted at the Quantum Alliance Initiative.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Due to the deep interconnectivity between public and private institutions and the inherent sensitivity of equity and credit markets, the financial sector network presents a prime target for a quantum attack. Even if America's financial sector could install sufficient protections against conventional cyberattacks, it will remain a valuable and vulnerable target for a quantum-powered cyberattack.

Despite the many benefits that quantum computing is poised to bring to the financial sector, the threat of quantum-enabled cyberattacks and, more specifically, quantum decryption holds the potential to outweigh any gains in computational efficiency and accuracy. The impact of a cascading quantum attack on major banks, the Federal Reserve, or stock exchanges and derivative exchanges could be calamitous for the United States and the global economy. The risk of a catastrophic attack and financial collapse rises to levels that eclipse the 2008–09 crisis or the Great Depression.

Consequently, now more than ever, cyber threats, especially in the future quantum-enabled era, pose a critical risk to our national, economic, and even societal security—especially within the financial sector. While there are numerous attack vectors for a quantum-enabled adversary to exploit and a variety of points of failure within the vast financial system, experts have placed growing emphasis on the threat of a breakdown in the interbank payment system, specifically real-time-gross-settlement (RTGS) systems such as the Fedwire Funds Service that the US Federal Reserve provides.

The combination of the reliance on digital security that will be exposed to quantum intrusion, internally centralized operational design, and the overall concentration of network topology within Fedwire drastically increases the potential for a systemically disruptive event. If an adversary prevents the settlement of cross-border and domestic transactions between banks operating within the Fedwire RTGS system, a cyberattack could lead to liquidity issues for receiving parties, contract breaches, and payment and obligation failures, among other issues.

The high degree of interconnectivity within the financial sector can accelerate financial contagion and spread systemic risk. Consequently, a cyber disruption to Fedwire can ignite a chain effect in which the initial halt in interbank transaction processing can swell into liquidity crises in the financial system at large. Once a cryptographically relevant quantum computer exists, it could access the Fedwire network and initiate a disruption to payments, cause coordination failures within the system that hinder efforts toward resilience, and ultimately irreparably affect the US economy in the fashion of, or likely worse than, the 2008 financial crisis.

To account for both the direct financial impacts to the affected bank and the cascading effects throughout the broader financial system and the US macroeconomy, we implemented a two-staged economic analysis to quantify the total indirect economic impacts of a quantum computer cyberattack on the Fedwire interbank payment system. Our analysis demonstrates that such a hack would result in declines in annual real GDP ranging from over 10 percent in the baseline scenario to 17 percent in the maximum impact attack scenario, which begins with the initial attack scenario and lasting through the resulting six-month recession. Furthermore, our results indicate that such a decline in aggregate output would comprise a loss of between $2 and $3.3 trillion in indirect losses alone, as measured by GDP-at-risk.

Overall, our results demonstrate that a quantum-enabled cyberattack on Fedwire, or any other RTGS system or key financial market infrastructure (FMI), would result in catastrophic financial losses for the national economy. It could well launch us into the next Great Depression due to the intensity and duration of the first-, second-, and third-order indirect impacts modeled in our analysis.

The US government has designated financial services infrastructure as critical to national and economic security. Fortunately, both policy and technological solutions exist. However,

without the system-wide adoption and implementation of quantum-safe encryption, quantum key distribution, or post-quantum cryptography, the US financial system will remain under threat, and our collective economic security will be at stake as the quantum future takes shape.

Regardless of financial and technological resilience, both regulators and market participants need to take on this known threat and win the quantum arms race.

We present four steps that policymakers can implement to get a head start in this quantum race.

First, they need to adopt and migrate to the National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) standards for Fedwire protection with a clear timeline for implementation and replacement of legacy encryption systems.

Second, the chair of the Federal Reserve should call a Quantum Security Summit involving America's largest banks and financial institutions to insist they start laying out plans for becoming quantum-secure.

Third, Congress needs to set a deadline for all 12 Federal Reserve banks to be quantum-secure.

Finally, the government should create a quantum security taskforce at the Federal Reserve to oversee and implement the migration timeline.

Please note that we originally derived our econometric calculations at the end of the second quarter of 2022. While we acknowledge that there have been profound changes in the financial system and the general economy since then, we emphasize that our results highlight the risks associated with critical infrastructure left exposed to the emerging quantum threat. Furthermore, although our analysis relies on several assumptions and on extrapolated data and information (see Appendix B), our results are likely an underrepresentation of the impacts of such a catastrophic event.

1. INTRODUCTION

Key Takeaways:

- It is imperative to develop plans and deploy solutions that will protect against quantum decryption, including quantum-resistant cryptography and quantum-enabled cryptographic technologies.
- Since 2021, the Quantum Alliance Initiative at Hudson Institute has been generating a series of econometric studies on the quantitative cost of future quantum computer attacks. Our research outlined trillions of dollars at risk in the event of a major hack of electrical utilities or cryptocurrencies.

> I would say that the risk that we keep our eyes on the most now is cyber risk. So you would worry about a cyber event . . . scenarios in which a large payment utility, for example, breaks down and the payment system can't work. Payments can't be completed . . . Things like that where you would have a part of the financial system come to a halt, or perhaps even a broad part.
>
> —Federal Reserve Chairman Jerome Powell[1]

Quantum computing (i.e., harnessing the power of quantum physics as the basis for processing data and information) is about to transform our technologically driven world. Powered by the elusive mechanical forces of quantum physics, these entanglement-based computers hold the potential to advance society and enhance the human condition in a range of fields,

Photo: People walk by the New York Stock Exchange at the start of the trading day on June 3, 2022, in New York City. (Photo by Spencer Platt/Getty Images)

from improving pharmaceutical research to constructing exact models for measuring climate change, solving the complex mathematical problems that underlie the physical sciences, and revolutionizing medical science in the form of quantum sensors.

At the same time, the very properties quantum computers will use to solve the most complex mathematical problems ever imagined—problems beyond the capability of even the most powerful supercomputers—will also enable them to unravel "unsolvable" mathematical formulas. Such formulas underpin today's public encryption systems that protect vital data and networks, from banks and financial markets to air traffic control systems and the power grid—not to mention our government's most sensitive information.

This is because current encryption regimes rely on the difficulty associated with the factorization of immensely complex numbers, which classical computers might take years or decades to crack, if they can at all. But future quantum computers will excell at this kind of factorization. In a matter of minutes or even seconds, large-scale quantum computers will become the master code-breakers and master-key makers, which can give adversaries direct access to our most sensitive information, communications, and techno-infrastructure.

Regarding future quantum computers, the RAND Corporation report *Securing Communications in the Quantum Computing Age* concludes:

> Their unprecedented power may also enable them to crack the digital encryption system upon which the modern information and communication infrastructure depends. By breaking that encryption, quantum computing could jeopardize military communications, financial transactions, and the support system for the global economy. . . . The vulnerability presented by quantum computers will affect every government body, critical infrastructure, and industry sector.[2]

Experts also agree that this threat is unlike any the United States has ever encountered. Unlike traditional cyber threats, the quantum hack will be largely *undetectable* because covert quantum intrusion will appear legitimate and authorized—for as long as the intruder wishes to have access to data and networks.

It will be *instantaneous* since all public encryption systems will be instantly vulnerable through the same decryption process—unlike classical hackers who must rely on a series of trial-and-error attacks on one target at a time. Finally, it will be *ubiquitous* in that it can remain undetectable indefinitely, whether in the form of a continuous data breach or full-scale disruptive cyber-Armageddon, or anything in between. In addition, it will be able to read encrypted data that hackers are stealing today for decryption by a quantum computer tomorrow.

So, while quantum computer technology may take another decade to reach the level needed to carry out a large-scale attack, the quantum threat exists now thanks to data harvesting and advances in hybrid quantum computer systems that can already overtake RSA-based encryption. In short, quantum computers pose both conventional and unconventional defense challenges—challenges that are both imminent and potentially catastrophic to America's critical infrastructure, particularly its financial system.[3]

The White House and the Quantum Computer Threat

Therefore, it is imperative to develop plans and deploy solutions that will protect against quantum cyberattacks, including quantum-resistant cryptography and quantum-enabled cryptographic technologies, before the potential threat becomes a looming reality.

In January 2022, the White House acknowledged the reality of this threat by issuing NSM-8, the first memorandum from the White House national security apparatus to specifically mention quantum-resistant cryptography in the context of current feder-

al cybersecurity planning. The document specifically instructs the National Security Agency to release to chief information officers of governing agencies handling classified or sensitive information any relevant documents relating to "quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary."[4]

The document states:

> Within 180 days of the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA, where appropriate in accordance with section 1(b)(iv)(A) and (B) of this memorandum, and shall report to the National Manager, at a classification level not to exceed TOP SECRET//SI//NOFORN.[5]

Yet while the government is responding to protect its most valuable assets, it is not specifically addressing the threat to the private sector, especially the financial system.[6]

Quantum Alliance Initiative: Confronting the Quantum Computing Threat

Launched in 2018, the Quantum Alliance Initiative (QAI) was created "to develop and champion policies that allow the US and its allies to win the race to a universal quantum computer, while simultaneously working to ensure that both will be safe from a future quantum computer cyberattack within five years."[7]

We are now at that five-year mark. Since its founding, QAI and its 20 members from 10 countries have been successful in advancing policies that will keep the United States and its allies, particularly its Five Eyes intelligence partners, at the forefront of quantum research, from quantum computers and sensors to quantum and post-quantum cryptography. QAI has also helped ensure that the US and its allies are quantum-ready and quantum-safe.

Those efforts have included supporting the National Quantum Initiative, passed by Congress and signed by President Donald Trump in 2020; the series of national security memoranda (No 8–10) requiring US government agencies handling national security materials to prepare a timetable for being quantum-secure; and the Quantum Computing Cybersecurity Preparedness Act, sponsored by Congressman Ro Khanna (D-CA) and passed by Congress in 2022.

At the same time, however, QAI was also established to "develop a strong international quantum community that spans the quantum technology spectrum, from quantum computers and sensors to quantum and post-quantum cryptography."[8] For that reason, QAI includes members from 10 countries, including members from the Five Eyes intelligence community nations. We also created an international consortium of companies and labs to draw up the first-ever global standards of Quantum Random Number Generators (QRNGs) and Quantum Key Distribution (QKD), which were submitted to the International Telecommunications Union in Geneva, Switzerland, and which were approved in 2019–2020.

We also published a report, *Five Eyes on Quantum*, that included a strategic plan for incorporating quantum cooperation across the Five Eyes intelligence community and Japan.[9] Our quantum summit with Japanese and American scientists, including those from the Los Alamos and Lawrence Livermore national labs, held at Hudson Institute in January 2020, marked another step in the development of international cooperation in quantum information science between the US and its leading allies, particularly the Five Eyes countries.

Although QAI has been providing important thought leadership for all aspects of this crucial area of information technology for the twenty-first century—including the quantum interface with artificial intelligence, 5G, blockchain, autonomous systems, and other advanced technologies—our central focus has been and remains quantum security, including cooperation with the other Five Eyes intelligence countries.

To that end, in 2020 QAI partnered with Oxford Economics, one of the world's leading econometric firms, to generate a series of reports that provide detailed analysis of the economic impact of a future quantum computer attack on key US infrastructure, including the impact on domestic economic growth as well as the larger global economy. Since 2021, the Quantum Alliance Initiative at Hudson Institute has been generating a series of econometric studies on the quantitative cost of future quantum computer attacks. It has produced two reports:

- The first of these reports, *Risking Apocalypse? Quantum Computers and the US Power Grid*, was released in December 2021.[10] In *Risking Apocalypse?*, our research showed that in terms of revenue-at-risk, utility companies would lose over $50 billion due to a quantum computer attack. We also found that the direct GDP-at-risk exceeded $8.9 trillion in direct costs to the American economy.[11]

- The second, *Decrypting Crypto: Cryptocurrencies and the Quantum Computer Threat*, was published in April 2022.[12] In *Decrypting Crypto*, our study estimated that the overall cost of a major hack and devaluation of Bitcoin alone would equal $3 trillion in direct and indirect losses.[13]

This report is the third of this series utilizing the Oxford Economics Global Economic Model. It analyzes several scenarios involving a future quantum computer attack on the US financial system, specifically the Fedwire interbank payment system used for transferring funds within the Federal Reserve network, including its effects on the global financial system. After detailing the impact of a quantum computer intrusion into a crucial part of the US financial infrastructure, it also provides an overview of possible solutions and quantum cybersecurity protections.

As part of this series, we have conducted the following study of a future quantum computer attack on the US financial system, specifically on the existing Fedwire interbank payments system. The results of this study build on the preliminary econometric research our team conducted over the past three years and were initially reported in the May 2021 *Forbes* column "Getting the Big Banks to Confront the Quantum Challenge."[14]

Using basic calculations and extrapolated data and trends from two previous studies, we made rudimentary estimations of such a hypothetical quantum-enabled event while also considering the systemic risk specific to the financial sector.[15] Compared to a conventional cyber disruption in the US financial system, which on average would cost $581 billion, the effects of a quantum computer–enabled cyberattack would increase this average cost by 25 to 235 percent, according to our preliminary findings. Specifically, we initially estimated that a single-day cyberattack on one of the top five largest financial institutions in the US (by assets) that disrupts access to Fedwire would result in losses ranging from $726 billion to roughly $1.95 trillion on average.[16] Furthermore, we estimated that a quantum computer attack would impair over 60 percent of total assets in the banking system due to bank runs and endogenous liquidity traps.

While these numbers were daunting, they were far from precise. Furthermore, these figures do not consider the systemic effects of the attack on other sectors, firms, and even households in the broader economy. The purpose of this current study is to provide that additional precision in our calculations, including considering those aforementioned systemic effects.

All these reports and conferences, and efforts to educate Congress and the executive branch on the future threat of quantum computer decryption, has been aimed to fulfill QAI's mission to "promote public awareness as well as among government and corporate leaders, of the critical importance of quantum technology in the coming 'post-digital age'—including interface with artificial intelligence, 5G, blockchain, autonomous systems, and other advanced technologies."[17]

Cyberattacks, Quantum Computers, and the Financial System

Low-frequency, high-impact events—so-called black swans—represent a fundamental policy dilemma. Although their occurrence is inherently rare, such events often impose economic costs of a magnitude and extent that are fundamentally difficult to measure. Policymakers are left with limited information to influence decision-making in planning to mitigate innumerable consequences. Accordingly, planning for these events is often relegated as a low priority if not entirely forgotten. But as the COVID-19 pandemic has demonstrated, there is an existential necessity for sound mitigation and response policies in the face of black swan events. While responding to current crises is paramount, preparing for the *next* disruptive event is of equal, perhaps greater importance.

Due to the deep interconnectivity between public and private institutions and the inherent sensitivity of equity and credit markets, the financial network presents a prime target for a future quantum attack.

Even now, US leaders have long recognized that America's financial sector is dangerously vulnerable to traditional cyberattacks. Despite many warnings and hundreds of millions of dollars spent on cybersecurity, experts agree that America's financial sector remains dangerously vulnerable to traditional cyberattacks. A 2020 Boston Consulting Group report found that financial firms are 300 times more likely to come under cyberattack than other business firms.[18] Similarly, IBM Security identified the financial sector as the most-attacked industry in four of the last five years, accounting for 22 percent of all cyberattacks in 2021.[19]

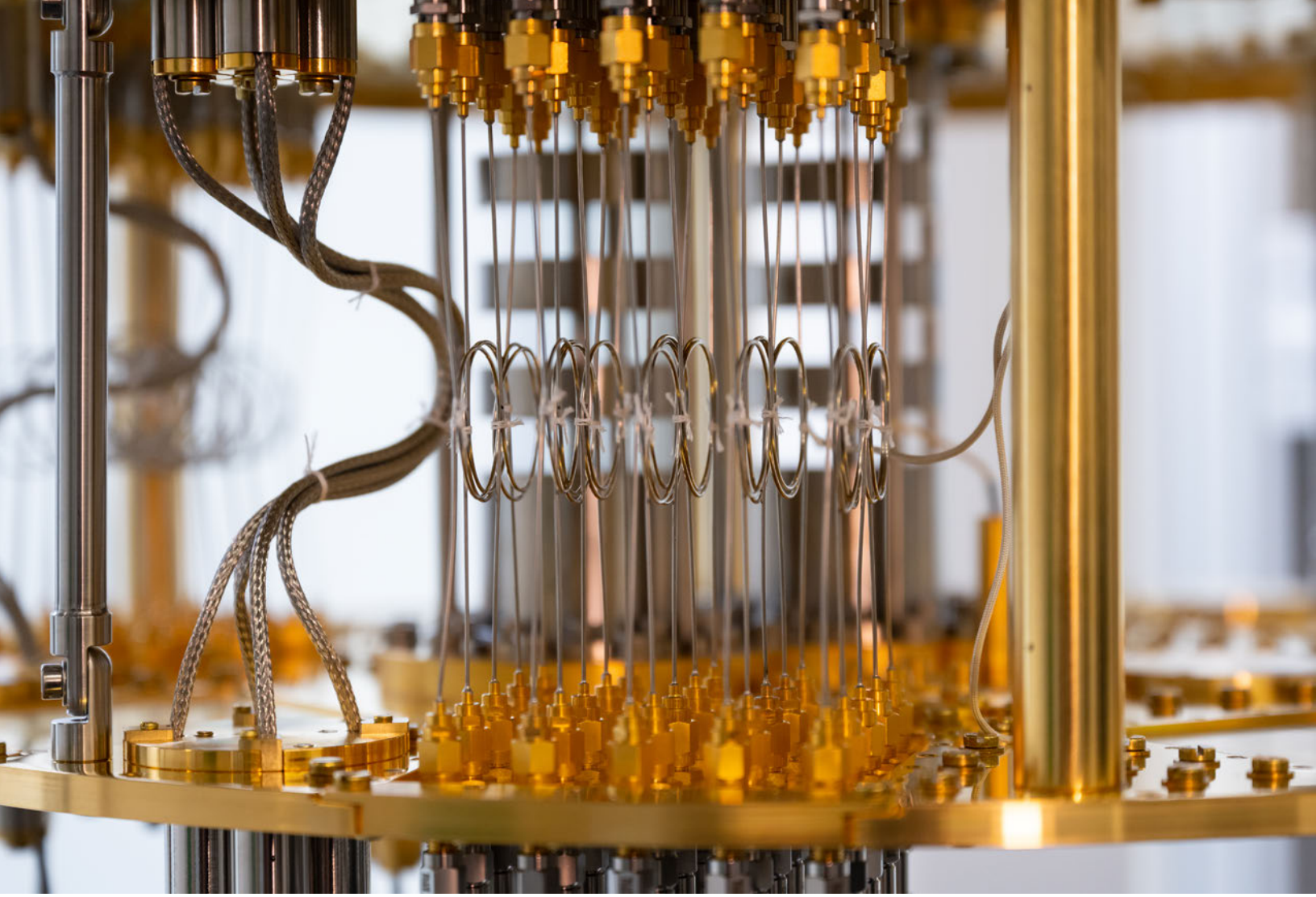
Even if America's financial sector could install sufficient protections against conventional cyberattacks, it will remain a valuable and vulnerable target for a quantum-powered cyberattack since these protections rely on public encryption regimes.

Once a quantum computer has covertly gained access to the network, any number of viruses or types of attacks could infiltrate and spread with incalculable speed through our fiscal sector. From a simple data breach or halt to trading of a single bank to fraudulent transactions that crash stock exchanges and alter overnight lending rates via the SWIFT Network, the attack could take many forms—all of which attackers will execute with apparent authenticity, leaving their infiltration undetected and hindering response and recovery.

For example, the New York Fed released a paper in January 2020 (revised May 2021) that demonstrated an attack on a single large bank could spread to nearly 40 percent of the US financial network.[20] The impact of a cascading quantum attack on major banks, the Federal Reserve, or stock exchanges and derivative exchanges would be even more calamitous for the US and the global economy. The potential catastrophic attack and financial collapse rise to levels that eclipse the 2008–09 crisis or the Great Depression.

As noted, the report by the Quantum Alliance Initiative on the impact of a quantum computer attack on cryptocurrencies found that an attack on Bitcoin alone would have a devastating impact on the larger economy. Our April 2022 quantitative analysis detailed how such an attack would result in direct losses to cryptocurrency investors of approximately $1.87 trillion and cost the broader US economy upward of $1.47 trillion in additional indirect impacts.[21] This is so despite the fact that cryptocurrencies, including Bitcoin, are still a relatively small part of the overall financial system.

In this policy report, we present comprehensive qualitative research and novel quantitative analysis to test the impact of quantum computer attacks on much larger and more vital aspects of this financial system. Building on some three years of research, and the initial calculations described briefly above, we consider the impact of quantum decryption on a single feature of the financial system, namely the Fedwire Funds Service. Utilizing various econometric methods, we implemented a two-staged economic analysis to more accurately quantify the total indirect economic impacts of a quantum computer cyberattack on the Fedwire interbank payment system.



2. WHAT IS A QUANTUM COMPUTER?

Key Takeaways:

- Quantum computers (QCs) are a subset of quantum information technologies that harness the unique properties of subatomic particles in their quantum-physical state for information processing and data calculation purposes.
- Properties of quantum mechanics allow QCs to reduce the difficulty of solving certain mathematical problems, allowing for exponentially faster cracking of the fundamentals of most of today's encryption standards.

Quantum computers (QCs) are a subset of quantum information technologies that harness the unique properties of subatomic particles in their quantum-physical state for information processing and data calculation purposes.

On the quantum scale, many properties—energy, position, momentum, spin—exist in a state that physicists describe using a probabilistic wave function. The much-touted Schrödinger equation describes the evolution of this wave function. Once we have measured a physical property, the associated wave function collapses, and a single numerical value can represent the measured property. The measurement of one property (i.e.,

Photo: A cryostat from a quantum computer stands during a press tour of the Leibniz Computing Center in Garching, Bavaria, on July 14, 2022. (Photo by Sven Hoppe/picture alliance via Getty Images)

position), can affect the measurement and the available information associated with other complementary properties (i.e., momentum).

The basis of digital computation is binary digits, or bits, consisting of zeros and ones. These values correspond to the potential energy difference within the transistors of an integrated circuit. Then logical gate operations in a central processing unit (CPU) manipulate these bits to carry out basic calculations. Scaling and compiling these bits and operations make everything digital computers do possible.

QCs process information with their own set of logic gate operations, but via a fundamentally novel approach. Instead of using transistors, they use quantum bits, or "qubits," as they are commonly known. Examples of qubits include the spin of an electron or the polarization of a physical photon rather than the electrical signal in classical computation. The spin of an electron or the intrinsic angular momentum of a particle can exist in "up" or "down" states (i.e., zero or one). Due to the quantum measurement property, quantum systems will yield a single state upon measurement. However, qubits can also exist in a state of superposition (i.e., a linear combination of zero and one) until measured. Before measurement, the state of qubits evolves with its underlying quantum mechanical state. Yet the system will collapse to an observable state once measured. The probabilistic wave function defines the probability of collapsing into either an "up" or "down" spin state.

