

STANFORD UNIVERSITY

THE STANFORD EMERGING TECHNOLOGY REVIEW 2025

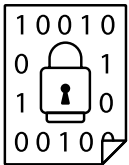
A Report on Ten Key Technologies and Their Policy Implications

CO-CHAIRS Condoleezza Rice, John B. Taylor, Jennifer Widom, and Amy Zegart

DIRECTOR AND EDITOR IN CHIEF Herbert S. Lin | **MANAGING EDITOR** Martin Giles







CRYPTOGRAPHY

KEY TAKEAWAYS

- Cryptography is essential for protecting information, but alone it cannot secure cyberspace against all threats.
- Cryptography is the enabling technology of blockchain, which is the enabling technology of cryptocurrencies.
- Central bank digital currencies (CBDCs) are a particular type of cryptography-based digital currency supported by states and one that could enhance financial inclusion. Although the United States lags some countries in experimenting with a CBDC, it may benefit from a cautious, well-timed approach by learning from other nations' efforts.

Overview

The word *cryptography* originates from Greek words that mean “secret writing.” In ancient times, cryptography involved the use of ciphers and secret codes. Today it relies on sophisticated mathematics to protect data from being altered or accessed inappropriately.¹ We are typically unaware that many of our day-to-day interactions with computers and the internet involve cryptography, from securing our online shopping to protecting our cell phone calls.

Cryptography is often invisible, but it is essential for most internet activities such as messaging, e-commerce, banking, or even simple internet browsing. Yet cryptography alone will never be enough to ensure the confidentiality, integrity, or availability of information. Inherent vulnerabilities in the software code that underpins all our internet-connected devices and the strong incentives for bad actors—from criminals to nation states—to engage

Cryptography is often invisible, but it is essential for most internet activities such as messaging, e-commerce, banking, or even simple internet browsing.

in cyberattacks that exploit human and technical vulnerabilities help to explain why cybersecurity will be an ongoing challenge.

Cryptography Basics: Public Keys, Private Keys, and Hashes

Here's an example: Drew has a private message intended only for Taylor. To keep it confidential, she scrambles (encrypts) the message using an encryption algorithm and transmits the scrambled message to Taylor as ciphertext. When Taylor receives the ciphertext, he unscrambles (decrypts) it to reveal what it originally said. This piece of decrypted text is known as the plaintext. Along comes Ellen, a third-party eavesdropper who wants to see the plaintext, so she must use any means at her disposal to break the cryptographically provided protection.

An example of an encryption algorithm is the shift cipher. Each letter in the plaintext is replaced by a letter that is some fixed number N of positions later in the alphabet. For example, if $N = 2$, Drew substitutes an A in the plaintext with a C in ciphertext, B in plaintext with D in ciphertext, and so on. If $N = 3$, then Drew substitutes A in plaintext with D in ciphertext. To decrypt the ciphertext, Taylor must know that Drew is using the shift cipher and must also know the value of N so that he can invert it. For example, knowing that $N = 2$, he knows to write down A when he sees C in the ciphertext. (Note that modern encryption algorithms are more sophisticated and secure than what has been presented here; they are also harder to explain.)

In this scenario, both Drew and Taylor must share a secret piece of information, namely N . N is the cryptographic key, which in general is a string of digits needed both to encrypt and to decrypt the message. Drew and Taylor must also know that the algorithm is the shift cipher. If Ellen somehow learns both of those facts, she can decrypt the message as well. This type of encryption algorithm—of which the shift cipher is an example—is known as symmetric cryptography, or secret-key cryptography. It requires a secure key distribution, which is a method of distributing secret keys to all parties who should have them—but preventing those who shouldn't from obtaining them.

Symmetric key cryptography proved to be cumbersome because parties wishing to communicate securely must connect physically to share the cryptographic key before such a communication can take place. Imagine how awkward phone communications would be if you had to meet every telephone partner in person before talking to that party.

In the 1970s, Stanford professor Martin Hellman and Whitfield Diffie codeveloped a technique known as asymmetric cryptography, or public-key cryptography. Public-key cryptography relies on a public key for encrypting messages that is freely available to everyone, which means it can be widely distributed even over insecure channels. However, decrypting a message requires a private key that is held only by the authorized party (see figure 3.1).² Although it is theoretically possible to derive a private key from a public key, that process (if well designed) would

take much too long for practical purposes (it would take longer than the age of the universe). It is this essential property that is placed at risk by quantum computing, as discussed below.

The mathematics of cryptography also underlie the creation of secure hashes. A hash is designed to accept a message of any length and compute a unique fixed-length string of numbers—called the hash value—corresponding to that message. Hashes have two key properties. First, it is extremely difficult to find another message that results in the same string of numbers. Second, if all you have is the string of numbers, it is infeasible to recover the original message.

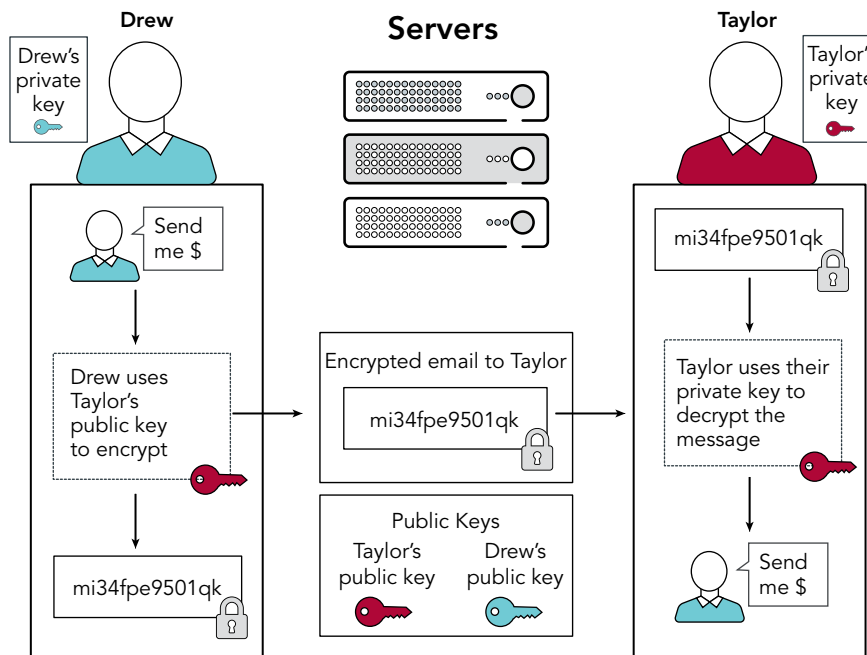
Using a secure hash function, the sender can use public-key cryptography to provide assurances of integrity—information that cannot be tampered with or altered in any way—and identity, in that the