Adding more qubits to the quantum computing process—a process termed *entanglement*—increases its computing power exponentially by linking, coupling, or correlating two or more quantum objects in a specific way such that the same quantum state subsumes them.[22] Scientists may correlate and link these particles even at great distances. Entanglement introduces new ways to shape information processing in quantum technology, in which future QCs will have the capacity to solve problems exponentially faster than today's most powerful supercomputers.[23] Accordingly, current classical supercomputers would require more bits than all of the atoms on Earth to simulate a 100-qubit QC, and more bits than the total number of atoms in the known universe to model a 280-qubit quantum machine.[24]

These quantum properties—along with constructive and destructive interference of the wave function—allow enhanced parallel processing of information, or quantum parallelism, that can reduce the number of steps in solving various problems.[25]

The great challenge for quantum computing is mapping problems onto qubit circuitry and physical computational architecture such that these computers can provide a practical computational advantage. There is no single path to making a QC. The essential question in the field concerns finding or creating suitable environments to generate the desired quantum mechanical effects. Subsequently, physicists and engineers have to address issues with scaling, performing logic gate operations, and conducting error correction and readout processes. The challenge will be finding innovative and efficient ways to exploit these elusive problems using the natural tendencies of quantum mechanical systems in practical applications.

One specific quantum application, Shor's algorithm, allows for exponentially faster cracking of integer factoring problems and discrete logarithm problems that are fundamental to most of today's encryption standards.[26] In general, public key encryption schemes employ a large, difficult mathematical problem to encrypt data. The computational intensity or intractability of these large problems provides security. Integer factoring is the basis of the RSA algorithms, a major public key (or asymmetric) encryption protocol that forms the primary cryptographic method for many financial systems and networks, including online banking and interbank payment transfers.[27] Shor's algorithm lays this RSA protocol bare by exponentially reducing the number of steps required to find the period (and thereby the integer factors). Integrating all the quantum processes—parallelism, interference, etc.—a future QC running Shor's algorithm will work

thousands of times faster than classical supercomputers to factorize these large prime numbers and crack RSA encryption.

Because Shor's algorithm can so effectively break these cryptographic standards down, it will soon expose many of our public key security protocols—the encryption layer over private key protocols like AES. Additionally, some quantum speedups may be polynomial, not exponential. Take, for example, Grover's search algorithm.[28] Originally developed to search databases, Grover's algorithm is highly effective in combing unstructured data to find the input associated with some output. Its successful implementation on a future QC can lead to a quadratic speedup in information processes (it takes steps to perform a search). Equally, Grover's search algorithm can solve cryptographic problems that would take a classical supercomputer 1 million computational steps in only 1,000 steps on a future QC.[29] Grover's search introduces novel forms of preimage attacks and collision attacks of hash functions.

Therefore, hackers can harness Grover's search for decryption purposes as well, potentially to unravel certain symmetric key protocols, including those that underpin the primary interbank payment network in the US—the Federal Reserve's Fedwire Funds Service. Thus, much of what underpins cybersecurity infrastructure is vulnerable to a future quantum-enabled cyberattack. Utilizing quantum-physical properties, QCs employing algorithms such as Shor's or Grover's will be able to hack previously impenetrable digital financial networks and systems in a matter of minutes.

Although there are classical methods of securing RSA and AES encryption today, such as by using longer keys, these augmented encryption standards will not be immune to the accelerating pace of advances in quantum computing. As of 2021, over 87 known projects worldwide aimed to build quantum computing systems using a myriad of different core technologies.[30] Consequently, new decryption schemes and algorithmic optimizations continue to emerge as research in the quantum information science field increases. Thus, "even if one does not plan to use quantum computation, one must be knowledgeable about it because of its ability to break current public-key cryptographic standards" and the threat posed by potential quantum-enhanced classical or hybrid cyberattacks, such as harvest-now-decrypt-later intrusions.[31]

3. APPLICATIONS OF QUANTUM COMPUTERS IN FINANCE

Key Takeaways:

- In the case of modeling and simulations, QCs could accelerate analysis, specifically with Monte-Carlo Integration (MCI), which is already critical to finance for its applications to risk and pricing predictions, driving market forecast predictions and risk analysis.
- QCs will be able to solve optimization problems more efficiently, helping to determine the best allocative investment strategy for portfolios, formulate hedging strategies, and outline lucrative arbitrage opportunities for investors without impractical time lags.
- Quantum computing promises to boost the development of artificial intelligence and machine learning algorithms, which are already revolutionizing anomaly detection within the financial and banking sectors.

Due to the inherent properties of QCs and the accompanying potential for quadratic or exponential speedups in computational ability over that of classical devices, there is vast potential for quantum technology to enhance processes that are otherwise inaccurate, time-consuming, or both—even in the near term with noisy intermediate-scale quantum (NISQ) devices. This is especially true for financial problems and analyses, which like physics and chemistry rely heavily on stochastic

Photo: (Getty Images)

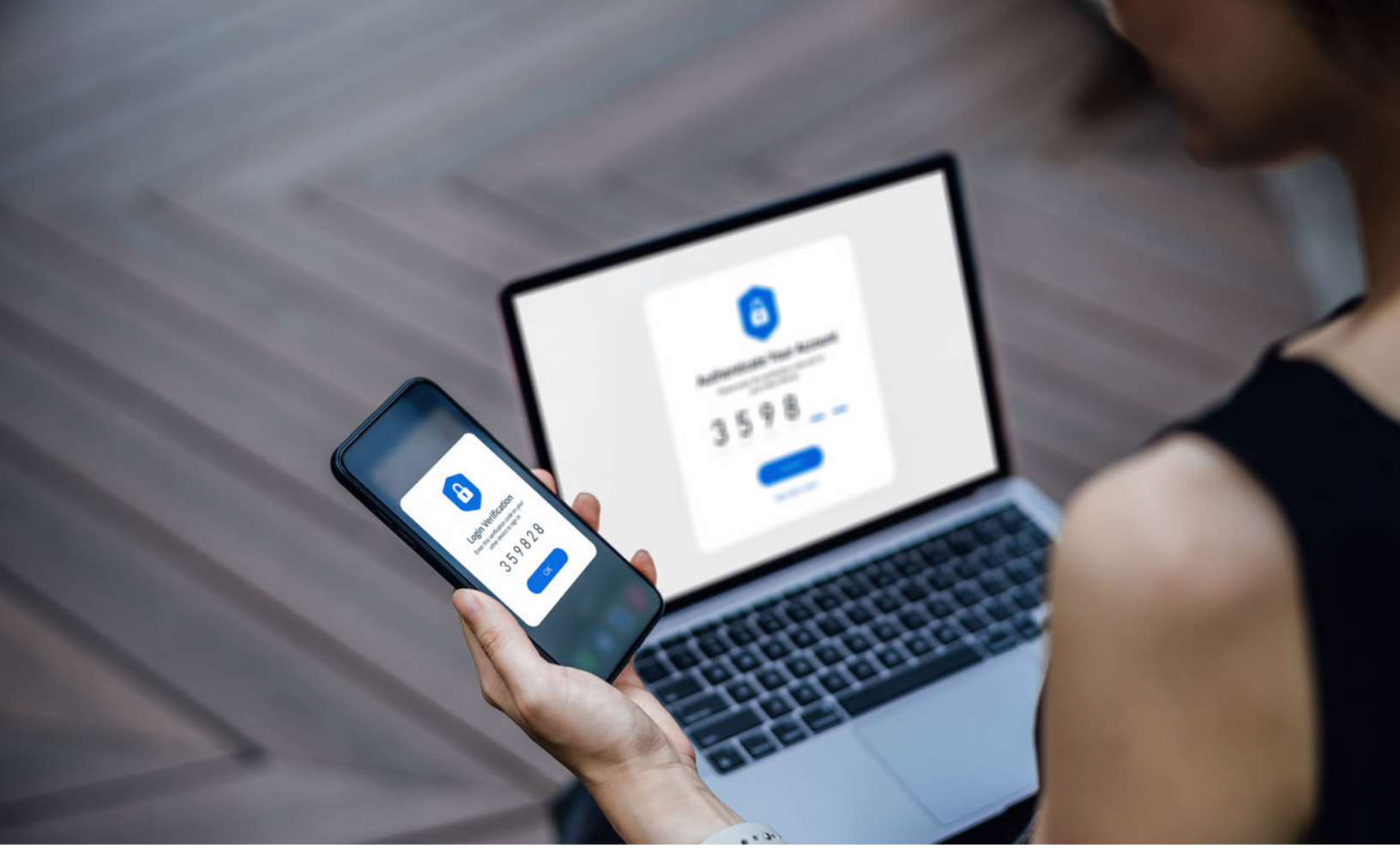
variables as inputs into their models and equations. With use cases ranging from risk modeling and market simulations to optimization problems and machine learning applications, the financial sector is poised to become an early adopter of quantum computing. Furthermore, the ability of quantum devices to overcome and even accelerate analysis in the presence of approximations offers exceptional benefits to financial analysis, where certainty in market conditions, and therefore modeling parameters, is often elusive. Pairing quantum computing with the industry's access to capital and long track record of incorporating technological innovations into its operations puts the financial sector on pace to become a critical first-mover in the adoption of quantum computing.

The benefits of quantum computing are especially promising for the financial sector in three core areas: modeling and simulations, optimization, and machine learning. In the case of modeling and simulations, which drive market forecast predictions and risk analysis in the industry, quantum computing may offer up to a quadratic speedup over classical analysis, specifically with the computationally intensive form of Monte-Carlo Integration (MCI). Already critical to finance for its applications to risk and pricing predictions, MCI utilizes stochastic variable sampling to approximate solutions that are intractable with traditional analysis or classical numerical methods due to their sensitivity to poor scaling with high dimensional problems.[32] Quantum-enabled MCI promises to deliver this simulation and modeling capability almost in real-time and without the need to over-simplify modeling assumptions to estimate an unknown financial quantity, such as options and collateralized debt obligations derivative assets, which computers analyze as the function of nondeterministic input variables.[33]

Optimization problems are another key area in financial analysis, and are likely the most promising and commercially relevant applications on near-term quantum devices. Analysts use them to numerically determine the best allocative investment strategy for portfolios, formulate hedging strategies, and outline lucrative arbitrage opportunities for investors. Experts believe that near-term QCs will be able to solve these problems more efficiently than classical machines, which often create impractical time lags that limit the practicality of optimization analysis in the field.[34]

Finally, quantum computing promises to boost the development of artificial intelligence and machine learning algorithms, which are already revolutionizing anomaly detection within the financial and banking sectors. Despite this, classical machine learning approaches to fraud detection not only are computationally and temporally restrictive but also incorrectly flag legitimate transactions as fraudulent up to 80 percent of the time.[35] In addition to improving the computational efficiency of this data-intensive task, quantum computing will increase the practical accuracy of machine learning for the industry.

Although central to modern financial analysis, these applications—modeling, optimization, and machine learning—require vast amounts of computational power to achieve the necessary precision for their solutions. This gap between analytical demand and computational ability makes the adaptation of QCs, even in the near term, an appealing undertaking. Moreover, the combination of these three near-term applications of quantum computing will transform modeling and predicting financial crashes and economic downturns from an imprecise art to a more robust scientific analytical practice.



4. SYSTEMIC CYBER RISK TO THE FINANCIAL SYSTEM

Key Takeaways:

- In the post-COVID-19 work-from-home environment, more firms have adopted remote network access regimes, effectively broadening the attack surface and increasing the points of entry for a successful cyberattack.
- Network contagion, where impacts on a firm spread throughout its network—either digital, physical, or both—propagates significantly in the financial sector, and especially in a cyber-enabled financial network.
- Financial institutions are particularly exposed to this kind of cyber risk due to their reliance on critical infrastructures and their dependence on highly centralized and interconnected banking and payment networks.

The threat of quantum-enabled cyberattacks will overshadow the many benefits that quantum computing is poised to bring to the financial sector. Specifically, the risk of future quantum decryption may outweigh any gains in computational efficiency and accuracy for finance. Even in a world recovering from COVID-19, cyber risk remains an elevated threat. In the post-COVID-19 work-from-home environment, the threat of malicious cyber incidents has risen as more firms have adopted remote network access regimes, effectively broadening the attack surface and increasing the points of entry for a successful cyberattack.[36] Now more than ever, cyber threats, especially in the future quantum-enabled era to come, pose a critical risk to

Photo: (Getty Images)

our national, economic, and even societal security—especially within the financial sector.

According to Nicolaus Bernoulli's expected utility theory, risk is the product of the probability of a given outcome and its consequences.[37] In 2018 the Financial Stability Board expanded this definition by applying economic theory to cyber risk.[38] In this regard, we may define cyber risk as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems."[39] Reports such as the World Economic Forum's annual Global Risks Report make the rise and primacy of cyber risks evident. It includes the "failure of cybersecurity measures" in its top ten global risks, in terms of both potential impact and likelihood, over the next five years. Notably, the 2022 WEF report highlights the risk of QC-enabled cyber threats and quantum decryption, "which poses a significant security risk because of . . . the financial . . . data protected by these [encryption] keys."[40] Cyber risk is not only an operational concern but also a financial one. Simply put, cyberattacks pose an often incalculable risk to affected firms and organizations.

Nonetheless, a growing field within economics attempts not only to study cyber risk but also to quantify it. Utilizing a Pareto model to both analyze the likelihood and quantify the impact of a significant data breach within the next half-decade, along a similar timeline to that laid out in the WEF report, Kwangmin Jung estimates the probable maximum financial cost of such an extreme data breach event at well over half a billion dollars.[41] Central to the study of cyber risk, and consequently the enumeration of its impacts, are the cascading effects that manifest particularly within the interdependent cyber network. Although not unique to cyber risk, this network contagion, where impacts spread from one firm and reverberate throughout its network—either digital, physical, or both—propagates significantly in the financial sector and especially in a cyber-enabled financial network. In 2018 the Financial Stability Board defined contagion as distress that a single financial institution or sector experiences and transmits to other institutions or sectors due to direct exposures between them, or as commonalities that lead to a general loss of confidence in those institutions or sectors.[42]

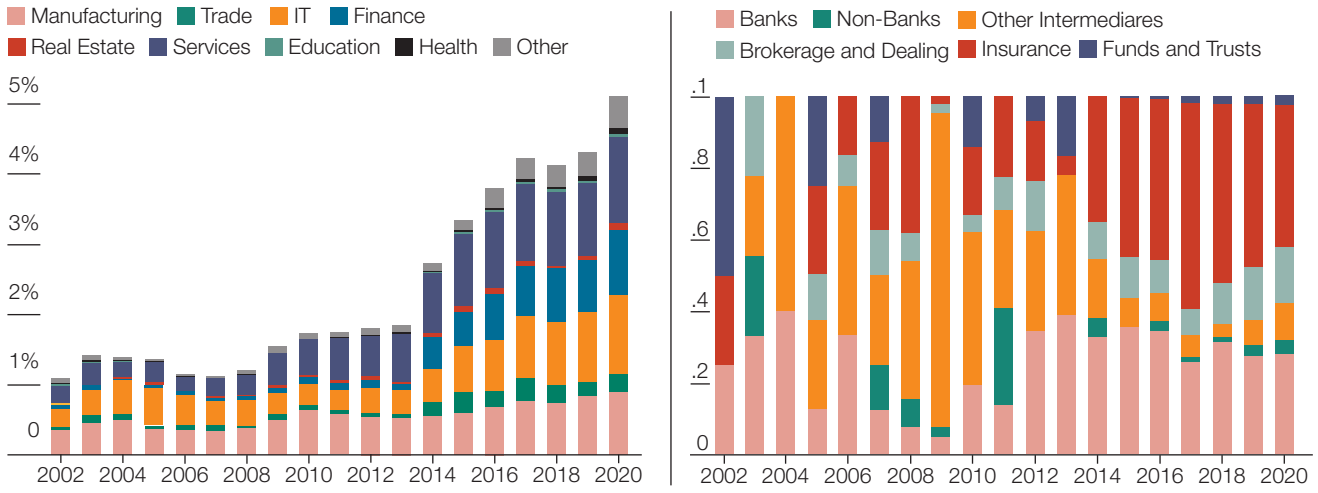
Figure 1: Stock Price of Affected Firms after the 2017 NotPetya Cyberattack

Note: Figure shows the seven days before and after news of the attack was released, with a dashed line indicating the release date.

Source: Matteo Crosignani, Marco Macchiavelli, and André F. Silva, *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains*, Staff Reports No. 937 (New York: Federal Reserve Bank of New York, 2021), https://www.newyorkfed.org/research/staff_reports/sr937, 9.

Demonstrating the significance of network contagion and the scaling factor of indirect costs associated with systemic cyber risk, the econometric analysis by Matteo Crosignani et al. found that the damages to firms that the 2017 NotPetya cyber incident directly attacked or impacted amounted to just under $2 billion.[43] However, when analyzing the indirect costs that interconnected firms incurred, their analysis suggests network contagion from the attack resulted in a fourfold amplification of the direct costs, with indirect costs of the NotPetya cyberattack amounting to over $7 billion in lost profits and other damages. In addition to initial direct costs, Crosignani et al. document the

Figure 2: Decomposition of Global Cyber Risk by Major Industry (left, percentage of calls discussing cyber risk) and Within the Finance Sector (right, finance industries defined based on 4-code NAICS classification)



Source: Adapted from Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk" (working paper no. 28906, National Bureau of Economic Research, Cambridge, MA, June 2021), https://www.nber.org/papers/w28906, 51–52.

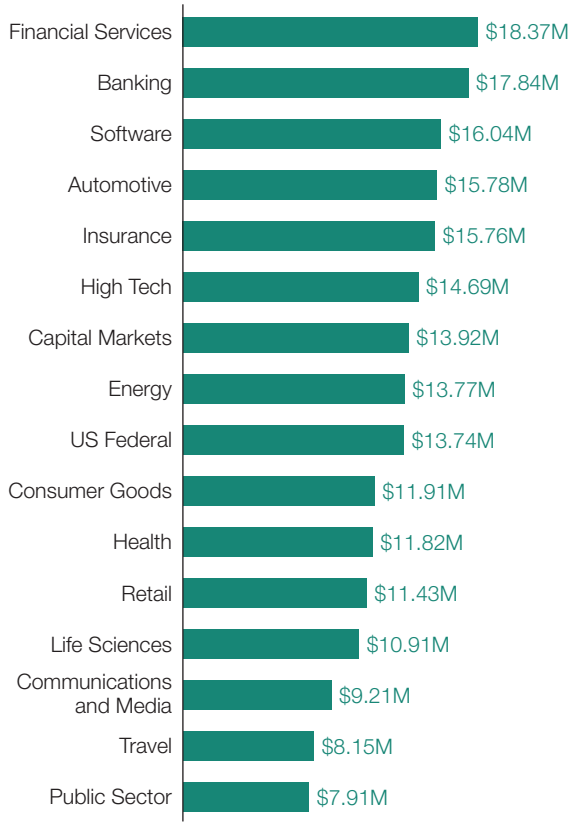
resulting 5 percent collapse in the stock price of firms directly hit by the NotPetya cyberattack (see figure 1).[44] Consequently, whether or not it directly affects a firm's real-world supply or customer network, cyber risk guarantees that the impacts of a digital cyber threat will spread like wildfire throughout the vast cyber and physical networks that uphold our modern economy.

Financial institutions are particularly exposed to this level of cyber risk due to their reliance on critical infrastructures and their dependence on highly interconnected banking and payment networks.[45] Central banks have been the targets of malicious cyber intrusions, including data breaches at the Cleveland, New York, and St. Louis Federal Reserve Banks in 2010, 2012, and 2013 respectively.[46] Although accustomed to risk, the financial industry has become one of the most cyber-exposed economic sectors over the past decade. One-fifth of all global cyber risk exposure envelops the finance industry, and financial intermediaries account for nearly half of the industry's exposure.[47] Particularly exposed within this subsector are large banks with high liquidity ratios, making depository institutions at the center of the financial network lucrative and opportune targets for adversarial cyber actors, as depicted in figure 2.

In addition to being heavily targeted, the financial sector incurs the heaviest costs from cyber risk on average. Accounting for the two highest costs incurred from cyberattacks per organization, the financial services industry and the banking industry face $18.37 and $17.84 million respectively each year, as figure 3 details.[48] Therefore, the financial sector faces a dual-edged threat from cyber risk: traditional economic and financial network risks, and cyber-induced risk to the infrastructures that enable those connections.

Jan-Philipp Brauchle et al. define financial stability as "a state in which the key macroeconomic functions, that is, the allocation of financial resources and risks as well as the settlement

Figure 3: Annual Estimated Average Cost of Cyberattacks to Major Firms by Industry



Source: Adapted from Francisco Luque, José Herrera, José Munera López, and Paul Williams, "Cyber Risk as a Threat to Financial Stability," *Revista de Estabilidad Financiera* (Banco de España), no. 40 (Spring 2021), 185.

---

of payment transactions, are performed efficiently—particularly during unforeseen events, stress situations, and periods of structural adjustment."[49] Synthesizing this concept with the definition of cyber risk mentioned above, we may define financial cyber risk as operational risks to information and technology assets within the financial sector that have consequences affecting the confidentiality, availability, or integrity of information or information systems critical to the efficient allocation of financial resources and risks in the settlement of payment transactions across the financial network, which in turn transmits a general loss of confidence outward and threatens the key macroeconomic functioning of the industry as a whole.

Therefore, this dual threat can weigh heavily on firms and organizations within the financial sector and, given the sector's high degree of interconnectivity, can weigh down the financial network's web to a degree that threatens overall financial stability. Furthermore, as the financial sector is systemically vital to the functioning of the economy, this risk may threaten the overall health of our national economy. Emanuel Kopp et al. provide a seminal analysis of cyber risk as a threat to financial stability and thus a textbook source of financial contagion and systemic risk for an economy:

> Idiosyncratic cyber shocks can trigger funding liquidity risks, which can then morph into market liquidity shocks as firms are forced to shed assets, pulling down asset prices. It may also be the case that concerns over the integrity of counterparties leads firms to stop interacting with certain market participants, exacerbating pressures on the market-based recycling of liquidity. Materializing liquidity and market risk shocks can ultimately lead to solvency problems in financial institutions. Close direct connections through interbank and transfer markets, and indirect relationships (liquidity cascades) allow shocks to spread quickly throughout the system. An institution's inability to meet payment or settlement obligations—for example because their internal record-keeping or payments systems have been compromised—can cause a name crisis, which would have adverse effects on funding liquidity and knock-on effects to other institutions which were counting on the availability of these liquidity flows. Liquidity shortages can lead to fire-sales which then feed into asset valuations and

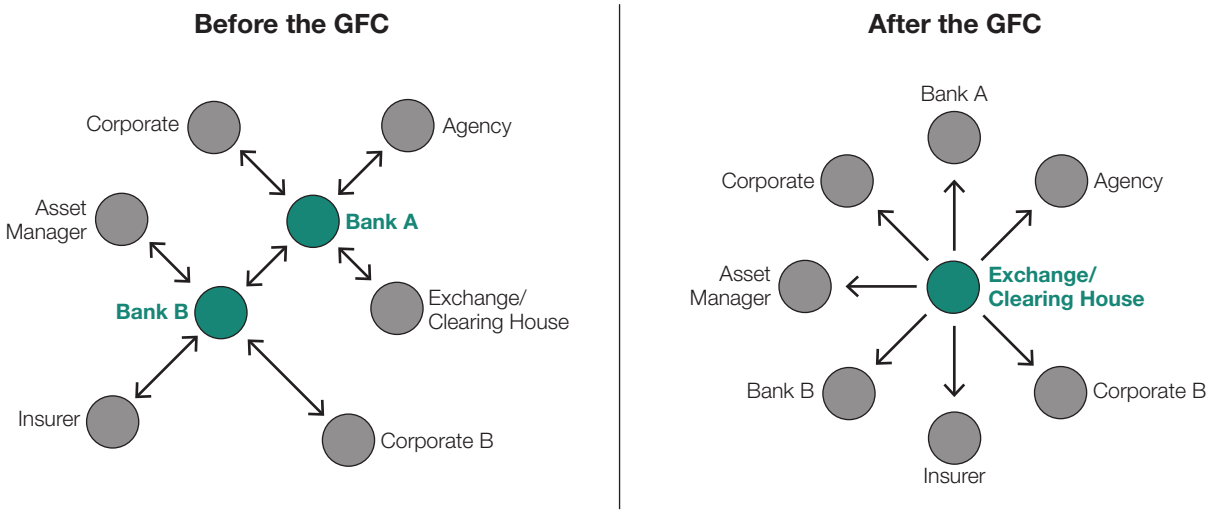
> spread to all kinds of market participants that are invested in or are trading a particular asset or asset class. Over time, liquidity risk-induced losses eat into firms capital and end up weakening financial institutions' solvency positions.[50]

In this manner, a single cyber incident against the financial system—or even a single actor in the financial system—can not only seize up liquidity in the network but grind the entire network to a halt, catapulting banks into the red and sending asset prices in connected markets into freefall. This cascading failure or contagion within the financial market is as much a feature of the network structure as it is a source of risk. The financial system is an inherently complex system-of-systems "made up of individual layers that have evolved collectively over time, and that have become more complex and complicated in equal measure."[51] Accordingly, this complexity introduces an asymmetry between cyber adversaries and cybersecurity actors that benefits attackers and makes the eventual success of a financial system cyberattack inevitable. Furthermore, the 2020 report for the European Union's European Systemic Risk Board by Greg Ros details how the inherent complexity of the financial system leads to the procyclicality of systemic risks over the span of its institutional evolution, similar to the paradox of deterrence in traditional analyses of defense economics:

> If the future state of a system is in part based on its past states, adverse feedback loops could feed a progressive build-up of fragility and aggregate risks. These risks are not directly attributable to the activities of a single institution, but derive instead from collective behaviour, which leads to an amplification of volatility in the financial sector and in the real economy.[52]

Following the Great Financial Crisis of 2008, regulators in the United States moved to consolidate the interbank payment

Figure 4: Restructuring of Financial Ecosystem to a Centralized Network after the Great Financial Crisis



Source: Adapted from Vedral, Bobby, "The Vulnerability of the Financial System to a Systemic Cyberattack," in *Going Viral: 13th International Conference on Cyber Conflict*, edited by T. Jančárková, L. Lindström, G. Visky, and P. Zotz (Tallinn, Estonia: NATO CCDCOE Publications, 2021), https://ccdcoe.org/uploads/2021/05/CyCon_2021_Vedral.pdf, 105.

ecosystem from a complex and overlapping web of bespoke contracts to one revolving around a central FMI network. Although this has been effective in facilitating regulatory oversight, from a cybersecurity perspective it has created a single point of failure with no clear substitutes in case of disruption or cyber incursion, as shown in figure 4.[53] Consequently, regulators have consolidated the digital infrastructure of the financial sector, whereas they have left the physical economic linkages between industry actors convoluted. The result is akin to a single doorway into an ammunition depot: once an adversary is inside, any spark can set off the entire tinder box.

Business disruptions are more likely to introduce network contagion effects than incidents of cyber-borne fraud.[54] In their 2020 report, Brauchle et al. also highlight how cyber risks exhibit certain characteristics and propagate differently than conventional economic risks within the financial network. Because their effects are nonlinear, a cyberattack against a critical FMI can rapidly transmit solvency and liquidity stress to a multitude of recipients simultaneously, including those outside of the attacked institution's immediate financial network, potentially destabilizing the whole financial system. One such characteristic unique to financial cyber risk is that whereas a single successful attack impacting just one systematically important financial agent can evolve into a direct threat to the entire financial system, the same is true for an orchestrated attack on a critical mass of nonessential or non-systemically important institutions. One analysis found that a 1-unit increase in the number of directly impacted firms for a given cyber event statistically correlates to an increase in expected costs of 2.6 percent due to the event.[55] This relationship between costs and the number of targeted banks is of a larger degree than that between firm size alone and direct costs, demonstrating the potential magnitude increase in impacts due to contagion spillovers in simultaneous or multi-firm cyberattacks. Consequently, a business disruption of an FMI or a set of large financial institutions could have a drastic impact due to risk concentration in the network and the lack of substitutes in the case of FMIs.

This fact holds true not only from the cyber network perspective but also considering the financial ties that uphold that network. Regardless of how many FMIs or other agents a single cyber incident directly impacts, the necessity of free-flowing liquidity within the financial system ensures that liquidity and solvency issues reverberate throughout the network, especially if it affects a payment system. The 2020 European Systemic Risk Board report highlights the increased vulnerability of market participants to second-round financial defaults when an attack does not immediately target them, noting that when "the failure of a single institution triggers contagious defaults, the high number of financial linkages also increases the potential for contagion to spread more widely."[56] In the same manner, it concludes:

> If the interbank market is experiencing distress and shrinks, banks short of liquidity may be unable to borrow all the money they need from the market, and may be forced to sell their illiquid assets. In the presence of fire sales, market demand for illiquid assets becomes inelastic, depressing the market prices of these assets and resulting in effective losses for banks. These fire sales spillovers create an incentive to hoard liquidity, which can in turn induce another wave of sales, activating a liquidity spiral that could cause the interbank market to freeze completely.[57]

Cyberattacks have the potential to affect even the core elements of the global financial system and, given the broad interconnectedness of these systems, may have implications for financial stability at large. Although some have attempted to address this emerging and evolving risk, they have based their actions on a traditional and antiquated paradigm that assumes that all interbank payment systems are a closed system and that all security relies solely on trust among its participants and operators. The maintenance of a sufficiently high level of trust—both within market participants and by the population at large—serves as a crucial guard against instability within the economic and finan-

cial system. Market liquidity, for example, relies critically on the systemic trust in the security and reliability of RTGS systems and other key FMIs. Moreover, there exists an intrinsic and inverse relationship between uncertainty and confidence or trust within the financial system and the interbank payment system especially. Exploring this link, the report notes that uncertainty surrounding "the circumstances which caused the disruption, the actual effect of the disruption, or the possibility of containing or minimising the impact" can quickly diminish or destroy the systemic trust.[58] Current security architecture reflects the structural "trust paradigm" that the participants share; as a consequence, once they are "in" the network system, participants assume there is no need to verify or closely monitor messages or transactions between them.[59]

Moreover, the timing of a cyber disruption can have sweeping implications for both the intensity of the initial shock to a given FMI or financial institution and the trajectory of effects as the shock propagates throughout the financial system. If disruption affects a systemically important FMI or other core financial node during critical periods—such as near the end of the day—or during periods of increased transactions and payment traffic, a relatively small shock can undergo significant amplification as it reverberates through the financial network.

Beyond the timing, the duration of a shock is also critical: "any disruption of financial market infrastructure that lasts more than two hours and/or prevents settlement by the end of the day could arguably be considered systemically important."[60] In addition to the implications of when a cyberattack occurs, timing has further implications in systemic cyber risk, especially in the financial system, where there exists a positive correlation between the length of time required to detect a data breach and the financial impacts. According to the 2018 Cost of a Data Breach Study, a joint effort by IBM and Ponemon Institute, the mean time to identify a successful cyber incursion was 163 days in the financial sector, and the average detection time increased markedly for deliberate malicious data breaches.[61] This delay has significant implications for a scenario in which an adversary is strategically planning a cyberattack to inflict maximum impacts, especially in the quantum-enabled case, when an attacker may covertly (or seemingly legitimately) access an FMI network and lurk or conduct harvest-now-decrypt-later incursions.

The financial sector provides services to other critical sectors via the payment systems. Therefore, a successful cyberattack against crucial FMIs or payment services, particularly interbank payment systems such as Fedwire, can adversely impact the wider economy. Similar to a classic defensive paradigm, there is an information asymmetry in cybersecurity that gives adversarial actors the advantage. Furthermore, the network dynamics of the financial sector, both in terms of a centralized network design and convoluted economic ties between agents, ensure that any disruption will have drastic impacts on market prices and the general flow of liquidity. Likewise, these factors promote, or at very least facilitate, a general lack of clarity and information sharing, making threat detection and response coordination cumbersome—again, to the advantage of an intruder:

> Cybersecurity is a matter of the ecosystem of each financial institution, and simultaneously, the whole financial sector . . . thus cybersecurity requires a shared responsibility and common endeavor on the part of important stakeholders which amplifies the risk of coordination failures.[62]

Therefore, financial institutions should be aware that attackers can overcome their countermeasures, even strong defenses, and therefore they cannot consider these defenses fully trustworthy. As an assessment for the Bank of Spain stated, "cyber incidents may have a high degree of inevitability. In fact, cyber incidents have the potential to impair the operational capabilities of financial institutions to a point that compromises their viability."[63]

5. WHAT IS FEDWIRE?

Key Takeaways:

- Real-time-gross-settlement (RTGS) systems allow for instant and irrevocable settlement of individual transactions between banks on a case-by-case basis. Due to the velocity and volume of interbank payments, RTGS systems serve as the interstate system for liquidity in the financial system.
- The largest and most broadly employed RTGS system in the United States is the Federal Reserve's Fedwire Funds Service, or Fedwire. In 2020 the aggregate value of Fedwire transfers was roughly 40-fold greater than US GDP.
- There is a positive relationship between growth in Fedwire transaction value and GDP growth, which is econometrically estimated below. As the financial sector's contributing share to US GDP has grown significantly over recent decades, there may be a stronger dependency between Fedwire and GDP growth in the future.

While there are numerous attack vectors for a quantum-enabled adversary to exploit, and a variety of points of failure within the vast financial system, a growing emphasis has been placed on the threat of a breakdown in the interbank payment system, specifically real-time-gross-settlement systems. RTGS systems are an approach to the logistically challenging issue of interbank payments across the sprawling network of institutions in the financial system. These critical FMIs allow instant and irrevoca-

Photo: A screen displays market activity at the New York Stock Exchange on March 3, 2023, in New York City. (Photo by Fatih Aktas/Anadolu Agency via Getty Images)

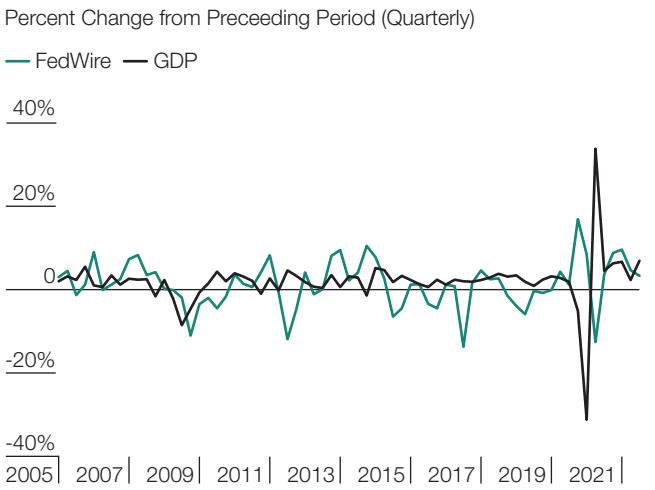
ble settlement of individual transactions between banks on a case-by-case basis.[64] Due to the velocity and volume of interbank payments, RTGS systems serve as the interstate system for liquidity in the financial system. As previous studies of both systemic risk and cyber-specific risk have outlined, a disruption to an RTGS system threatens to not only disrupt the banking system but also dislodge trillions of dollars of liquidity throughout the financial system.

Although countries use a variety of RTGS systems globally, the largest and most broadly employed system in the United States is the Federal Reserve's Fedwire Funds Service, or simply Fedwire. Introduced in 1918 as a limited network of telegraphic lines connecting the various Federal Reserve banks, Fedwire has grown to become the leading RTGS system by total value of aggregate payments worldwide. Consequently, it is a central source of financial activity and productive capacity in the US economy. Indeed, in 2020 the aggregate value of Fedwire transfers was roughly fortyfold greater than US GDP.[65]

While the link between the value of Fedwire transfers and aggregate US economic activity is not well established, extensive research has examined the link between financial sector activity and GDP, especially as the financial sector's overall contribution toward economic growth has grown over the past half-century and currently stands at roughly one-fifth of overall GDP.[66] Naturally, we may assume that the increase in the value of payments in the Fedwire system, which services and facilitates the entire financial sector, would positively impact the growth rate of GDP in the United States. Indeed, their growth rates exhibit similar, if not parallel, patterns.

As figure 5 shows, the patterns of growth between US GDP and Fedwire transaction value seem to mirror one another, with Fedwire transactions perhaps a leading indicator of GDP growth cycles. Anton Badev et al. also observe this phenomenon through their econometric analysis of the Fedwire-GDP relationship. Utilizing private Federal Reserve Fedwire transaction data, they found a positive and statistically significant relationship between the growth of daily Fedwire transaction value and the growth of domestic GDP with a single-year lag. More specifically, they found that daily growth in Fedwire value has a correlation coefficient of 0.77, indicating that a single-unit increase in the growth rate of daily Fedwire value leads to a 0.77-unit increase in the growth rate of domestic output the following year. However, they note that this dependent relationship is only indirect as the Fedwire transaction value reflects activity only in the financial sector rather than in the entire aggregate economy. Nonetheless, as we noted earlier, the financial sector's contributing share to US GDP has grown significantly over recent decades, potentially indicating a stronger dependency between Fedwire and GDP growth.

Figure 5: Relationship between Growth Rates of Fedwire Transaction Values and US Gross Domestic Product



Source: Based on data from the Federal Reserve and US Bureau of Economic Analysis.

Building on the results from Badev et al., we analyzed this relationship using the publicly available, albeit less granular, time-series data on quarterly growth of Fedwire transaction value. To account for this difference in the data, and improving on previous studies, we analyzed our Fedwire data against

Table 1*:* Granger-Causality Relationship between Fedwire Transaction Values and US GDP Growth

VAR GRANGER CAUSALITY RESULTS VARIABLES IN QUARTERLY GROWTH RATES (2004Q2-2021Q4)			
EQUATION	P-VALUE	F-TEST RESULT	INTERPRETATION
FedWire does not Granger-cause GDP	0.0002	Reject	Quarterly growth in FedWire transaction value does Granger-cause GDP growth
GDP does not Granger-cause Fedwire	0.1796	Do not reject	GDP growth does not Granger-cause groeth in FedWire transaction value.

Table 2: OLS Regression Estimation Results: Relationship between Fedwire Transaction Value and US GDP Growth

DEPENDENT VARIABLE: GROWTH IN FEDWIRE TRANSACTIONS VALUE, PERCENT CAHNGE (QUARTERLY, 2005Q2-2021Q4)					
VARIABLE	LAGS	COEFFICIENT	SIGNIFICANCE	R-SQUARE (ADJ. R-SQUARE)	DW STAT
GDP Chained Quantity Index Growth, Percent Change	1 Quarter	0.3888843	***	0.2115 (0.1856)	1.81413
	2 Quarters	0.2318302	**		

Source: Based on data from the Federal Reserve and US Bureau of Economic Analysis.

Note: *** and ** denote significance at 1 percent and 5 percent levels respectively; variable lags selected via SBIC criteria; DW Stat corresponds to the regression output's Durbin-Watson test statistic.

quarterly (instead of annual) growth in aggregate output. Jointly, our time-series analysis covers the period beginning in the third quarter of 2005 and ending in the final quarter of 2021, due to data availability. Our analysis began with a test for statistical, or Granger, causality, which tests for the predictive causality between two data sets. We found that growth in quarterly Fedwire transaction value does indeed Granger-cause, or lead, quarterly growth in US GDP during the period examined.[67]

Having established the direction of precedence between Fedwire and aggregate output, we performed a simple univariate regression to quantify this relationship. Our findings, as reported in table 2, indicate that the relationship between quarterly growth in Fedwire transaction value and US GDP is both positive and statistically significant: a 1-unit increase in the growth rate of Fedwire transaction value leads to a 0.39-unit increase in quarterly GDP growth a quarter later, and an additional increase of 0.23 units the following quarter, all else equal.

While these figures seem insignificant at a glance, it is important to remember the historical fluctuations in GDP growth cycles, which normally run around 3 percent growth in a given quarter. Therefore, our findings indicating that a single percentage point increase in the quarterly growth rate of Fedwire transaction value leads to a 0.39 percentage point increase in quarterly GDP growth in the following quarter (and a further increase of 0.23 percentage points in GDP after two quarters) not only affirms the findings of Badev et al. but also establishes the statistical importance of the financial sector in the overall economy. Furthermore, our results reflect the pronounced role of Fedwire as the lifeblood of both the financial system and the US economy at large.

This vast Fedwire system, which services well over 5,000 accounts with balances (as of 2020), is consolidated into a single network that the Federal Reserve Board of Governors operates and secures.[68] Aptly named FEDNET, this payments network is secured by common proprietary encryption protocols based on National Institute of Standards & Technology (NIST) encryption guidelines for the federal government, or the Federal Information Processing Standards (FIPS). According to the Federal Reserve Banks' Certification Practice Statement on Public Key Infrastructure (PKI), as of June 2021 digital encryption key pair generation "must meet or exceed FIPS 140 Security Level 2 (or the equivalent)."[69] Thus, although encouraged to meet the 2022 encryption security standards for the Advanced Encryption Standard (AES) as recommended by NIST in FIPS 197, the Federal Reserve and Fedwire are only required to maintain digital keys that are Data Encryption Standard (DES) compliant. It is important to note that the DES standard, as recommended under FIPS 140-2, was originally released in 2002 and is noteably exposed to quantum decryption, if not classical decryption as well.[70] Further safeguards—including dual-factor authentication, monthly passcode changes, and a physical USB security token—protect account holders and transactions on the network. "Multiple out-of-region backup data centers and redundant out-of-region staffs for the data centers" ensure further security.[71]

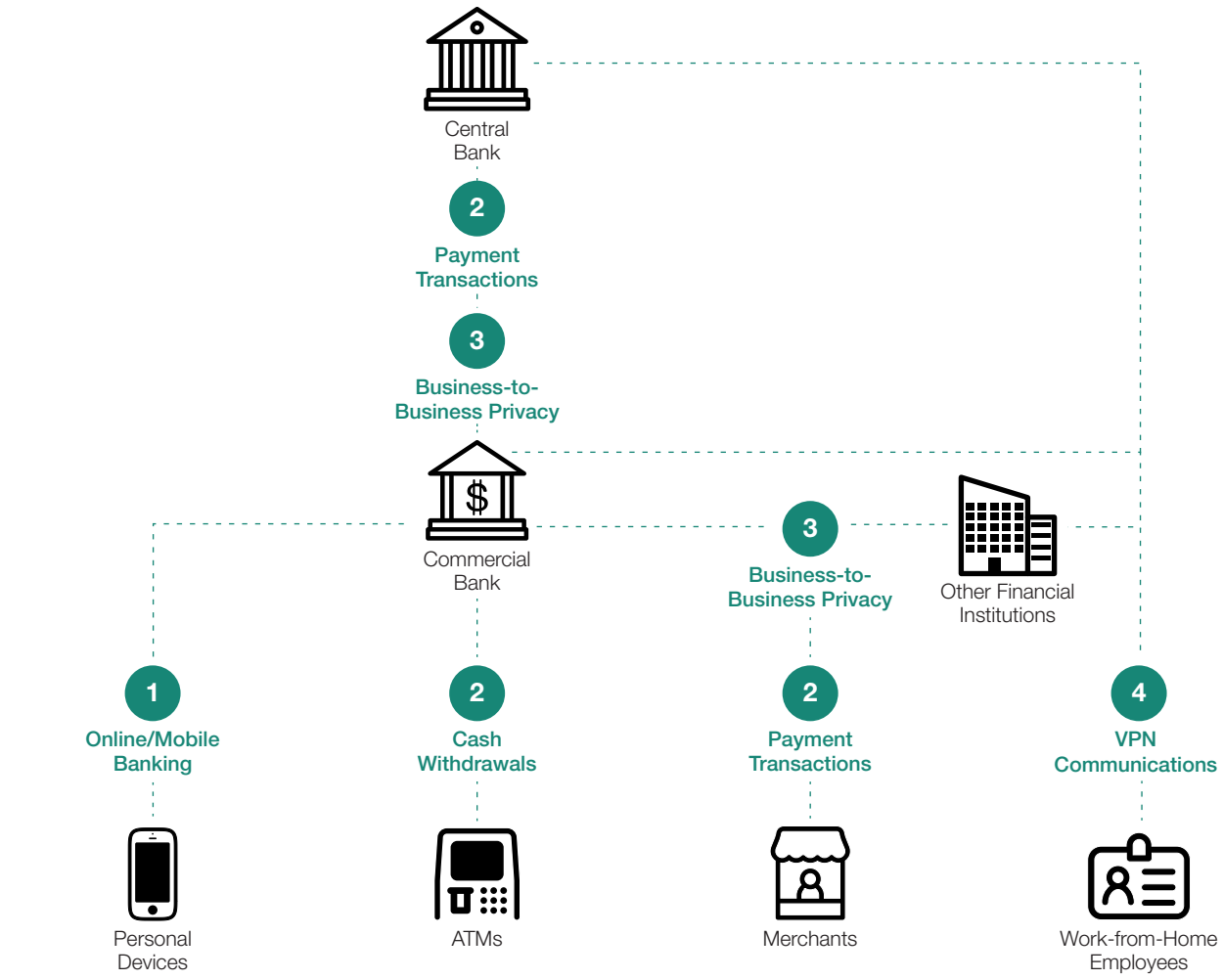
So far, the system has been effective. According to the Federal Reserve's own 2014 internal security audit, "the availability standard for the Federal Funds Service is 99.9 percent of operating hours," which it continues to achieve.[72] Despite the heavy security regulations, individual participants of Fedwire are responsible for their user-end security and operational resilience. Consequently, two security concerns exist—especially in the face of a quantum future. First, the deputation of end-user security responsibility presents a weakest-link scenario whereby the failure of a single participating institution to adequately secure its Fedwire access points permits an adversary entry into the entire network. Second, the reliance on NIST AES encryption standards means that any future quantum-enabled actor can employ Grover's algorithm to force entry into the Fedwire network regardless of the point of access.

This is due to the ability of future QCs to solve the complex mathematical problems that underpin today's principal cryptographic standards exponentially faster than the most powerful contemporary digital supercomputers, making AES and other algorithms standardized by NIST obsolete.[73] Successful quantum-enabled cyberattacks against these standard cryptographic algorithms would compromise the security of banking networks and other financial service connections, including RTGS systems like Fedwire. Yet, the risks arising from quantum decryption depend on the type of cryptography the US economic systems employ. For example, to break AES-256, which is the most ubiquitous symmetric key encryption algorithm—including by the Federal Reserve—an adversary would require over 7 billion years of brute-force methods with a classical supercomputer.[74]

However, a QC that employs Grover's search algorithm greatly reduces this complexity. Similarly, a fully functioning QC can break an asymmetric encryption key in mere hours using Shor's algorithm and subsequent optimizations thereof, making public key cryptography obsolete. Furthermore, ongoing developments in quantum computing and research in quantum algorithm optimization promise to decrease the time requirements for such quantum decryption. Given the numerous improvements and optimizations derived from Shor's algorithm since its inception, it is reasonable to assume that as research progresses new algorithms and iterations of existing algorithms will be discovered to reduce the processing requirements and increase their potential to make contemporary cryptography obsolete.[75]

Consequently, the "critical security services supporting the financial sector would be compromised by a sufficiently powerful quantum computer, threatening sensitive information managed and communicated by financial institutions and central banks."[76] Figure 6 depicts the potential impacts of this quantum threat on

Figure 6: Potential Impacts of Quantum Computers on Different Elements of the Financial System.



1 Online/Mobile Banking
Compromising customer-to-central bank/commercial bank/broker or e-commerce connections to commit unauthorized transactions, including CBDC

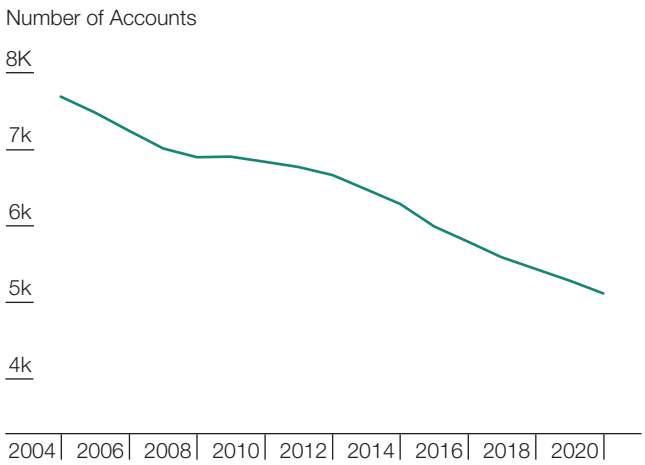
2 Payment Transactions and Cash Withdrawals
Committing unauthorized transactions against existing payment systems, and ATM machines.

3 Business to Business Privacy
Compromising widely used point-to-point secure communications between financial institutions, brokers and businesses

4 VPN Communications
Compromising VPN connections used for staff to work-from-home to access organizations internal and sensitive resources

Source: Adapted from Jose Deodoro, Michael Gorbanyov, Majid Malaika, and Tashin Saadi Sedik, "Quantum Computing and the Financial System: Spooky Action at a Distance?" (working paper, Asia and Pacific Department, International Monetary Fund, Washington, DC, 2021), https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159, 13.

Figure 7: Steady Decline in the Number of Fedwire Accounts with Balances since 2004, Demonstrating Consolidation of US Banking and Concentration of Interbank Payments



Note: To compute this metric we first exclude the activity of central banks, designated financial market utilities, excess balance accounts, and international organizations. From the remaining accounts, we keep only those that have positive balances.

Source: Adapted from Badev, Anton, et al., "Fedwire Funds Service: Payments, Balances, and Available Liquidity" (Finance and Economics Discussion Series 2021-070, Board of Governors of the Federal Reserve System, Washington, DC, 2021), https://www.federalreserve.gov/econres/feds/fedwire-funds-service-payments-balances-and-available-liquidity.htm, 15.

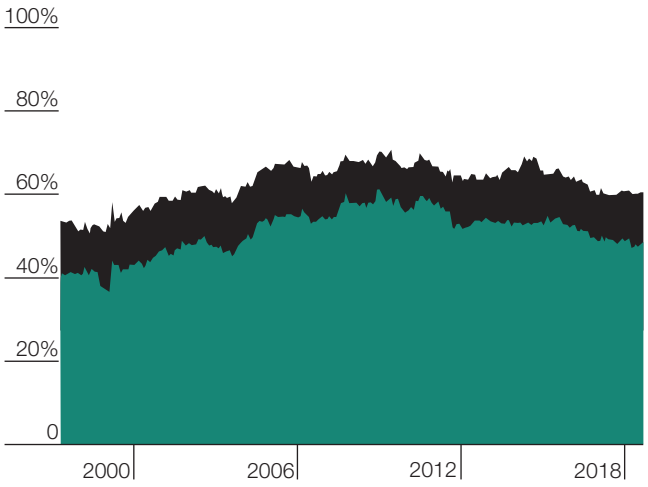
the various communication protocols in the financial system. As a result, a quantum-enabled attacker may covertly impair or otherwise disrupt critical infrastructures, including Fedwire, that today's standardized cryptography secures.

Although the Federal Reserve monitors it internally, Fedwire transaction information remains rather enigmatic, with transaction records containing only the sending bank's identification number, the receiving institution's identifier, the transaction time stamp, and the value transmitted.[77] A limit of $10 billion for single transactions within Fedwire and the lack of descriptive information on transactions—such as multiple chained or joined payments—hamper in-depth analysis of network dynamics. Moreover, the Federal Reserve tightly controls transaction data, limiting public or other, non-Federal Reserve borne analysis to a less granular time-series data set with only monthly aggregate value and volume information, which it publishes online.[78] While this stringent control of transaction data permits customer privacy and enables the Federal Reserve to centralize and streamline security operations, it likewise presents challenges for systemic cyberattack response. In the event of a catastrophic network breach, which is possible under the quantum scenario, this central control may delay the announcement to network participants and core nodes, which in turn may make a systemic event appear to be an isolated incident—in effect hindering detection and response time and even obfuscating the true extent of a given cyberattack.

Though it is the largest RTGS system globally, as of 2020, Fedwire had only some 5,125 accounts with balances operating within the network. While still encompassing a large number of participating institutions, when compared to the nearly 8,000 accounts with balances in 2004, this downsizing of nodes within the network indicates a broader shift in the Fedwire network topology (see figure 7).[79]

A parallel development within Fedwire during this same period is a concentration of payment value among the largest participating institutions. According to the 2021 report by Federal Reserve economists utilizing internal Fedwire transaction data, the Fedwire network is a highly concentrated network with the largest value of payments originating from a relatively small number of participating banks.[80] Further examination of the distributions of both volume and value within Fedwire "reveals a highly-concentrated system in which relatively few banks generate disproportionately high value of payments,"[81] where roughly 75 percent of value transacted within Fedwire originated from payments exceeding $100 million.[82] Despite this, such high-value payments accounted for only 1 percent of total Fedwire payment volume over the period. Moreover, other Federal Reserve economists have noted, again using non-public Fedwire

Figure 8: Concentration of Fedwire Transfers: Share of Payments Sent



Source: Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, *Cyber Risk and the US Financial System: A Pre-Mortem Analysis*, Staff Reports No. 909 (New York: Federal Reserve Bank of New York, 2021), https://www.newyorkfed.org/research/staff_reports/sr909.html, 11.

transaction data, that the top five banks by assets account for roughly half of total payments, while the top ten banks by size together account for over 60 percent of Fedwire transaction value (figure 8).[83] Consequently, the Fedwire network topology represents a scale-free network in which payment value is concentrated among very few hub nodes—or, more plainly, "Fedwire is a system that connects a lot of small financial institutions with a few banking giants."[84]

While this scale-free characteristic is not inherently problematic, as it facilitates the general banking system and transfer of liquidity that power the financial system globally, it can prove catastrophic under the proper circumstances. This is due to the inability of scale-free networks to handle large, idiosyncratic shocks or disruptions to the system. Although scale-free networks have "significant tolerance for random failures," Fedwire and other such networks are "highly vulnerable to targeted attacks."[85] Given the high concentration of liquidity among a few large banks within the banking system, a targeted large-scale attack—such as a QC-enabled disruption—against a core node in the Fedwire network would turn the entire US interbank payment system into a "coupled system where payments cannot be initiated until other payments complete," creating choke points in the smooth flow of liquidity in the financial sector.[86] Researchers have thoroughly documented the prospect of liquidity risk within the interbank payment system, especially within the Fedwire network. In their 2021 report for the Federal Reserve, Badev et al. note the following:

> The fact that high-value Fedwire payments are so heavily concentrated in a small number of large institutions increases liquidity risk in the system, as the proper functioning of each of these large institutions is tied closely to the smooth flow of payments through the system.[87]

Therefore, while any given shock or disruption may occur only within the Fedwire network, a shock of sufficient size that targets or otherwise impairs a core network node will not remain insulated within the network. Given the crucial role of liquidity within the banking and broader financial system, a sudden constriction of available liquidity can cause the financial sector, and consequently, the macroeconomy at large to grind to a halt.[88] This point was reiterated in a recent report from the Atlantic Council, noting especially the risk arising from a targeted attack on Fedwire:

> A targeted attack on wholesale payment infrastructures, such as the Fed's domestic funds transfer system, Fedwire, could cause major global financial shocks, including severe liquidity shortfalls, commercial bank defaults, and system-wide outages that would affect most daily transactions and financial stability. There would also be secondary effects, including severe market volatility.[89]

Thus, while Fedwire plays an essential role in the functioning of the financial system and the US economy, there exists a threat trifecta that a quantum-enabled adversary could exploit to wreak havoc on the United States. The combination of reliance on digital security that will be exposed to quantum intrusion, internally centralized operational design, and the overall concentration of network topology within Fedwire drastically increases the potential for a systemically disruptive event. As we have demonstrated above, once a QC exists, it could access the Fedwire network to initiate a disruption of payments, cause coordination failures within the system to hinder efforts of resilience, and ultimately impact the US economy irreparably in the fashion of, or likely worse than, the 2008 financial crisis. Even in the best-case scenario, in which an adversary gains access to Fedwire and merely makes their presence known, the damage will be notable, and systemic trust in a key pillar of the financial system will be washed away since "if you can't trust Fedwire, you can't trust the Fed. The efficiency of American commerce depends on that trust."[90]

6. WHAT WOULD A QUANTUM COMPUTER ATTACK ON FEDWIRE LOOK LIKE?

Key Takeaways:

- If a single bank of sufficient size cannot process transactions and post margins, the disruption could spread rapidly to counterparties and other financial market infrastructures, leading to heightened liquidity and solvency risk throughout the system.
- An attack could also spark a demise in systemic confidence with the potential of triggering further, second-round bank runs, worsening liquidity issues and even leading to bank failures throughout the financial system.
- These impacts will worsen under prolonged outages, leading to cascading liquidity and solvency risks, freezing up vital flows of capital, depressing markets and asset prices, and slashing confidence and trust within the system while simultaneously escalating market volatility and the risk of a general, economy-wide bank run.

> An attack that compromises an institution's system or data can impair its ability to service creditors not directly affected by the attack. In addition, an attack on a trading platform, a settlement and payments system, or a central securities depository could have a major impact on the financial system as a whole because these are critical infrastructures on which financial firms depend and for which there are few substitutes.
>
> —Loretta J. Mester, president and CEO, Federal Reserve Bank of Cleveland[91]

Given the role of payment and settlement systems as critical financial market infrastructure, any successful attack against an RTGS system could have extreme consequences. As we outlined above, if conditions prevent the settlement of cross-border and domestic transactions between banks operating within the Fedwire RTGS system, a cyberattack could lead to liquidity issues for receiving parties, contract breaches, and payment and obligation failures, among other issues. The high degree of interconnectivity within the financial sector can augment financial contagion and spread systemic risk. Outages in key FMIs,

Photo: (Getty Images)

especially RTGS systems, can inhibit access to capital or assets for otherwise stable financial institutions, preventing the institutions from adequately managing their exposure to broader market risk and potentially leading to solvency concerns. Consequently, a cyber disruption to operations at key FMIs, such as Fedwire, can ignite a chain effect across the system in which the initial halt in interbank transaction processing can swell into liquidity crises in the financial system at large. Moreover, even if it is initially isolated to a single institution or bank, the disruption of outgoing payments may cause settlement issues for network counterparties, as these secondary institutions often rely on incoming payments from such a key network node to balance their own capital flows and meet liquidity requirements.[92] Thus, in a scenario that incapacitates a major Fedwire participant, several peripheral banks may fail to meet intraday liquidity and solvency requirements, further accelerating the risk of contagion in the system.

For example, within financial institutions, if a single bank of sufficient size cannot process transactions and post margins, the disruption could spread rapidly to counterparties and other financial market infrastructures, leading to heightened liquidity and solvency risk throughout the system.[93] Ashwin Clarke and Jennifer Hancock demonstrated that the total value of unsettled payments varies according to the time of the RTGS system disruption and the participant FMI's size or overall market share. Nonetheless, given the dominance of Fedwire within the domestic (and international) interbank payment network, any disruption to Fedwire transfers can thrust financial institutions into a liquidity crisis, let alone on seasonally high payment days.[94]

Such an attack could also spark a demise of systemic confidence with the potential of triggering further, second-round bank runs, worsening liquidity issues and even leading to bank failures throughout the financial system. This could materialize through reduced volume of transactions in connected markets, increased price volatility and potential stock market crashes, broad runs on withdrawals, and a reduction in capital flows. The contagion throughout the vast financial network would continue with the expectation of direct impacts on stock and derivatives markets, only further tightening liquidity and depressing prices within the financial sector. In addition to the second-round effects of contagion in the interbank network, there are both direct and indirect impacts of cyber incidents for a given individual firm. As when one casts a stone into a still pond, firms incur the initial or direct costs early and quickly before the impacts of a cyber disruption reverberate and spread widely throughout its market structure and ultimately its supply chain. In this way, indirect costs of systemic cyber incidents affect financial institutions over a protracted period and are objectively more difficult to attribute and quantify, presenting significant challenges to any containment or mitigation efforts.[95] Such scenarios would inevitably hamper economic growth in the countries they initially affect, and perhaps others through the financial system network, holding the potential to "weigh heavily on the functioning of the financial system" as a whole.[96]

While the financial sector is a frequent and lucrative target for cyber intrusions and attacks, econometric estimates of the impacts of cyberattacks generally, let alone those targeting the financial sector, are both scarce and largely lacking in crucial details. Due to our reliance on a complex and under-secured cyber network, the potential for a cyber black swan is increasing exponentially. We saw the potential for this systemic risk in the 2017 NotPetya cyberattack, which despite targeting Ukraine ended up costing Maersk an estimated $250 to $300 million in losses.[97] Within this unsecured network, one area in particular stands out as a prime target for a cyberattack, in terms of both exposure and potential impact: America's financial sector, particularly the Fedwire interbank payment system. Given their high dependence on technology, numerous network connections, and vital role in the financial system, systematically important RTGS systems—such as Fedwire—are prime targets for malign cyber actors keen on causing maximum damage to the system. As Frank Adelmann et al. assessed, "a successful cyberattack on a systemically important payment system that processes

large-value and time-critical transactions could transmit disruption to the entire financial system (across borders as well as domestically) with system, institutional, and environmental interdependencies."[98]

Indeed, the costs of past disasters in the financial network have been large. A 2009 study implemented a computable general equilibrium (CGE) model to calculate the costs of the tragic events of September 11, 2001. It found that the attacks cost the US financial sector roughly $17 billion (2006 USD) in losses over the two years that followed.[99] Many experts warn that this amount will be minuscule compared to a cyber disruption within the financial system. Nonetheless, there is a clear absence of projects that adequately study this threat. Additionally, those that do exist are prone to vast undercounts.

Utilizing a standard financial value-at-risk framework to quantify cyber risk for the financial sector, Antoine Bouveret finds that average losses from cyberattacks would result in losses of $97 billion, or 9 percent of banks' net income in a baseline scenario.[100] In a more extreme case, average losses from cyberattacks increase to $268 billion, or just over a quarter of banks' net income, with risk indicators ranging between roughly $350 billion and $530 billion, or over a third to over half of net income. The introduction of contagion effects across financial institutions within the network increases aggregate losses by approximately 20 percent. Crucially, Bouveret estimated these results utilizing industry data from market participants such as cyber insurers and cybersecurity companies, which may be subject to bias given their financial incentives to overstate losses.

In the same year, researchers published another crucial study that also elucidated the effect of network contagion on the overall impacts of cyber incidents. Attempting to tackle the technically cumbersome and elusive issue of estimating cyberattacks at large in a variety of industries, Paul Dreyer et al. introduced a novel approach to quantifying the impacts of cyber risk. In their study, the RAND team estimated both direct and systemic costs resulting from a variety of cyber incidents utilizing a sectoral input-output model. However, this study was limited in the examination of firm-level cyberattacks outside of the financial sector. Moreover, its model was limited to analyzing systemic costs in terms of the backward supply linkages or upstream supply chain effects of cyber incidents. Nonetheless, the authors concluded that the systemic costs—including both upstream and downstream costs—could greatly outweigh the direct impacts of a given cyber incident.[101] Consequently, in any quantitative analysis of cyber risk, especially within the financial sector, it has become paramount to include the impacts of cascading or contagion effects.

More recently, in their 2020 paper, Rokhaya Dieye et al. empirically estimate the macroeconomic losses from cyberattacks impacting the financial sector in the United States. Their results indicate that in the event of a cyberattack targeting the financial sector, macroeconomic impacts would reverberate throughout other industry sectors and cost the US economy approximately $131.5 billion to $400 billion in the baseline and worst-case modeling scenarios respectively.[102] Collectively, the works of Bouveret and Dieye et al. set a standard for the scale of expected losses due to cyberattacks in the financial sector. Yet, importantly, although both studies include the overall impacts of an attack in the financial sector, neither provides a thoroughly granular investigation of the mechanisms by which contagion spreads. However, in 2021 Rustam Jamilov et al. provided the first analysis to attempt to tackle this issue. Utilizing a quarterly data set covering more than 12,000 firms in 85 countries, the authors found that cyber risk exposure negatively and significantly correlates to stock returns of affected firms, where each additional mention of cyber risk terms on a firm's quarterly earnings calls reduces the institution's weekly stock returns by over 4 basis points.[103] Furthermore, their model demonstrates that idiosyncratic cyber risk can propagate throughout a network of interconnected firms in stock markets and cause contagion in the aggregate financial system.

Utilizing a novel theoretical and quantitative approach, Jonathan Welburn and Aaron Strong extended a sectoral-level input-output model to estimate the impacts of cascading cyber failures in a variety of industries. Specifically focusing on cascading failures, the RAND team captured the consequences of a single cyber event that propagates outward in both cyber networks and supply chain networks, leading to a domino-like effect across interconnected and interdependent firms. Analyzing both historical and hypothetical cyber incidents, they studied firms like the banking giant JP Morgan Chase. In this hypothetical cyberattack, Welburn and Strong estimate that a cyber incident that stops all of JP Morgan's retail banking activities for a single day would cause direct losses of up to $56 million for the bank, while potential upstream and downstream losses from the event could reach $145 million and nearly $4 billion respectively.[104]

Although the study makes significant contributions toward quantifying the impacts of cyber disruptions, it is worth noting that the report falls short in considering banking and financial sector–specific contagion effects. As the authors state, in the case of JP Morgan Chase, "our analysis could even underestimate total impacts" as an outage affecting banking services "could lead to many systemic impacts, notably bank runs," which are not addressed in their model.[105] Furthermore, despite noting that "absent advances in postquantum cryptography, the advent of quantum computing could enable encryption breaking en masse, leading to concern over large scale independent failures," the model fails to address a potential quantum-enabled cyber incident, which would greatly exacerbate the total impacts.[106]

Despite distinguishing between the overall origin and immediate trajectory of traditional operational risk and cyber-induced shocks to the financial system, Thomas Eisenbach et al. highlight the similarities between the two in their eventual impacts, emphasizing that a single shock that results in direct costs to the affected bank would ripple throughout the financial network and spill over to counterparties within the sector through liquidity runs that would eventually reach the real economy.

Yet the team from the Federal Reserve Bank of New York underscores the fact that a cyber event, unlike traditional financial risk, may be a deliberate act to damage the financial system and thus presents unique challenges to the sector. Furthermore, the paper asserts that "high-value payment and settlement systems may be natural candidates for a malicious attacker intent on inflicting the largest possible damage to the financial system and the broader economy" by immobilizing capital of everyday borrowers and investors, regardless of a general run or other changes in behaviors of the affected party and their immediate network.[107] Making matters worse, the very structure of Fedwire allows even an impaired (or otherwise cut-off) bank to continue to receive incoming payments into its reserves account regardless of its ability to remit or otherwise disperse outgoing transfers. Consequently, a cyberattack that impairs a bank's access to Fedwire creates a liquidity trap in the highly active interbank payment network.

Additionally, the paper details how asymmetric information plays a detrimental and amplifying role in systemic cyber risk to the financial sector. This information asymmetry can arise through various channels, from the complications and general lack of transparency within the financial network to the delay in disclosure of an incident to the broader network while the attacked institution decides on its communication strategy. Accordingly, incomplete information about the location of a liquidity shock within the financial network has been shown to drive banks to "engage in individually prudent but systemically harmful actions" in forming their optimal response to a cyber shock.[108] Typically, in the post-Dodd-Frank banking environment, when liquidity is scarce throughout the financial sector, banks manage same-day liquidity levels by delaying payments and precisely timing inflows and outflows to avoid solvency risks. Thus, this individually optimal response can create both clusters and delays in the aggregate value of payments throughout the financial

network.[109] When paired with the Fedwire mechanism that allows for liquidity traps, heightened uncertainty, and information asymmetry issues, this behavior can quickly spark liquidity spirals that cascade throughout the sector and even ignite into a general bank run.

Expanding on these observations, Eisenbach et al. utilized private Federal Reserve data on Fedwire transactions to quantify systemic cyber risk in the RTGS system network. Unlike earlier studies, this report provides a more granular examination of how a single cyberattack can cascade throughout the financial network. However, it falls short in terms of quantification in that it expresses the modeled results as percentages of impaired bank assets rather than dollar amounts. Nonetheless, the analysis is groundbreaking in the study of financial cyber risk, particularly within the Fedwire RTGS system.

The Eisenbach et al. model begins by assuming that any one of the top five US banks within the Fedwire network, by size of total consolidated assets, falls victim to a cyberattack in which the attacked institution can receive but not remit payments for a single day. Such impairment in the payment system could make it difficult to shift liquidity between accounts within the same bank holding company, let alone outward to other banks within the Fedwire payment network. Throughout the day, as the attacked, core-node bank accumulates payments from counterparties within the RTGS network, this systemically important bank "soaks up liquidity, effectively acting as a liquidity black hole."[110]

The authors then model how and where this lack of payments induces liquidity dislocation throughout the Fedwire network and estimate the impact in terms of the percentage of US bank assets that become impaired, excluding the target bank. In this context, "a bank is considered *impaired* if its end of day reserves fall sufficiently below the bank's past daily reserve average."[111] With these assumptions and parameters accounted for, Eisenbach et al. estimate that, on an average day, if a malicious actor attacks any of the top five banks, approximately 38 percent of total bank assets within the Fedwire network become impaired. According to the authors, the result of this baseline scenario "reflects the high concentration of payments between large institutions, and the large liquidity imbalances that follow if even one large institution fails to remit payments to its counterparties," quantifiably confirming the scale of the threat posed by an attack against Fedwire.[112]

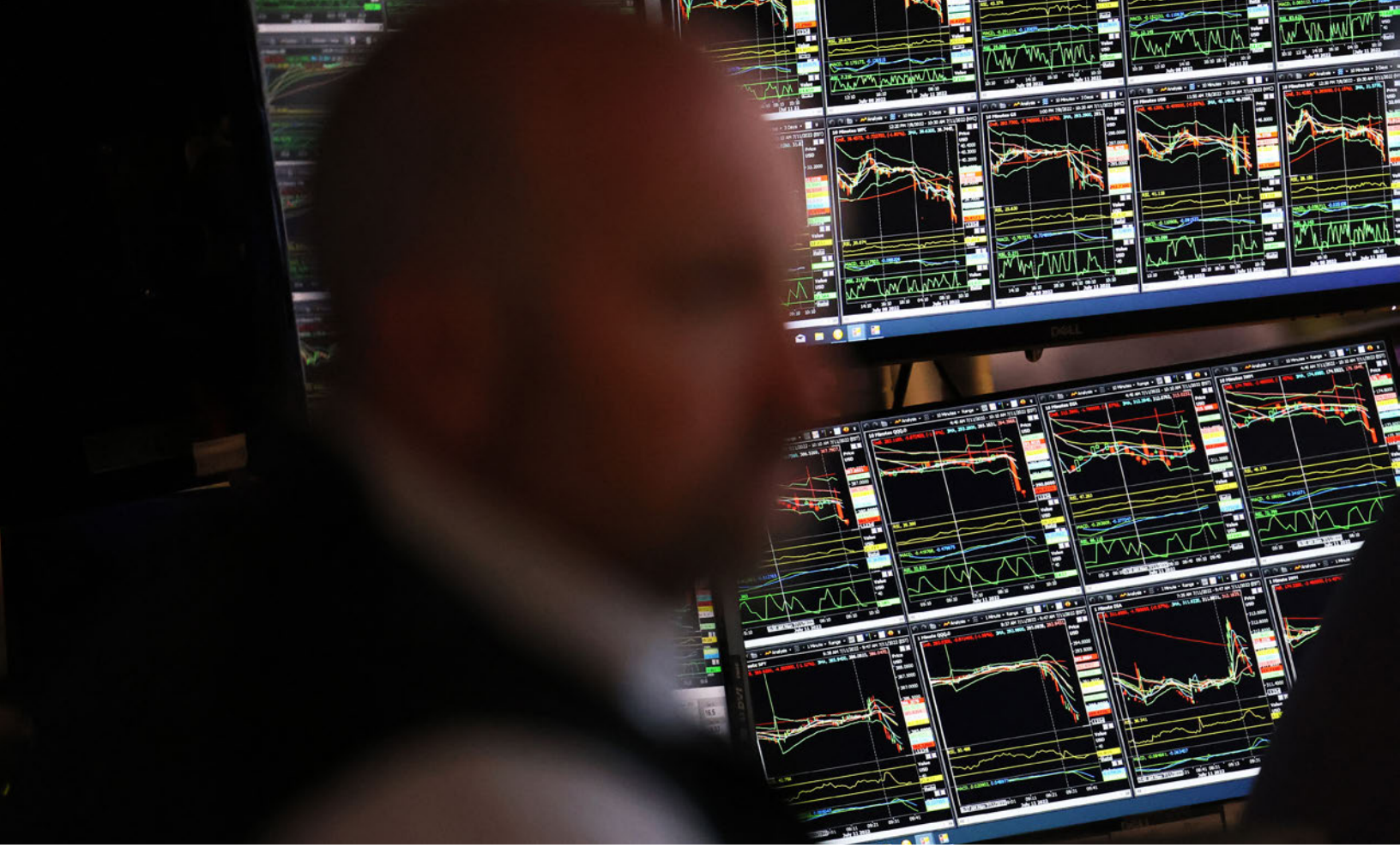
Having established this baseline, the paper goes on to consider other, more extreme scenarios in the authors' model. Of particular interest is their analysis of an adversarial cyber actor that can obtain private information on both a target bank and its network interconnectedness. As the authors note, "One distinguishing feature of cyber attacks is that they may be designed for maximum disruption. The extent to which an attacker is informed with respect to the payment system, the targeted institution, and its relation to the payment network, may dictate the magnitude of systemic risk arising in an attack."[113] Under such a scenario, in which the attacker can infiltrate the targeted top-five bank undetected and extract data on the target's activities and internal network mechanisms, the average maximum impact within the Fedwire network increases by approximately 63 percent from the baseline modeling scenario. Although the authors contend that "access to such detailed information may be unlikely," this scenario unfolds similarly to how one would expect a quantum cyber intrusion into Fedwire to manifest.

Moreover, the analysis goes on to estimate the magnitude of the increase in impairment impact on days when Fedwire transfer payments are especially high. Correspondingly, on any of the 12 such seasonal days, an attack against a top-five bank would see an increase of roughly 11 percent more impaired bank assets from the baseline scenario. Additionally, an attack on the single worst seasonal day for one of the top five banks adds an additional 38 percent impairment when compared to the average. Moreover, Eisenbach et al. extend the model to determine the increase in impact from the baseline scenario if these attack scenarios persisted longer than a single day. They found the

average impact in terms of liquidity shortfall grows from $44 billion in impaired assets on the first day of the attack to $85 billion by the second day. However, by the fifth day of persistent disruption of a top-five bank's payment access, the incremental increase from the day prior is only $28 billion in assets.[114] As such, the impact of a persistent cyber disruption to Fedwire operations at a top-five bank grows logarithmically over time.

Concluding their analysis, Eisenbach et al. examine the reverse-case scenario to determine the number of smaller banks that would need to be attacked to impair a top-five bank as described earlier. In this reverse-engineered analysis, their model estimated that a cyberattack that disrupted 24 small banks (with under $10 billion in assets) or just 10 medium-sized banks (with $10–$50 billion in assets) would form the critical mass of impaired assets, and consequently of interbank liquidity and Fedwire transfers necessary to yield their top-five bank scenarios.[115]

Consequently, as the literature demonstrates, a cyberattack against one of the top five banks in the Fedwire network, or against a small group of less significant banks, can generate drastic impacts on the attacked institution(s) as well as on the financial system at large. If major financial institutions of sufficient size cannot fully access the Fedwire network or otherwise process transactions, cascading liquidity and solvency risks will arise throughout the sector, freezing vital flows of capital, depressing markets and asset prices, and slashing confidence and trust in the system while simultaneously escalating market volatility and the risk of a general bank run. Furthermore, these impacts will only worsen under prolonged outages or, most alarmingly, in the case of a quantum-enabled cyberattack on the Fedwire RTGS system, where an adversary would not only be able to facilitate intrusion but conduct harvest-now-decrypt-later infiltrations to gain insight into how to cause maximum disruption and wreak financial chaos on the US economy.



7. METHODOLOGY AND TOPOLOGY OF DIFFERENT MODELING SCENARIOS

Key Takeaways:

- We implemented a series of seven shocks to four variables of interest (liquidity, financial market volatility, and market confidence) to accurately capture the overarching impacts of a systemic financial cyber risk event targeting Fedwire. Furthermore, we scaled all GEM shocks to reflect varying degrees of five different attack scenarios based on the literature.
- We modelled our output in baseline-case ("Quantum_Baseline") and worst-case ("Quantum_Max") scenarios, which depict an attack against Fedwire on both regular days and on the single largest payments day of the year and with private information on both the target bank(s) and their network interconnections, representing action by an attacker who has lurked within or harvested data on the entire Fedwire network.

To account for not only the direct financial impacts on the affected bank but also the cascading contagion effects throughout the broader financial system and the US macroeconomy, as outlined above, we implemented a two-staged economic analysis to quantify the total indirect economic impacts of a QC cyberattack on the Fedwire interbank payment system.

We began by establishing the direction of, or Granger-causality between, quarterly growth in Fedwire transactions and the

Photo: Traders work on the floor of the New York Stock Exchange during morning trading on July 11, 2022, in New York City. (Photo by Michael M. Santiago/Getty Images)

Table 3: OLS Regression Estimation Results: Relationship between Fedwire Transaction Value and Financial Sector Variables

DEPENDENT VARIABLE: GROWTH IN FEDWIRE TRANSACTIONS VALUE - UNIVARIATE REGRESSIONS PERCENT CHANGE (QUARTERLY, 2005Q2 - 2021Q4)					
VARIABLE	LAGS	COEFFICIENT	SIGNIFICANCE	R-SQUARE (ADJ. R-SQUARE)	DW STAT
GDP Chained Quantity Index Growth Percent Change (Quarterly)	1 Quarter	0.389	***	0.212 (0.186)	1.81
	2 Quarters	0.232	**		
HYI: High Yield Index (liquidity proxy) Percent Change (Quarterly)	1 Quarter	-0.110	***	0.186 (0.173)	1.77
VIX: CBOE Market Volatility Index Percent Change (Quarterly)	1 Quarter	-0.053	***	0.158 (0.131)	1.85
	2 Quarters	-0.054	*		
CIX: Yale Stock Market Confidence Index Percent Change (Quarterly)	1 Quarter	-0.148	*	0.109 (0.080)	1.86
	2 Quarters	-0.220	**		

Note: ***, **, and * denote significance at 1 percent, 5 percent, and 10 percent levels respectively; variable lags selected via SBIC criteria; DW Stat corresponds to the regression output's Durbin-Watson test statistic.

Source: Based on data from the Federal Reserve, US Bureau of Economic Analysis, Yale School of Management, ICE Data Indices LLC, and Chicago Board Options Exchange.

quarterly growth rate in US GDP, which, as section 5 explains, demonstrated that growth rates in quarterly Fedwire transactions "lead," or Granger-cause, GDP growth. This indicates that an increase (or decrease) in the growth rate of Fedwire transaction values in each quarter will lead to a corresponding increase (or decrease) in GDP growth in the following quarters.

Having established the direction of this relationship, we utilized univariate regression to quantify it. In addition to the relationship between Fedwire growth and GDP growth, we analyzed the relationship between quarterly Fedwire growth and other variables of interest from our qualitative analysis above. Namely, we examined the effect of Fedwire growth on quarterly change in proxies for liquidity, financial market volatility, and market confidence—all of which a successful cyberattack against Fedwire would affect either directly or indirectly and would likewise cause second-order impacts to overall GDP. The results of these calculations, tabulated in table 3, allow us not only to quantify the magnitude of the relationships but also to calibrate the percentage results from Eisenbach et al. in terms applicable to econometric modeling of total indirect impacts.[116]

As we outlined above and detailed in sections 5 and 6, the analyses by Eisenbach et al. and Badev et al. are largely non-reproducible as they both utilize non-public Fedwire transaction data. Additionally, the representation of the Eisenbach et al. findings in terms of the percentage of impaired assets hinders supplementary analysis, which often (as in this case) requires dollar amounts for calculations.[117] Consequently, using the less granular, publicly available Fedwire transaction data in conjunction with data points we extrapolated from Eisenbach et al., we used a bootstrap methodology to approximate the dollar amount of the average

Table 4: Oxford Economics GEM Shock Calibration Information

PERCENTAGE OF DAILY FEDWIRE TRANSFERS (VALUE) IMPAIRED IN BASELINE OF EISENBACH, ET AL. (2021) [DERIVED IN APPENDIX B FROM AUTHORS' CALCULATIONS & DATA EXTRAPOLATED FROM EISENBACH, ET AL. (2021)]				AGGREGATE BANK ASSETS IMPAIRED (PERCENTAGE MULTIPLIER) [RELATIVE TO VARIOUS SCENARIOS DESCRIBED IN EISENBACH, ET AL. (2021)]					
				15%	CYBER_BASELINE (PERCENT)			QUANTUM_ BASELINE (PERCENT)	QUANTUM_ MAX (PERCENT)
					1 DAY	2 DAY	5 DAY	1 DAY	1 DAY
REGRESSION VARIABLE	REGRESSION LAGS	REGRESSION COEFFICIENT	GEM VARIABLE & DURATION	GEM SHOCK	1.38	1.513	1.608	1.475	1.6194
GDP Chained Quantity Index Growth Percent Change (Quarterly)	1 Quarter	0.389	"GDP (2025Q2-2025Q4)"	-5.83%	8.05%	8.83%	9.38%	8.60%	9.45%
	2 Quarters	0.232	"GDP (2025Q3-2026Q1)"	-3.48%	4.80%	5.26%	5.59%	5.13%	5.63%
High Yield Index (liquidity proxy) Percent Change (Quarterly)	1 Quarter	-0.110	"Credit Conditions (2025Q2-2025Q4)"	-1.66%	2.28%	2.51%	2.66%	2.44%	2.68%
VIX: CBOE Market Volatility Index Percent Change (Quarterly)	1 Quarter	-0.053	"VIX (2025Q2-2025Q4)"	0.80%	1.10%	1.21%	1.29%	1.18%	1.30%
	2 Quarters	-0.054	"VIX (2025Q3-2026Q1)"	0.81%	1.11%	1.22%	1.30%	1.19%	1.31%
CIX: Yale Stock Market Confidence Index Percent Change (Quarterly)	1 Quarter	-0.148	"Equity Shock (2025Q2-2025Q4)"	-2.21%	3.05%	3.35%	3.56%	3.26%	3.58%
	2 Quarters	-0.220	"Equity Shock (2025Q3-2026Q1)"	-3.30%	4.56%	5.00%	5.31%	4.87%	5.35%

Source: Based on data from the Federal Reserve, US Bureau of Economic Analysis, Yale School of Management, ICE Data Indices LLC, Chicago Board Options Exchange, and Eisenbach et al. (2021).

daily value of Fedwire transfers for the top five banks in 2018. This dollar-denominated amount is roughly equal to the total average value of impaired Fedwire transfers in the baseline scenario that Eisenbach et al. described. Finally, utilizing the regression coefficients from table 3, we can relate the dollar amount of impaired Fedwire transfers to the amount of aggregate bank assets and represent these figures in terms of shocks to GDP, liquidity, market volatility, and market confidence and prices applicable to the Oxford Economics' Global Economic Model (GEM) to calculate the total costs for varying degrees of attack scenarios.[118]

Accordingly, and as we have detailed in table 4, we implemented a series of seven shocks to the four variables of interest to accurately capture the overarching impacts of a systemic

financial cyber risk event targeting Fedwire as it reverberates throughout the vast financial network and ultimately the US economy. We carefully calibrated each of the shocks using our two-staged economic analysis, which correlated our regression analyses with the network impairment effects of Eisenbach et al. Furthermore, we scaled all GEM shocks to reflect varying degrees of five different attack scenarios based on the literature.

Thus, for all scenarios, we assume that the attacked bank(s) can receive but not remit payments over the duration of the quantum attack.[119] *Cyber_Baseline* corresponds to our baseline scenario of a single-day cyberattack (a highly sophisticated classical computer attack or a basic QC attack) against Fedwire at an average top-five bank by assets (or, in the reverse case, 24 small banks with under $10 billion in assets each, or 10 medium banks with $10–$50 billion in assets each) on an average day. We then extend this Cyber_Baseline scenario to represent a similar baseline attack that impacts Fedwire transactions as above over two and five days respectively.

Next, we developed a more advanced attack scenario that more accurately reflects expected quantum adversarial capabilities. This *Quantum_Baseline* scenario represents a single-day quantum cyberattack against Fedwire as in the first scenario, but on one of 12 seasonally high payment days and with private information about the target(s). This scenario represents an attack by a quantum attacker who has lurked within or conducted harvest-now-decrypt-later attacks on a bank's network.

Finally, we modeled the worst-case scenario as *Quantum_Max*, which depicts an attack against Fedwire as in the Quantum_Baseline scenario, but on the single largest payments day of the year and with private information on both the target bank(s) and their network interconnections—representing action by an attacker who has lurked within or harvested data on the entire Fedwire network. We have tabulated the different shocks, their duration, and the various scaled scenarios in table 4.

8. ECONOMIC IMPACTS OF A QUANTUM COMPUTER CYBERATTACK ON THE FEDWIRE INTERBANK PAYMENT SYSTEM

Key Takeaways:

- Utilizing original econometric models in addition to the Oxford Economics Global Economic Model (GEM), we found that a quantum computer attack on FedWire and against US banks would have drastic consequences for the financial sector itself, and reverberate throughout the entire US macroeconomy.
- In summary, a single-day quantum computer attack on a top-five bank would cost the US economy between $2 and $3.3 trillion in indirect impacts alone.
- Impacts are measured in terms of foregone GDP (GDP at Risk), or the difference between the projected GDP in a normal future vs. our various attack scenarios.

According to our analysis, a quantum-enabled hack impairing access to the Fedwire interbank payment system for select groups of banks, as outlined in section 7, would have daunting impacts on the immediately targeted institution as well as on other banks within the Fedwire network. Moreover, these cascading impacts would quickly spread through contagion channels

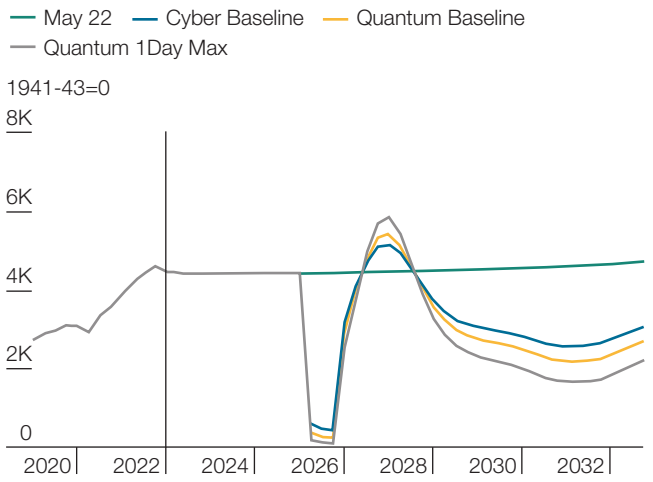
Photo: (Getty Images)

to the broader financial system, creating a self-propelling risk mechanism and ultimately crashing the US economy at large. Such a targeted attack against key interbank network nodes, as modeled in the quantum scenarios, would invariably cause a significant systemic shock resulting in economic losses limited neither to the targeted institution nor to the financial network alone. As we have mentioned throughout this report, such an initial idiosyncratic shock to even a single actor within the fragile and convoluted RTGS system network would spark an internal liquidity black hole, leading to cascading liquidity and solvency risks and escalating levels of endogenously forgone payments and accelerating solvency risks throughout the network.

Given these initial shocks and their resulting liquidity crunch within the Fedwire network, credit conditions throughout the broader financial system, and even within the economy at large, would tighten. This negative shock to credit conditions, outlined above in our scenario, would directly affect consumption and both business and residential investment, further depressing equity and housing prices in the economy and impacting mortgage liabilities in the residential sector, although to a lesser degree. The resulting contraction in output would reflect the systemic impact of tighter credit conditions, increased financial volatility, and depressed equities on consumption, investment, and prices as the endogenous liquidity traps stemming from the hack of Fedwire reverberate throughout the financial system, pass further to the general economy, and lead to second-order impacts (see figures 9–13).

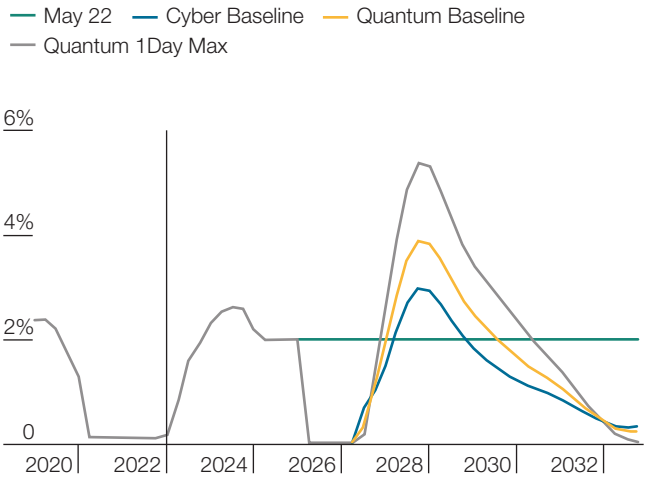
Although these first-order impacts represent a systemically critical risk in themselves, the propagation of the shock through second- and third-order impacts ensures the scenario evolves into a financial catastrophe. As we have modeled in the GEM and detailed above, these second-order impacts would result in significant shocks to financial market volatility and overall confidence, spiraling equity prices, and tightening liquidity and credit conditions in other financial subsectors throughout the network. Finally, the impairment of Fedwire in our various scenarios would again reverberate through the financial system in third-order effects whereby the general decline in market sen-

Figure 9: Projected Traditional Equity Prices in the US Broader Financial Sector after a Quantum Computer Attack on Fedwire



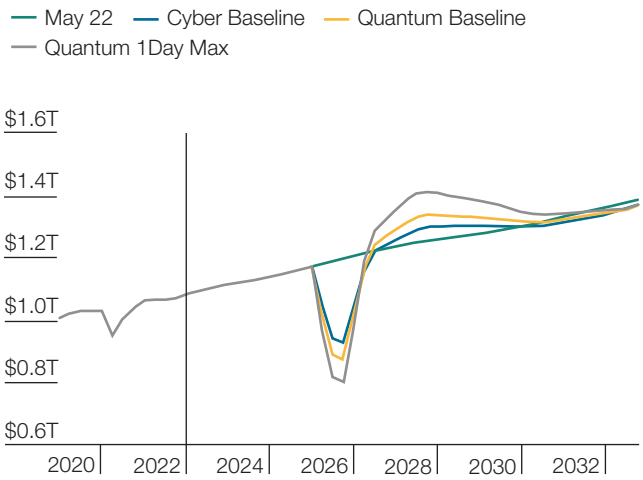
Source: Based on data from Oxford Economics.

Figure 10: Projected US Central Bank Policy Rate after the Impairment of Fedwire by a Quantum Computer



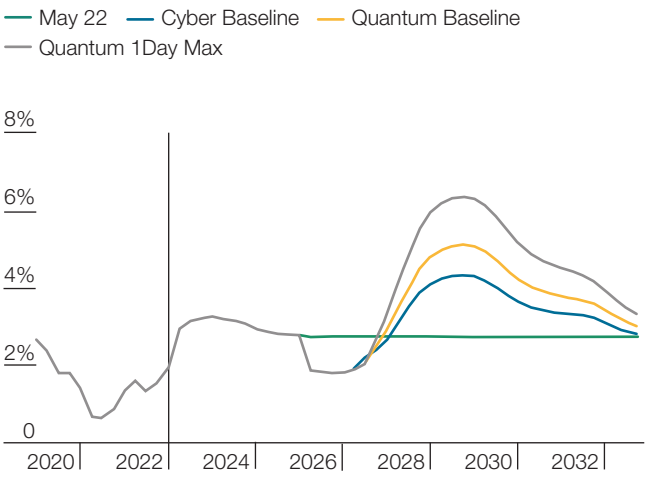
Source: Based on data from Oxford Economics.

Figure 11: Projected Decline in US Fixed Investment after a Quantum Cyberattack



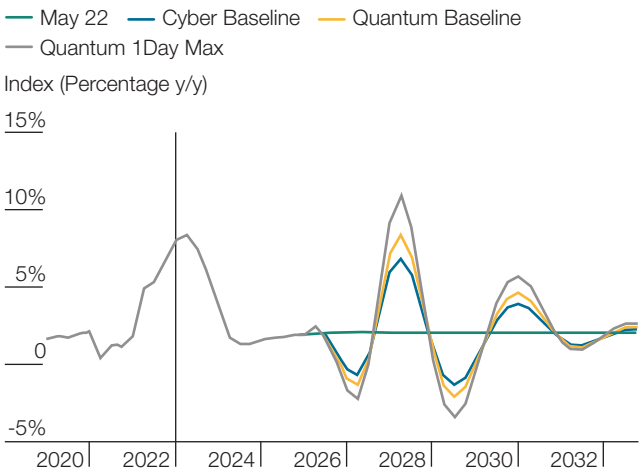
Source: Based on data from Oxford Economics.

Figure 12: Projected US Bond Yields after a Quantum Hack of the Interbank Payment System



Source: Based on data from Oxford Economics.

Figure 13: Projected US Consumer Price Index Turbulence after a Quantum Cyberattack



Source: Based on data from Oxford Economics.

timent, prices, and liquidity would generate general bank run conditions, solidifying the reach of the initial shock to the broader macroeconomy.

For example, equity prices would fall sharply as a result of the sudden changes in market conditions and sentiment, such as that which would result from our modeling scenarios. Our econometric modeling demonstrated that these second-order effects would manifest in the form of a sharp increase in market volatility through the VIX Index, with a corresponding negative impact on the overall prices of equities that further augments market volatility and, when paired with liquidity issues, would spark fire sales and potentially a general financial run. The overall impact on business and consumer confidence ignited by the initial Fedwire impairment and resulting liquidity shocks would generate a ripple of cascading second-order impacts that would beget negative wealth effects, freeze capital flows, and generally reduce confidence throughout the economy. Consequently, these second-order impacts would lead to a procyclical decline in aggregate demand that would ultimately yield a fall in output in most industrial sectors and a vast, economy-wide contraction. These third-order impacts could feed back into the financial system and further propel the decline in financial activity.

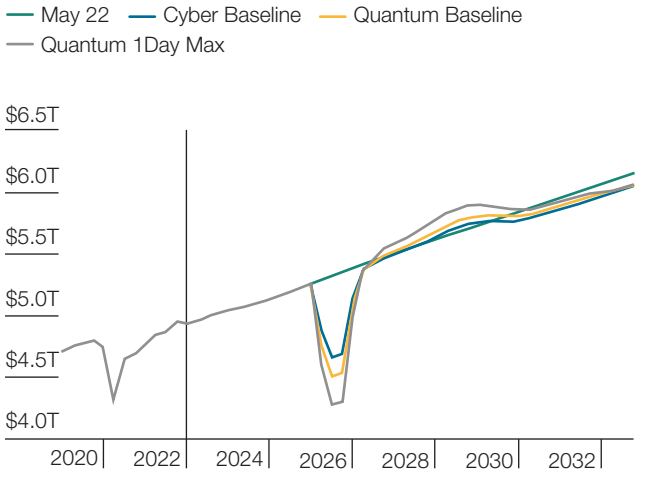
Table 5: Summary of Findings: Economic Impact of a Quantum Computer Cyberattack on the Fedwire Interbank Payment System

OXFORD ECONOMICS GEM MODELING RESULTS FOR THE U.S. ECONOMY					
MODELING SCENARIO	CYBER-ATTACK DURATION	DURATION OF RESULTING RECESSION	"GDP-AT-RISK (BILLIONS, CHAINED 2012 USD)"	"GDP-AT-RISK (PERCENT OF 2021 ANNUAL GDP)"	PERCENT INCREASE FROM 1-DAY CYBER_ BASELINE
Cyber_Baseline	1 Day	6 Quarters	-2077.07	-10.69%	
	2 Day		-2292.67	-11.8%	10.4%
	5 Day		-2406.94	-12.4%	15.9%
Quantum_Baseline	1 Day		-2577.72	-13.3%	24.1%
Quantum_Max	1 Day		-3306.57	-17.0%	59.2%

Source: Based on data from the Federal Reserve, US Bureau of Economic Analysis, Yale School of Management, ICE Data Indices LLC, Chicago Board Options Exchange, and Eisenbach et al. (2021).

Due to the centralized topology and central role of the Fedwire network within the financial system, coupled with the high degree of potential systemic financial cyber risk stemming from the threat of quantum decryption and manifesting through liquidity cascades, our analysis demonstrates that a quantum computer hack of a bank's access to Fedwire would result in declines in annual real GDP ranging from over 10 percent in the baseline scenario to 17 percent in the maximum impact attack, from the initial attack scenario through the resulting six-month recession. As we have summarized in table 5 and represented graphically in figures 14 and 15, our results indicate that such a decline in aggregate output would comprise $2–$3.3 trillion in indirect losses alone, as measured by GDP-at-risk.[120] Moreover, in all the scenarios we modeled, the jolting decline of GDP from the quantum hack of Fedwire would plunge the US economy into a minimum of a six-month recession.

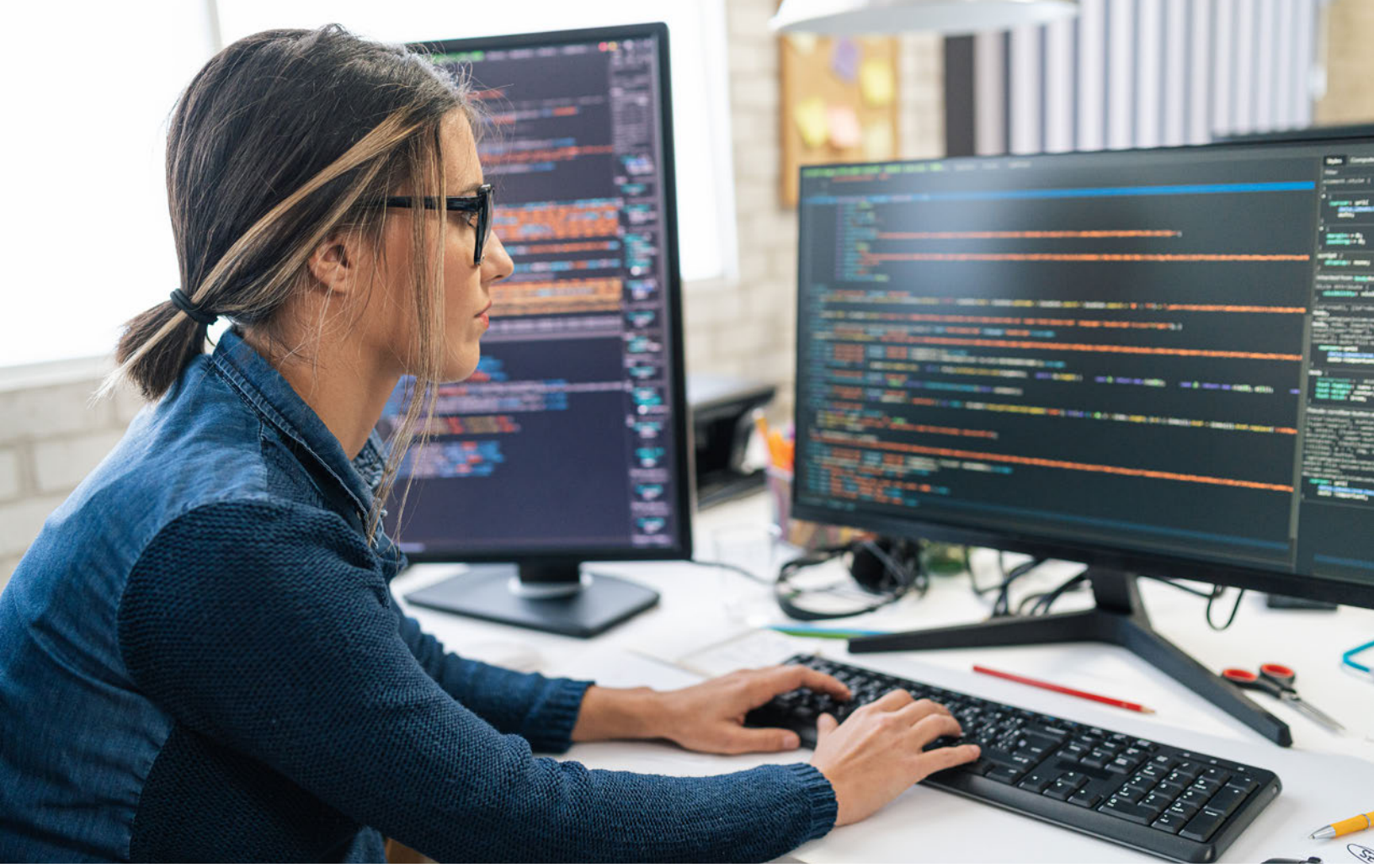
Figure 14: Projected US GDP after a Quantum Computer Cyberattack Impairing Fedwire



Source: Based on data from Oxford Economics.

Although our analysis relies on a number of assumptions as well as on extrapolated data and information, our results likely underrepresent the impacts such a catastrophic event would produce as we limited our estimations to a closed US financial system. If a cyber incident of the scale we depicted even in our mere

baseline were to unfold, the vast international ties within the global financial system would undoubtedly augment contagion and reverberation effects. Overall, our results demonstrate that the quantum-enabled impairment of Fedwire, or of any other RTGS system or key FMI, would result in catastrophic financial losses for the national economy. It could launch us into the next Great Depression due to the intensity and duration of the first-, second-, and third-order indirect impacts originating from a liquidity black hole and from an undersecured nationally critical infrastructure: our interbank payment system, Fedwire Funds Service.



9. RISK MITIGATION

Key Takeaways:

- Without coordination mechanisms and industry-wide minimal requirements, including those set by government regulation, the private market will underinvest in defensive preparations—leaving our financial sector, and thus the entire economy, exposed to the quantum decryption threat.
- Some quantum cybersecurity solutions utilize the physical properties that enable quantum computation. These entanglement-based cryptographic methods, including quantum-key distributions (QKD) and quantum random number generators (QRNG), provide novel capabilities in to improving current security protocols.
- Previous encryption standardization and cryptographic migration efforts, such as those led by NIST leads—including the migration from DES to the current AES algorithm for symmetric-key encryption—suggest that it takes at least a decade to replace widely deployed cryptography.

> Because attacks continue to grow in sophistication, even the best cyber controls will not be able to stop all determined attackers.
>
> —Loretta J. Mester[121]

The US government has designated financial services infrastructure as critical to national and economic security. Given the lack of substitutability and the role of key digital traffic hubs in the financial

Photo: (Getty Images)

system—such as Fedwire and other RTGS systems—not only are such interbank payment systems potential hubs for financial contagion, but their quick replacement may also be a practical impossibility, hindering efforts to achieve a speedy recovery for the financial system as a whole. To be effective, cybersecurity efforts require mechanisms for preventing successful attacks, limiting their impact, and promoting a quick, reliable recovery.

Currently, there exists a classical public goods dilemma in systemic financial cyber risk: because individual firms must handle the costs associated with protecting their own data and networks, and because of network externalities associated with contagion spillovers in both the cyber realm and financial system, banks and other financial actors cannot reap the full benefits of their own cybersecurity investments.[122] This weakest-link security formulation implies that investment in cybersecurity generates positive externalities for all banks. Therefore, the marginal product of investment in cybersecurity is also higher for banks that invest at a lower level than the market or network average. As a bank balances the marginal benefit and cost of cybersecurity when choosing its investment level, the bank has an incentive to free-ride on the higher levels of cybersecurity of others within the network.[123] Resultantly, as individual firms do not internalize the spillover effects that their own inadequate cybersecurity imposes on other banks and on the broader economy (or conversely, as individual firms cannot capture the full benefits of their defensive investments), banks and other financial institutions lack the private incentive to invest in cybersecurity and operational resilience at the systemically optimal level, thereby implying the under-provision of the public good.[124] Without coordination mechanisms and industry-wide minimal requirements, including those set by government regulation, the private market will underinvest in defensive preparations—leaving our financial sector and thus the entire economy exposed to the quantum decryption threat.

The solutions to this quantum threat to financial stability, as analyzed above, are as complex as the dilemma at hand. Yet, paramount to mitigating this risk is the overarching approach that economists Stephen Cecchetti and Kermit Schoenholtz best summarized in their 2018 essay on the acclaimed blog *Money, Banking, and Financial Markets*:

> To stay competitive, firms and regulators will need to anticipate and focus on *prospective* risks, rather than merely ensure compliance with rules that address past incidents. Most important, they will need to avoid the kind of "failure of imagination" that the 9/11 Commission cited as one of the key sources of U.S. vulnerability to that attack. The rapid changes in both technology and the financial system bring not only new opportunities, but the possibility for previously unimagined catastrophes as well.[125]

Nonetheless, there are important lessons to learn from past incidents and apply to the threats that this report anticipates and analyzes. First, engineers need to build resilience into both the cyber and financial systems. Yet, importantly, cybersecurity regimes that both anticipate and safeguard against the risk of quantum decryption have to reinforce both cyber and financial resilience. Such cybersecurity mechanisms exist today in the form of quantum-safe encryption, quantum key distribution, or other post-quantum and quantum-based cryptographic methods.

Some of these quantum cybersecurity solutions utilize the very physical properties that enable quantum computation. These entanglement-based cryptographic methods, including quantum key distributions (QKD) and quantum random number generators (QRNG), provide novel capabilities to improve current security protocols.

As we detailed in our April 2022 report, "a random number is generated by a process with a completely unpredictable outcome whose outcome cannot be reliably reproduced using the same process."[126] The generation of such random numbers forms the foundation for nearly all current cryptographic pro-

cesses, although the formulation of true randomness is a computationally hard task. Consequently, experts have linked many malign cyber intrusions and hacks to insufficiently random cryptographic keys. Yet, as we described above, the unique properties of quantum physics and subatomic particles are inherently random. In this manner, the first entanglement-based solution, QKD, represents a novel approach to distributing quantum-generated random numbers in the form of secure keys between separate locations on a trusted point-to-point basis.[127]

The second solution is quantum random number generators, entanglement-based devices that generate truly random numbers for encrypting messages and other cryptographic keys by integrating this inherent quantum-physical randomness.[128] Some post-quantum cryptography and cybersecurity companies are already introducing QRNGs to their security catalogs. Thus, the straightforward introduction of QRNGs to current security regimes is the logical first step in improving cryptographic key randomness and improving quantum security now.

Another security solution is post-quantum cryptography. Although the method is based on classical computation, government and academic researchers alike are working on classical cryptographic methods to improve the security of existing software-based signatures and key exchanges to maintain their viability in the coming post-quantum era.[129] Various products available for operational deployment today incorporate aspects of different classical algorithms to create hybrid cryptographic solutions. Although the ultimate test for these post-quantum and hybrid solutions will be the introduction of a sufficiently powerful QC, the US government has been testing and implementing a set of quantum-resistant algorithmic standards since 2016. Despite numerous setbacks and the historical precedent for lengthy cryptographic migrations, NIST hopes to complete and begin rolling out these QRA standards by 2024.[130]

However, previous encryption standardization and cryptographic migration efforts, such as those NIST leads—including the migration from DES to the current AES algorithm for symmetric key encryption—suggest that replacing such widely deployed cryptography takes at least a decade.[131]

The migration to quantum-resistant algorithms and other quantum-safe cybersecurity mechanisms is likely to be a much more lengthy and complex process given the ubiquitous use of AES throughout US government networks and systems, including Fedwire. Therefore, even once NIST announces the standardization of a quantum-safe algorithm, and if all product providers made their software quantum-resistant, the migration of critical infrastructure networks, including Fedwire and other RTGS systems, would take an urgent and orchestrated public-private effort for timely achievement. Furthermore, once the time-consuming migration process is finally underway, government agencies and private institutions alike will need a different approach to cyber risk management and the formation of financial system and cyber network resilience as a stopgap in the interim. Therefore, in focusing on prospective threats and anticipating systemic financial cyber risk, market participants and regulators alike need to utilize the emerging quantum-enabled class of cybersecurity protocols to implement resilience measures. These mechanisms vary from the technological to the regulatory as we have reviewed below.

Following a wide-scale disruption to the US financial system, like that which occurred on September 11, 2001, the rapid recovery and resumption of core clearing and settlement activities—such as those provided by Fedwire and other RTGS systems that support financial markets—is critical to the containment and the resolution of systemic risk. Further analyzing systemic risk in the Fedwire network from a game-theoretical perspective, Morten Bech and Rod Garratt highlight Fedwire's critical role in maintaining the resilience of the financial system itself and of its participants, given its core function within the clearing and settlement process. Within this critical role, the authors detail the vital function of Fedwire in coordinating the transmission of payments between banks in its daily operations.[132] They con-

clude that policymakers' ability to maintain Fedwire's smooth functioning and thus to sustain this coordination, "where banks tend to settle promptly and synchronize their payment activity, can potentially be instrumental in mitigating the impact of a wide-scale disruption to the financial system."[133]

Accordingly, the US government can preserve this coordination through various policy approaches to both facilitate the smooth flow of payments and preserve liquidity levels. Firstly, the paper emphasizes the role of liquidity injections in aiding policymakers' ability to preserve interbank coordination. Hence, Bech and Garratt argue that the ability of banks within the Fedwire network to maintain payment coordination, and therefore to avoid widespread systemic risk contagion, depends critically on the relative cost of liquidity and the cost of postponing payments. With this in mind, the paper details how the Federal Reserve implemented its policy response of providing unprecedented amounts of liquidity to the financial system at little or no cost on September 11, 2001, to minimize the risk of banks withholding payment processing, and ultimately to preserve the pre-crisis level of interbank coordination in clearing and settling payments. Simply put, "The cheaper the liquidity, the more likely banks will be to maintain coordination by themselves."[134]

Moreover, the paper underscores the pivotal role large banks fulfill in maintaining both the flow of payments and liquidity coordination between banks. Accordingly, if the Federal Reserve can ensure the survival and solvency of the largest players in the Fedwire system, it can thereby support the smooth functioning of Fedwire given the large share of payments concentrated among the largest banking institutions. In conjunction with or as an alternative to liquidity injections by the central bank, if the Fed can "persuade the large banks to wait for small banks to resume timely processing following a disruption, then more drastic measures . . . might not be required to restore coordination."[135] Although Bech and Garratt conclude that the Fed can achieve this persuasion via an appeal to morality, more rigid operational requirements or regulation may be more reliably effective than "moral suasion" alone in preserving interbank coordination, especially when it is the large banks that a wide-scale disruption may impair, as is the case in our analysis. To that end, economists at the Bank of Spain noted in a 2021 journal article addressing cyber risk and financial stability that liquidity injections may fail to prevent contagion during a systemic event "if a critical financial market infrastructure suffers a cyber-incident that forces it to cease operations for a prolonged period."[136] Stressing the speed and scale at which a cyber disruption to a key FMI or RTGS system can metastasize throughout the financial network, Francisco Luque et al. reckon that existing central bank policy tools may be inadequate and insufficient for mitigating systemic risk events given the "uncertainty of the origin, intent and impact of a cyber-incident" in scenarios such as a quantum-induced disruption to Fedwire.[137] Eisenbach et al. reiterate this point, noting that "due to the unique properties of cyber events, traditional policy tools such as ex ante capital requirements or ex post liquidity provision may not be as effective" at mitigating a systemic event in the financial sector.[138]

Consequently, in scenarios such as the Fedwire disruption analyzed herein, the Fed should consider new policy options that allow for a pause or otherwise give affected systems and impaired institutions time to recover. Moreover, Eisenbach et al. consider how regulatory requirements such as the liquidity coverage ratio (LCR) "could be temporarily suspended if banks are technologically unable to address violations, limiting the knock-on effects of perceived impairment."[139] If authorities communicate such regulatory responses well throughout the financial sector, banks will have a reduced incentive to hoard liquidity and will encourage the timely fulfillment of payments and other obligations, helping to stabilize the entire financial system in the face of a disruption. In addition to diminishing the incentive to hoard capital and otherwise facilitating institutional coordination across the Fedwire system, the suspension of the LCR is "equivalent to an instant injection of several trillion dollars of reserves into the system," further alleviating liquidity pressures throughout the network.[140]

A distinguishing characteristic of cyber events, especially within complex cyber-physical networks such as the financial sector, is the information asymmetries arising from strategic uncertainty within financial institutions. Not only do such asymmetries catalyze coordination failures in the face of a market disruption, but the lack of systemic communication and information sharing hinders threat analysis and increases intervention and mitigation uncertainty from both the micro- and macro-prudential policy perspectives. Therefore, as Eisenbach et al. and other researchers have noted, "requirements to disclose to regulators even minor cyber events or to share with other banks information on threat assessments and contingency plans could increase resilience by . . . improving collective learning" within the financial system.[141] However, as policies dealing with information sharing and event disclosure have proven insufficient in preventing coordination failures when network participants alone endogenously determine them, legislative frameworks and regulatory oversight by the Federal Reserve or other agencies may be necessary for the design and maintenance of such communication protocols.[142]

Additionally, engineers can implement technological safeguards at both the firm and system levels to guarantee operational resilience and reduce the impact of data availability and integrity events. Such measures would include dedicated network backup sites and other security and operational redundancies. However, due to the systemic externalities and public-good investment failures we addressed above, the individual cost of backup facilities and other technological redundancies within the networks of core FMIs would likely outweigh the individual benefits that banks and other institutions would reap. Thus, ex ante public provision will likely be necessary for building such resiliency mechanisms.[143] Finally, to ensure timely coordination and proportional responses, policymakers and regulators should design these policy and regulatory responses to trigger automatically in incremental levels relative to the severity of the disruption.

Fundamentally, it is paramount for the financial system to institute both operational and cyber resilience. It needs to create and implement backups; institutional and technological redundancies; clear and quick information sharing, threat detection, and response coordination mechanisms; and automatic policy and operational contingency plans that both participants and regulators collectively design, systemically deploy, and institutionally know. This measure will prevent the failure of a single bank or groups of banks and critical FMIs, such as Fedwire, from becoming a catastrophic, system-wide failure.

However, these policy solutions are effective only when the Federal Reserve can identify a cyber disruption. More troubling are scenarios, such as the quantum-enabled cyberattack we outlined above, in which an intrusion is undetected or seemingly legitimate, communication is limited, and uncertainty perpetuates throughout an irresponsive financial system.

As Cecchetti and Schoenholtz conclude in a later essay, "Ultimately, we are in an arms race against malicious actors. No mechanism to prevent and mitigate attacks will be successful unless it anticipates hostile innovations."[144] Currently, the next hostile innovation is quantum-enabled decryption of critical financial networks and infrastructures. Our institutions have already anticipated this threat. However, they have yet to institutionally and systemically implement the known technological mechanisms capable of preventing this "hostile innovation" in the financial sector.

Consequently, we are at an inflection point—one where our collective financial, economic, and national security hangs in the balance. Absent the system-wide adoption and implementation of quantum-safe encryption, quantum key distribution, or other post-quantum cryptography, our mighty financial system will remain under threat and our economic security at stake as the quantum future takes shape. Regardless of financial and technological resilience, it is up to both regulators and market participants to take on this known threat and win the quantum arms race.

10. CALL TO ACTION AND CONCLUSION

> Cybersecurity is a public good: the overall financial system conveys benefits to us all. . . . The social benefit conveyed by a well-functioning and resilient financial system, one in which the public can continue to have a lot of confidence, likely requires a higher level of investment in cybersecurity than what individual firms would decide to do on their own. . . . The public good aspect of cybersecurity and the Federal Reserve's role in ensuring the resiliency of the financial system mean that the Fed has a role to play in helping the financial services industry improve its ability to prevent, detect, and recover from cyber-attacks.
>
> —Loretta J. Mester[145]

Through our qualitative and quantitative analysis, we demonstrate how a single quantum attack on one of the five largest US financial institutions (by assets), aimed at their access to the Fedwire Funds Service payment system, could trigger a cascading financial failure costing the US economy anywhere from $2 trillion to $3.3 trillion in indirect impacts alone. Indeed, a QC attack could impair approximately 62 percent of total assets in the banking system due to bank runs and endogenous liquidity traps.

Critics wave these estimates away by insisting that QCs capable of this kind of threat are—according to the experts—at least a decade away. The problem is that getting quantum-secure, including analyzing which data and networks need protection most and which legacy cybersecurity systems need

Photo: Customers use the ATM machines at a JPMorgan Chase bank in Midtown in New York on April 28, 2015. (Photo by Richard Levine/Corbis via Getty Images)

not only patched but completely replaced, can take almost as long.

At the same time, new developments in quantum science suggest that this complacency about the quantum threat timeline is misplaced. So-called quantum annealers, like those Canada-based D-Wave Systems, Inc. uses, are able to calculate the lowest energy level between the qubits' different states of entanglement, which equals the optimal solution.[146] These machines have proven their worth in solving optimization problems that usually stump classical computers.

Not surprisingly, scientists have been quietly finding ways to turn factorization into an optimization problem instead of relying Shor's algorithm, the paradigm for discussing quantum decryption since the 1990s. In 2019, scientific papers emerged that showed how to do this, including factorizing integers using "noisy" qubits (i.e., swarms of quantum bits that aren't perfectly entangled the way a large-scale computer requires).[147]

More recently, a paper published by 24 Chinese scientists claims they have devised an algorithm that could crack a very hard encryption nut (i.e., 2,048-bit RSA) using a 372-qubit quantum computer.[148]

While those claims have generated controversy, previous studies done using hybrid systems suggest the Chinese approach is directionally correct (i.e., that a large-scale quantum computer is not necessary for doing effective decryption but that it is at least theoretically possible at this stage to factorize large prime numbers using today's error-prone "noisy" quantum computers). This development can dramatically accelerate the timeline to a tangible quantum threat to existing encryption systems.

For these reasons, we can recommend a four-step program to protect Fedwire and related systems from the future quantum computer threat.

The *first step* is adopting the NIST PQC standards for Fedwire protection with a clear timeline for implementation and replacement of legacy encryption systems.

The *second step* is for the chair of the Federal Reserve to call a Quantum Security Summit involving America's largest banks and financial institutions to insist they start laying out plans for becoming quantum-secure.

The *third step* is for Congress to set a deadline for all 12 Federal Reserve banks to be quantum-secure. Now that NIST has its first select group of quantum-resistant algorithms, it is time for the government and Congress to make the private financial sector adopt those standards, and other mitigating technologies, to protect against the QC threat. That legislation should include a timeline for checks on implementation similar to NSM-10 for federal agencies.

The *fourth step* is to create a quantum security taskforce at the Federal Reserve to oversee and implement the timeline. Such a taskforce should include both cyber and financial industry experts, as well as advisors familiar with quantum computing and quantum-based cryptography. Its mandate should be subject to annual renewal, based on progress made toward quantum readiness and new developments in quantum technology.

APPENDIX A: GRANGER CAUSALITY AND OLS REGRESSION METHODOLOGY

To both establish the presence and quantify the degree of a relationship between Fedwire transaction value and GDP growth rates, we employed two separate econometric analyses: the Granger causality test and multiple ordinary least squares regressions. Both analyses utilized quarterly data beginning in 2005 Quarter 2 and ending in 2021 Quarter 4 due to data availability across all variables of interest. Specifically, those variables were growth in the Fedwire Funds Service quarterly value, US Gross Domestic Product chained quantity index, the ICE BofA US High Yield Index Option-Adjusted Spread, the Chicago Board Options Exchange Volatility Index (VIX), and the Yale School of Management Stock Market Confidence Index.

In accordance with contemporary econometric protocol, we tested all variables for stationarity, a statistical condition that affects the accuracy of time-series data modeling. We implemented multiple contemporary tests to assess the presence of a unit-root in the data, which makes the data non-stationary. Stationarity is desirable as it allows for accurate and consistent estimation. We determined that all variables were stationary at levels. Next, we utilized the Schwarz information criterion for optimal lag selection of the variables. With optimal lag selection established, we ran the Engle Granger augmented Dickey-Fuller test for cointegration, determining that no cointegration existed between Fedwire and the explanatory variables. In regression analysis, the endogenous variable is the one we are trying to explain or predict through the explanatory variable. That is, we are estimating the effect of the explanatory variable(s) on the endogenous (Fedwire) side of the equation.

With these tests concluded, we conducted the Granger test for statistical causality, which tests for the predictive causality between two data sets. We found that growth in quarterly Fedwire transaction value does indeed Granger-cause, or lead, quarterly growth in US GDP during the period examined. Whereas standard econometric regressions test only for correlation rather than theoretical causation, Granger causality, or precedence, "is a circumstance in which one time-series variable consistently and predictably changes before another variable."[149] In this way, it is more apt to call tests of Granger causality "predictive causality tests," as the statistical findings test whether *x* forecasts changes in *y* rather than assessing true theoretical causation. For more information, please see Granger's 1969 research.[150]

With the direction of precedence established between Fedwire and aggregate output, we performed simple univariate OLS regressions to quantify this relationship and that of the other abovementioned variables with Fedwire. As the relationships between our financial market variables—quarterly change in proxies for liquidity, financial market volatility, and market confidence—and GDP are well established in both theory and existing literature, we can confidently assume that if Fedwire is a determinant of GDP growth, as the Granger causality results establish, a similar relationship exists between Fedwire and our other explanatory variables. For all estimations, we employed a trio of statistical tests to ensure the estimated regressions were free of serial correlation in addition to having other statistically desirable characteristics. Serial correlation, also known as autocorrelation, is a statistical issue that causes bias in the standard errors of the coefficients, potentially leading to biased or erroneous conclusions about the statistical significance of the explanatory variables.

We utilize two methods of testing for first-order serial correlation, the Lagrange multiplier statistical test and the Durbin-Watson statistic. The latter is extremely useful for determining whether a regression is free of autocorrelation, as a DW statistic in and around 2.0 indicates an absence of serial correlation. In addition to testing for serial correlation, we implemented the Breusch-Pagan-Godfrey and Jarque-Bera tests for heteroskedasticity and normal distribution of the residuals of the regression. In addition to the Durbin-Watson statistics, we also report the R-squared and adjusted R-squared measures for each regression. In general, R-squared, or the coefficient of determination, is a statistical measure for the goodness of fit for a given model: the higher the value, the better the model depicts the propor-

tion of variance in the dependent variable that the independent variable can explain.

Our findings, as reported in tables 2 and 3, indicate that the relationship between quarterly growth in Fedwire transaction value and US GDP is both positive and statistically significant, where a 1-unit increase in the growth rate of Fedwire transaction value leads to a 0.39-unit increase in quarterly GDP growth a quarter later, and to an additional increase of 0.23 units the following quarter, all else equal. As with all coefficients from regression estimation, the condition of ceteris paribus holds in this relationship. Holding all other variables constant, a change in a single explanatory variable alone will yield a given change in the endogenous variable. This principle is implied for all other estimations, and we have outlined their results in the remainder of this paper. Conversely, we determined the relationship between Fedwire growth and the other financial variables is negative and of varying levels of significance. As we noted in tables 2 and 3, *** indicates a 1 percent significance level, and given the descending scale of statistical significance, the lower the level, the greater the significance of a variable.

Full results of the statistical tests we employed in this section, the regressions, and the diagnostic tests we utilized are available upon request. We have reported the derived elasticities for each analyzed variable in table 3 in the text. The results from this section enabled us to further analyze the relationship between Fedwire and the selected variables, to calibrate the Oxford Economics GEM, and to derive the indirect costs of the various attack scenarios analyzed.

APPENDIX B: OXFORD ECONOMICS GEM SHOCK CALIBRATION METHODOLOGY

To accurately capture the indirect impacts of a quantum hack of Fedwire, we implemented a total of seven shocks to four variables within the GEM: GDP, credit conditions, the VIX index, and equity prices. By shocking equity volatility, equity prices, and credit conditions, we captured the effects that such systemic financial contagion would have on economic confidence, the stock market, and ultimately the US economy. We carefully calibrated each of the shocks utilizing the regression coefficients from appendix A and table 3, which we then related to the dollar amount of impaired Fedwire transfers and the amount of aggregate bank assets. We represent these figures in terms of shocks to GDP, liquidity, market volatility, and market confidence and of prices applicable to the Oxford Economics' GEM to calculate the total costs of varying degrees of attack scenarios. We calibrated each of the shocks using our two-staged economic analysis, which correlated our regression analyses with the network impairment effects of Eisenbach et al. Furthermore, we scaled all GEM shocks to reflect varying degrees of five different attack scenarios based on the literature. Below we discuss the four variables and outline the methodology we utilized to calibrate shocks to the GEM. Further details about the calibration methodology, specifically the regression-based elasticities, are available in appendix A and upon request.

GEM Variables Shocked

The first variable we examined was gross domestic product, which represents the immediate first-order impact that a decline in Fedwire transaction value would have on gross output in the economy as indicated by our analysis in appendix A. Furthermore, after analyzing the other financial variables, we shocked GDP again to capture the second- and third-order impacts that the scenarios would have on the aggregate economy. As our analysis focused only on indirect impacts of the scenarios, the shocks to GDP help us bridge the impacts from the attack on Fedwire to the broader economy while not specifically addressing direct impacts.

Next we analyzed the VIX index, an indicator of US and global financial market volatility that the Chicago Board Options Exchange maintains; it is the option-implied volatility of the S&P 500 over the following 30 days. Shocks to the VIX are a useful tool for simulating short and sharp exogenous shocks to financial market volatility, economic confidence, and aggregate demand.

In addition to the VIX, we implemented shocks to equity prices. An equity shock within the GEM simulates exogenous shocks to the equity markets that are then transmitted to both the financial markets and the real economy. This variable directly affects the cyclically adjusted price-to-earnings ratio, which feeds through to the final value of the model's share price index. Such a shock is akin to an exogenous shock to equity risk premia and introduces significant international and real economy contagion spillovers. This shock effect spills over into business and consumer confidence, leading to greater aggregate economic impacts in addition to the general wealth effects that depressed equities imply.

Finally, the fourth model variable we shocked was credit conditions in the GEM. This variable, an index reflecting the availability of credit throughout the economy, generates exogenous shocks with effects akin to depressed levels in the credit supply. Credit conditions directly impact consumption, investment, and equity prices in the model. Additionally, this shock introduces recession effects to the housing sector.

Shock Calibration

Given the irreproducibility of the Eisenbach et al. results, the representation of their findings in terms of percentage of impaired assets and the use of non-public data hinders supplementary analysis, which often (as in this case) requires dollar amounts for calculations and calibration for the GEM shocks. Consequently, we implemented a reverse-engineering or bootstrap methodology to extrapolate an approximate dollar amount for the average daily value of Fedwire transactions that an attack would impair in the baseline scenario that Eisenbach et al. described. Beginning with the summary statistics of daily payments value transferred in Fedwire in 2018 and the distribution of total Fedwire payments by bank size in 2018, as detailed in tables B.1

Table B.1: Summary Statistics of Daily Payments Value in Fedwire, 2018

SUMMARY STATISTICS. THE TABLE SHOWS AVERAGE DAILY VALUE OF FEDWRIE TRANSFERS BY PERCENTILE DISTRIBUTIONS OF ALL BANKS IN US AS WEIGHTED BY TOTAL ASSET SIZE.							
	AVG.	ST. DEV.	P1	P25	P50	P75	P99
Total Sent i,t (Millions)	519.94	9588.86	0	0	0.37	3.16	7242.9
Avg. by Institution i (Millions)	508.75	9318.75	0	0.15	0.86	4.29	7818.85
Total on Day t (Trillions)	2.85	0.32	2.32	2.63	2.81	3.02	3.73

Source: Eisenbach et al., 2021, 15.

Table B.2: Distribution of Total Fedwire Payments by Bank Size

GROUP OF BANKS	PERCENTAGE OF TOTAL FEDWIRE PAYMENTS BY VALUEV
Top 5 Banks	50%
Top 10 Banks	60%

Source: Based on data from Eisenbach et al., 2021, 11.

and B.2 and found within the Eisenbach et al. report, we can relate this information to the total number of banks in the US at the end of 2018 by making some simplified assumptions.

As the Federal Reserve has reported, there were approximately 1,807 banks in the US with a positive account balance at the end of 2018. Given the information in table B.1, we know that the 99th percentile corresponds to 1 percent of all banks in 2018, which is 18.7 banks. For simplicity of calculation, we round this figure up to 20, which gives us an approximation of the number of banks in the 99th percentile from table B.1. This grouping represent the top 20 banks by asset size in 2018, which are available publicly from the Federal Reserve and which we have listed in table B.3.

By taking the summary statistics of this group of 20 banks from table B.3, we can derive the percentile distribution of 2018 averages of total bank assets for the top 20 banks in 2018. We present this information in table B.4, where the 75th percentile accounts for the top 25 percent of this group and thus corresponds to the top five banks in 2018. As we have detailed in table B.4, the top five banks by asset size in 2018 held $412,111.10 million on average.

Then, taking the total value of Fedwire transfers originated in 2018 from table B.5, which from publicly available data is known to be $716,211,759.00 million, and knowing that the top five banks by asset size accounted for roughly half of these transfers (table B.2), we can multiply the two figures to derive the approximate value of Fedwire transfers from the top five banks in 2018. As we have detailed in table B.5, we estimate this figure at approximately $358,105,879.50 million.

With the approximate value of Fedwire transfers sent by the top five banks now known, we then take the sum of the total 2018 average of consolidated assets for the top five banks in 2018, which we have calculated using publicly available data and tabulated in table B.6. Thus, the sum of 2018 average consolidated assets for the top five banks in the US was $7,519,577.00 million, which is our proxy for the average size of the top five banks by assets in 2018.

Table B.3: Top 20 Banks (by Assets in Millions of USD, 2018)

CORRESPONDS TO P99 OF EISENBACH, ET AL. (2021) FEDWIRE TRANSFERS		
BANK NAME / HOLDING CO NAME	BANK ID	2018 AVERAGE ASSETS
JPMORGAN CHASE BK NA/JPMORGAN CHASE & CO	852218	$2,194,947.75
BANK OF AMER NA/BANK OF AMER CORP	480228	$1,776,323.00
WELLS FARGO BK NA/WELLS FARGO & CO	451965	$1,686,522.00
CITIBANK NA/CITIGROUP	476810	$1,406,592.50
U S BK NA/U S BC	504713	$455,191.75
PNC BK NA/PNC FNCL SVC GROUP	817824	$369,030.50
T D BK NA/TD GRP US HOLDS LLC	497404	$295,893.00
CAPITAL ONE NA/CAPITAL ONE FC	112837	$293,744.75
BANK OF NY MELLON/BANK OF NY MELLON CORP	541101	$283,362.50
STATE STREET B&TC/STATE STREET CORP	35301	$241,361.50
BRANCH BKG&TC/BB&T CORP	852320	$216,677.75
SUNTRUST BK/SUNTRUST BK	675332	$204,320.25
GOLDMAN SACHS BK USA/GOLDMAN SACHS GROUP THE	2182786	$179,990.00
HSBC BK USA NA/HSBC N AMER HOLDS	413208	$175,197.00
ALLY BK/ALLY FNCL	3284070	$150,078.25
MORGAN STANLEY BK NA/MORGAN STANLEY	1456501	$141,601.00
FIFTH THIRD BK/FIFTH THIRD BC	723112	$140,682.75
KEYBANK NA/KEYCORP	280110	$136,483.25
NORTHERN TC/NORTHERN TR CORP	210434	$131,869.00
CHASE BK USA NA/JPMORGAN CHASE & CO	489913	$130,473.75

Source: Based on data from the Federal Reserve and corresponding to data in Eisenbach et al., 2021, 99.

Table B.4: Summary Statistics and Percentiles of Top 20 Banks in 2018 by Assets

AVERAGE DAILY VALUE OF FEDWIRE TRANSFERS BY PERCENTILE DISTRIBUTION OF THE TOP 20 BANKS IN U.S. IN 2018								
	OBSERVATIONS	AVERAGE	STD. DEV.	P1	P25	P50	P75	P99
Average by Institution *i* (millions)	20	$530,517.10	$652,524.40	$130,473.80	$145,839.60	$229,019.90	$412,111.10	$2,194,948.00

Source: Based on data from the Federal Reserve.

Table B.5: Value of Fedwire Transfers (Millions of USD)

YEAR	TOTAL VALUE OF TRANSFERS ORIGINATED	AVERAGE DAILY VALUE OF TRANSFERS SENT	APPROXIMATE VALUE OF FEDWIRE TRANSFERS SENT BY THE TOP 5 BANKS (BY ASSETS)
2018	$716,211,759.00	$2,853,433.00	$358,105,879.50

Source: Based on data from the Federal Reserve and Eisenbach et al., 2021.

Table B.6: Total 2018 Consolidated Assets for the Top 5 Banks by Assets (Millions of USD)

BANK NAME / HOLDING CO NAME	NAT'L RANK	BANK ID	2018 Q1	2018 Q2	2018 Q3	2018 Q4	2018 ANNUAL AVG.
JPMORGAN CHASE BK NA/ JPMORGAN CHASE & CO	1	$852,218.00	$2,198,296.00	$2,167,700.00	$2,194,835.00	$2,218,960.00	$2,194,947.75
BANK OF AMER NA/BANK OF AMER CORP	2	$480,228.00	$1,765,242.00	$1,759,530.00	$1,797,881.00	$1,782,639.00	$1,776,323.00
WELLS FARGO BK NA/ WELLS FARGO & CO	3	$451,965.00	$1,716,532.00	$1,675,077.00	$1,665,128.00	$1,689,351.00	$1,686,522.00
CITIBANK NA/CITIGROUP	4	$476,810.00	$1,406,778.00	$1,397,794.00	$1,415,081.00	$1,406,717.00	$1,406,592.50
U S BK NA/U S BC	5	$504,713.00	$452,256.00	$453,023.00	$456,011.00	$459,477.00	$455,191.75
Sum of Total 2018 Average Consolidated Assets for the Top 5 Banks in US (Millions)							$7,519,577.00

Source: Based on data from the Federal Reserve.

Dividing the average top-five bank size in table B.6 by the approximate value of Fedwire transfers sent by the top five banks (from table B.5) yields the approximate elasticity of bank assets to Fedwire transfers for the top five banks in 2018, which is 2.1 percent or 1.021. Next, by multiplying this assets-Fedwire elasticity by the average daily value of Fedwire transfers sent by the top five banks, found in the 75th percentile in table B.4, we derive the average daily value of Fedwire transfers for the top five banks in 2018. This figure, which is roughly $420,765.433 million as we have reported in table B.7, approximately equals the total average value of Fedwire transfers that the baseline scenario outlined in Eisenbach et al. would impair when an attack on a single top-five bank occurs and the bank can receive but not remit payments via Fedwire.

Then, taking the above dollar-denominated figure and dividing it by the average daily value of transfers sent over Fedwire in 2018, or $2,853,433.00 million in table B.5, we arrive at the percentage of Fedwire transfers that the Eisenbach et al. baseline scenario would impair, which is approximately 15 percent as we have reported in table B.7. Next, we take the regression coefficients for the various variables from table 3 in the text (and appendix A) and multiply them by 15 percent to yield the corresponding equivalent to the amount of Fedwire transfers impaired as a percentage shock to the matching GEM variable.

Finally, by multiplying these GEM multipliers, which we detailed in table 4 in the text, by the corresponding extrapolated percentage of impaired bank assets relative to the various scenarios that Eisenbach et al. described, we derive a given GEM variable's shock level. We have tabulated these final shock percentages in table 4 in the text.

Thus, through the above bootstrap methodology, we have successfully extrapolated the value of the top five banks' average daily Fedwire transfers and related the percentage results of the Eisenbach et al. paper in terms of dollar amounts of impaired payments. From there, we applied the regression coefficients from table 3 (explained in appendix A) to relate the dollar amount of impaired Fedwire transfers to the amount of aggregate bank assets and to represent these figures in terms of shocks to GDP, liquidity, market volatility, and market confidence and prices applicable to the Oxford Economics GEM to calculate the total indirect costs of varying degrees of attack scenarios. We present the results of this derivation in table 4 of the text.

ENDNOTES

1 Jerome Powell, "Jerome Powell: Full 2021 *60 Minutes* Interview Transcript," interview by Scott Pelley, *60 Minutes* CBS, April 11, 2021, https://www.cbsnews.com/news/jerome-powell-full-2021-60-minutes-interview-transcript/.

2 Michael J. D. Vermeer and Evan D. Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption* (Santa Monica, CA: RAND Center for Global Risk and Security, 2020), https://www.rand.org/pubs/research_reports/RR3102.html.

3 Arthur Herman, *Advancing the Quantum Advantage: Hybrid Quantum Systems and the Future of American High-Tech Leadership*, policy report, Quantum Alliance Initiative (Washington, DC: Hudson Institute, 2022), https://www.hudson.org/innovation/advancing-quantum-advantage-hybrid-quantum-systems-future-american-high-tech-leadership.

4 Joseph R. Biden, "NSM-8: Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," The White House, January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

5 Biden, "NSM-8: Memorandum."

6 This is true of the government's most recent efforts, the Quantum Computing Cybersecurity Preparedness Act, which President Biden signed into law on December 21, 2022. Although the QCCPA marks an important milestone for government quantum preparedness, it lacks in the areas discussed herein.

7 "Quantum Alliance Initiative," Hudson Institute, 2022, https://www.hudson.org/policy-centers/quantum-alliance-initiative.

8 Hudson Institute, "Quantum Alliance Initiative."

9 Arthur Herman, "Five Eyes on Quantum: Envisioning the Quantum Technology Alliance," Hudson Institute, November 2018.

10 Herman and Butler, *Risking Apocalypse? Quantum Computers and the US Power Grid.*

11 Arthur Herman and Alexander W. Butler, *Risking Apocalypse? Quantum Computers and the US Power Grid*, policy report, Quantum Alliance Initiative (Washington, DC: Hudson Institute, 2021), https://www.hudson.org/national-security-defense/risking-apocalypse-quantum-computers-and-the-us-power-grid.

12 Butler, Herman, and Pagano, *Decrypting Crypto*.

13 Alexander W. Butler, Arthur Herman, and Daley Pagano, *Decrypting Crypto: Cryptocurrencies and the Quantum Computer Threat*, policy report, Quantum Alliance Initiative (Washington, DC: Hudson Institute, 2022), https://www.hudson.org/technology/decrypting-crypto-cryptocurrencies-and-the-quantum-computer-threat.

14 Arthur Herman, "Getting the Big Banks to Confront the Quantum Challenge," *Forbes*, May 26, 2021, https://www.forbes.com/sites/arthurherman/2021/05/26/getting-the-big-banks-to-confront-the-quantum-challenge/?sh=185f874c7385.

15 Jonathan W. Welburn and Aaron M. Strong, "Systemic Cyber Risk and Aggregate Impacts," *Risk Analysis* 42, no. 8 (Aug. 2022): 1606–22, https://doi.org/10.1111/risa.13715; Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, *Cyber Risk and the US Financial System: A Pre-Mortem Analysis*, Staff Reports No. 909 (New York: Federal Reserve Bank of New York, 2021), https://www.newyorkfed.org/research/staff_reports/sr909.html.

16 In our preliminary analysis, all scenarios studied represent a successful cyberattack of increasing magnitudes on the Fedwire Funds Service payment system targeting one of the five largest institutions by assets. In all four scenarios, it is assumed the shocked institution can receive but is unable to remit any payments for a one-day period. Impact is measured in terms of assets impaired in resulting endogenous liquidity traps, foregone payments due to strategic run maneuvering in the network, and through direct operational losses incurred during the initial single-day period alone.

17 Butler, Herman, and Pagano, *Decrypting Crypto*.

18 Anna Zakrzewski et al., *Global Wealth 2019: Reigniting Radical Growth* (Boston: Boston Consulting Group, 2019), https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth.

19 IBM, *X-Force Threat Intelligence Index 2019*, IBM Security (Armonk, NY: IBM Corporation, 2019), 42, https://www.ibm.com/reports/threat-intelligence/.

20 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*.

21 Butler, Herman, and Pagano, *Decrypting Crypto*.

22 Butler, Herman, and Pagano, *Decrypting Crypto*.

23 Arthur Herman and Idalia Friedson, *Quantum Computing: How to Address the National Security Risk*, policy report, Quantum Alliance Initiative (Washington, DC: Hudson Institute, 2018), https://www.hudson.org/national-security-defense/quantum-computing-how-to-address-the-national-security-risk.

24 Jose Deodoro, Michael Gorbanyov, Majid Malaika, and Tashin Saadi Sedik, "Quantum Computing and the Financial System: Spooky Action at a Distance?" (working paper, Asia and Pacific Department, International Monetary Fund, Washington, DC, 2021), https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159.

25 Michael A. Nielson and Isaac L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition (Cambridge University Press, 2010).

26 Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (Santa Fe, NM: IEEE, 1994), 124–34, https://ieeexplore.ieee.org/document/365700.

27 Butler, Herman, and Pagano, *Decrypting Crypto*.

28 Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* [STOC '96] (New York: Association for Computing Machinery, 1996), 212–19, https://dl.acm.org/doi/proceedings/10.1145/237814.

29 Deodoro et al., "Quantum Computing and the Financial System."

30 Deodoro et al., "Quantum Computing and the Financial System."

31 Dylan Herman et al., "A Survey of Quantum Computing for Finance," arXiv, Cornell University, June 27, 2022, 3, https://arxiv.org/abs/2201.02773.

32 Herman et al., "A Survey of Quantum Computing."

33 Herman et al., "A Survey of Quantum Computing"; Deodoro et al., "Quantum Computing and the Financial System."

34 Herman et al., "A Survey of Quantum Computing."

35 Herman et al., "A Survey of Quantum Computing."

36 Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta, and David Whyte, "Covid-19 and Cyber Risk in the Financial Sector," *BIS Bulletin* (Bank for International Settlements), no. 37 (Jan. 2021), https://www.bis.org/publ/bisbull37.htm.

37 Daniel Bernoulli, "Exposition of a New Theory on the Measurement of Risk," *Econometrica* 22, no. 1 (1954): 23–36, https://doi.org/10.2307/1909829.

38 Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention* (Basel, Switzerland: Financial Stability Board, 2017), https://www.fsb.org/wp-content/uploads/R270617.pdf.

39 James J. Cebula and Lisa R. Young, *A Taxonomy of Operational Cyber Security Risks*, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute (Pittsburgh, PA: Carnegie Mellon University, 2010), 1, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395.

40 World Economic Forum, *The Global Risks Report 2022* (Cologny, Switzerland: World Economic Forum, 2022), 49, https://www.weforum.org/reports/global-risks-report-2022/.

41 Kwangmin Jung, "Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk," *North American Actuarial Journal* 25, no. 4 (June 2021): 580–603, https://doi.org/10.1080/10920277.2021.1919145.

42 Financial Stability Board, *Financial Stability Implications from FinTech*.

43 Matteo Crosignani, Marco Macchiavelli, and André F. Silva, *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains*, Staff Reports No. 937 (New York: Federal Reserve Bank of New York, 2021), https://www.newyorkfed.org/research/staff_reports/sr937.

44 Crosignani, Macchiavelli, and Silva, *Pirates without Borders*.

45 Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment" (IMF Working Paper 18/143, Strategy, Policy & Review Department, International Monetary Fund, Washington, DC, June 2018), https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.

46 Bouveret, "Cyber Risk for the Financial Sector."

47 Rustam Jamilov, Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk" (working paper no. 28906, National Bureau of Economic Research, Cambridge, MA, June 2021), https://www.nber.org/papers/w28906.

48 Francisco José Herrera Luque, José Munera López, and Paul Williams, "Cyber Risk as a Threat to Financial Stability," *Revista de Estabilidad Financiera* (Banco de España), no. 40 (Spring 2021): 181–205, https://www.bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/21/7_Cyber_REF.pdf.

49 Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist, "Cyber Mapping the Financial System" (Cyber Policy Initiative Working Paper 6, Carnegie Endowment for International Peace, Washington, DC, 2020), 2, https://carnegieendowment.org/2020/04/07/cyber-mapping-financial-system-pub-81414.

50 Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, "Cyber Risk, Market Failures, and Financial Stability" (IMF Working Paper No. 2017/185, Western Hemisphere and Monetary and Capital Markets Departments, International Monetary Fund, Washington, DC, 2017), 21–22, https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104.

51 Greg Ros, "The Making of a Cyber Crash: A Conceptual Model for Systemic Risk in the Financial Sector" (Occasional Paper Series No. 16, European Systemic Risk Board, Frankfurt, Germany, 2020), 32, https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op16~f80ad1d83a.en.pdf.

52 Ros, "The Making of a Cyber Crash," 36. Procyclicality can be defined as the exacerbation of the degree and impact of fluctuations in economic growth and market prices through individually advantageous actions in the short run that may be detrimental to the agent or in the aggregate over the longer-term evolution of the business cycle.

53 Bobby Vedral, "The Vulnerability of the Financial System to a Systemic Cyberattack," in *Going Viral: 13th International Conference on Cyber Conflict*, edited by T. Jančárková, L. Lindström, G. Visky, and P. Zotz (Tallinn, Estonia: NATO CCDCOE Publications, 2021), 95–110, https://ccdcoe.org/uploads/2021/05/CyCon_2021_Vedral.pdf.

54 Bouveret, "Cyber Risk for the Financial Sector."

55 Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach, "The Drivers of Cyber Risk" (BIS Working Papers No. 865, Monetary and Economic Department, Bank for International Settlements, Basel, Switzerland, 2022), https://www.bis.org/publ/work865.htm.

56 Ros, "The Making of a Cyber Crash," 23.

57 Ros, "The Making of a Cyber Crash," 52.

58 Ros, "The Making of a Cyber Crash," 51.

59 Antonino Fazio and Fabio Zuffranieri, "Interbank Payment System Architecture from a Cyber Security Perspective" (*Questioni di Economia e Finanza* occasional paper no. 418, Economic Research Department, Bank of Italy, Rome, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123094.

60 Brauchle et al., "Cyber Mapping the Financial System," 7.

61 Ponemon Institute LLC, *2018 Cost of Data Breach Study: Global Overview* (IBM and Ponemon Institute, 2018), https://www.intlx-solutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

62 Fazio and Zuffranieri, "Interbank Payment System Architecture," 10.

63 Luque, López, and Williams, "Cyber Risk as a Threat," 203.

64 Anton Badev et al., "Fedwire Funds Service: Payments, Balances, and Available Liquidity" (Finance and Economics Discussion Series 2021-070, Board of Governors of the Federal Reserve System, Washington, DC, 2021), https://www.federalreserve.gov/econres/feds/fedwire-funds-service-payments-balances-and-available-liquidity.htm.

65 Badev et al., "Fedwire Funds Service."

66 As of this writing, Badev et al. provide the only econometric examination of the link between Fedwire payments value and GDP growth rates. This text seeks to expand upon their findings.

67 Whereas standard econometric regressions test only for correlation rather than theoretical causation, Granger causality, or precedence, "is a circumstance in which one time-series variable consistently and predictably changes before another variable" (A. H. Studenmund, *Using Econometrics: A Practical Guide*, London: Pearson Education, 2016). In this way, it is more apt to call tests of Granger causality "predictive causality tests," as the statistical findings test whether *x* forecasts changes in *y* rather than assessing true theoretical causation. For more information, please see C. W. J. Granger, "Investigating Causal Relations by Econometric Models and Cross-spectral Methods," *Econometrica* 37, no. 3 (Aug. 1969): 424–38, https://doi.org/10.2307/1912791). For more information about the methodology and results in this section, please see appendix A.

68 Badev et al., "Fedwire Funds Service."

69 Federal Reserve Banks, "Certification Practice Statement of the Federal Reserve Banks' Services Public Key Infrastructure (Version 1.2)," FRBservices.org, last modified June 30, 2021. https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/063021-operating-circular-5-cps-pki.pdf, 37.

70 National Institute of Standards and Technology, "FIPS 140-2: Security Requirements for Cryptographic Modules," nist.gov, https://csrc.nist.gov/publications/detail/fips/140/2/final.

71 Federal Reserve Banks, "Fedwire Funds Service."

72 Board of Governors, "The Fedwire Funds Service," 27.

73 Deodoro et al., "Quantum Computing and the Financial System."

74 Deodoro et al., "Quantum Computing and the Financial System."

75 Deodoro et al., "Quantum Computing and the Financial System."

76 Deodoro et al., "Quantum Computing and the Financial System," 12.

77 Badev et al., "Fedwire Funds Service."

78 This data series is publicly available at Federal Reserve, "Fedwire Funds Service—Monthly Statistics," FRBservices.org, last modified Sept. 1, 2022, https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/monthly-stats.html.

79 Badev et al., "Fedwire Funds Service."

80 Badev et al., "Fedwire Funds Service."

81 Badev et al., "Fedwire Funds Service," 44.

82 Badev et al., "Fedwire Funds Service," 21.

83 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*.

84 Mark J. Bilger, "Cyber-Security Risks of Fedwire," *Journal of Digital Forensics, Security and Law* 14, no. 4 (April 2020): 2. https://commons.erau.edu/jdfsl/vol14/iss4/2/.

85 Bilger, "Cyber-Security Risks of Fedwire," 4.

86 Bilger, "Cyber-Security Risks of Fedwire," 5.

87 Badev et al., "Fedwire Funds Service," 22.

88 Liquidity is "a measure of the extent to which a market can

facilitate the trade of an asset at short notice, low cost, and with little impact on its price." In the event of a liquidity crisis, "demand for liquidity outstrips supply," leading to higher transaction costs and overall sluggish transactions and broader market inefficiency. "Indeed, such liquidity crises were at the heart of the financial crisis of 2007-8, as the value of many financial instruments traded by banks fell sharply without buyers" (Lewis Gudgeon et al., "The Decentralized Financial Crisis," in Crypto Valley Conference on Blockchain Technology [CVCBT], June 2020, 1–15, https://doi.org/10.1109/CVCBT50464.2020.00005).

89 Giulia Fanti et al., *Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency* (Washington, DC: Atlantic Council Geoeconomics Center, 2022), 2, https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/.

90 Bilger, "Cyber-Security Risks of Fedwire," 7.

91 Loretta J. Mester, "Cybersecurity and the Federal Reserve," speech to the Fourth Annual Managing Cyber Risk from the C-Suite Conference, Federal Reserve Bank of Cleveland, Cleveland, OH, October 5, 2021, https://www.clevelandfed.org/collections/speeches/2021/sp-20211005-cybersecurity-and-the-federal-reserve.

92 Frank Adelmann et al., "Cyber Risk and Financial Stability: It's a Small World After All" (Staff Discussion Notes No. 2020/007, International Monetary Fund, Washington, DC, 2020), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622.

93 Bouveret, "Cyber Risk for the Financial Sector."

94 Ashwin Clarke and Jennifer Hancock, "Payment System Design and Participant Operational Disruptions" (Research Discussion Paper 2012-05, Payments Policy Department, Reserve Bank of Australia, Sydney, 2012), https://www.rba.gov.au/publications/rdp/2012/pdf/rdp2012-05.pdf.

95 Adelmann et al., "Cyber Risk and Financial Stability."

96 Martin Boer and Jaime Vazquez, *Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System* (Washington, DC: Institute of International Finance, 2017), 7, https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf.

97 Welburn and Strong, "Systemic Cyber Risk and Aggregate Impacts."

98 Adelmann et al., "Cyber Risk and Financial Stability," 26.

99 Adam Z. Rose, Gbadebo Oladosu, Bumsoo Lee, and Garrett Beeler Asay, "The Economic Impacts of the September 11 Terrorist Attacks: A Computable General Equilibrium Analysis," *Peace Economics, Peace Science and Public Policy* 15, no. 2 (2009): art. 4, https://experts.illinois.edu/en/publications/the-economic-impacts-of-the-september-11-terrorist-attacks-a-comp.

100 Bouveret, "Cyber Risk for the Financial Sector."

101 Dreyer, Paul, et al. *Estimating the Global Cost of Cyber Risk: Methodology and Examples* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2299.html.

102 Rokhaya Dieye, Ahmed Bounfour, Atlay Ozaygen, and Niaz Kammoun, "Estimates of the Macroeconomic Costs of Cyber-Attacks," *Risk Management and Insurance Review* 23, no. 2 (Summer 2020): 183–208, https://doi.org/10.1111/rmir.12151.

103 Jamilov, Rey, and Tahoun, "The Anatomy of Cyber Risk," 25.

104 Welburn and Strong, "Systemic Cyber Risk and Aggregate Impacts."

105 Welburn and Strong, "Systemic Cyber Risk and Aggregate Impacts," 10.

106 Welburn and Strong, "Systemic Cyber Risk and Aggregate Impacts," 5.

107 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 2.

108 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 9.

109 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 9.

110 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 2.

111 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 2.

112 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 3.

113 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 3.

114 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 41.

115 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 35-6.

116 For a more detailed explanation of the Granger causality and regression results, please see appendix A. The resulting coefficients from the OLS regressions in table 3 can be interpreted as in section 5.

117 We assume that this irreproducibility is intentional to maintain the confidentiality of Fedwire participants and in the interest of economic and national security concerns.

118 Oxford Economics, "Global Economic Model," accessed Nov. 30, 2022, https://www.oxfordeconomics.com/global-econom-

ic-model. The GEM site, widely used by governmental and nongovernmental organizations alike, produces multivariate forecasts up to 10 years into the future for over 80 countries. By incorporating Keynesian principles in the short run and monetarist theory in the long run, this eclectic model allowed us to analyze the demand-driven effects of the attack scenario we described in this paper over the months and years following the attack. For a more detailed explanation of the derivation of the GEM shock calibrations, including the bootstrap methodology, please see appendix B.

119 Similar to Eisenbach et al., as pointed out in footnote 117, due to national security concerns, we will not precisely detail the methods through which a quantum-enabled adversary could achieve such a disruption to Fedwire, or banks' access thereof, but instead will outline the conditions under which we modeled this scenario.

120 *Indirect GDP-at-risk* refers to the integrated difference from the baseline (or unperturbed) economic forecast and our shocked-forecast GEM model.

121 Mester, "Cybersecurity and the Federal Reserve."

122 Benoît Cœuré, a member of the Executive Board of the ECB, reiterated this point in a speech in 2018: "We should see the global payment system for what it really is: an essential global public good whose integrity is increasingly being challenged by malicious cyberattacks" (Cœuré, "The Future of Financial Market Infrastructures: Spearheading Progress without Renouncing Safety," speech at the Central Bank Payments Conference, Singapore, June 26, 2018, https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180626.en.html).

123 Kartik Anand, Chanelle Duley, and Prasanna Gai, "Cybersecurity and Financial Stability" (Deutsche Bundesbank Discussion Papers No. 08/2022, Deutsche Bundesbank, Frankfurt, Germany, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4073158.

124 Stephen G. Cecchetti and Kermit L. Schoenholtz, "Cyber Instability," *Money, Banking, and Financial Markets* blog, July 16, 2018, https://www.moneyandbanking.com/commentary/2018/7/15/cyber-instability.

125 Cecchetti and Schoenholtz, "Cyber Instability."

126 Butler, Herman, and Pagano, *Decrypting Crypto*, 24.

127 Butler, Herman, and Pagano, *Decrypting Crypto*, 24.

128 Arthur Herman, *The Executive's Guide to Quantum Cryptography: Security in a Post-Quantum World*, policy guide, Quantum Alliance Initiative (Washington, DC: Hudson Institute, 2020), https://www.hudson.org/technology/the-executive-s-guide-to-quantum-cryptography-security-in-a-post-quantum-world.

129 Butler, Herman and Pagano, *Decrypting Crypto*.

130 National Institute for Standards and Technology, "Post-Quantum Cryptography," Computer Security Resource Center call for proposals, Nov. 1, 2022, https://csrc.nist.gov/projects/post-quantum-cryptography.

131 Deodoro et al., "Quantum Computing and the Financial System."

132 Morten L. Bech and Rod Garratt, *Illiquidity in the Interbank Payment System following Wide-Scale Disruptions*, Staff Report No. 239 (New York: Federal Reserve Bank of New York, 2006), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr239.pdf. This report references the findings of both (1) McAndrews and Rajan and (2) McAndrews and Potter in forming this conclusion. See James J. McAndrews and Samira Rajan, "The Timing and Funding of Fedwire Funds Transfers," *Federal Reserve Bank of New York Economic Policy Review* 6, no. 2 (July 2000): 17–32, https://www.newyorkfed.org/research/epr/00v06n2/0007mcan.html; James J. McAndrews and Simon M. Potter, "Liquidity Effects of the Events of September 11, 2001," *Federal Reserve Bank of New York Economic Policy Review* 8, no. 2 (Nov. 2002): 59–79, https://www.newyorkfed.org/research/epr/02v08n2/0211mcan.html.

133 Bech and Garratt, *Illiquidity*, 22.

134 Bech and Garratt, *Illiquidity*, 22.

135 Bech and Garratt, *Illiquidity*, 23.

136 Luque, López, and Williams, "Cyber Risk as a Threat," 199.

137 Luque, López and Williams, "Cyber Risk as a Threat," 200.

138 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 10.

139 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 10.

140 Cecchetti and Schoenholtz, "Cyber Risk, Financial Stability and the Payments System," *Money, Banking, and Financial Markets* blog, July 26, 2020, https://www.moneyandbanking.com/commentary/2020/7/26/cyber-risk-financial-stability-and-the-payments-system.

141 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System*, 10.

142 George-Marios Angeletos, Christian Hellwig, and Alessandro Pavan, "Signaling in a Global Game: Coordination and Policy Traps," *Journal of Political Economy* 114, no. 3 (June 2006): 452–84, https://www.journals.uchicago.edu/doi/abs/10.1086/504901.

143 Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System.*

144 Cecchetti and Schoenholtz, "Cyber Risk, Financial Stability and the Payments System."

145 Mester, "Cybersecurity and the Federal Reserve."

146 Arthur Herman, *Advancing the Quantum Advantage: Hybrid*

Quantum Systems and the Future of American High-Tech Leadership, policy report, Quantum Alliance Initiative (Washington, DC: Hudson Institute, 2022), https://www.hudson.org/innovation/advancing-quantum-advantage-hybrid-quantum-systems-future-american-high-tech-leadership.

147 Arthur Herman, "Q-Day is Coming Sooner Than We Think," *Forbes,* June 7, 2021, https://www.forbes.com/sites/arthurherman/2021/06/07/q-day-is-coming-sooner-than-we-think/?sh=b5158f43f5d5.

148 Bao Yan, et al., "Factoring integers with sublinear resources on a superconducting quantum processor," December 23, 2022, https://arxiv.org/pdf/2212.12372.pdf.

149 Studenmund, *Using Econometrics*, 375.

150 Granger, "Investigating Causal Relations."

Notes

Notes

Notes

Hudson Institute
1201 Pennsylvania Avenue, Fourth Floor, Washington, D.C. 20004
+1.202.974.2400 www.hudson.org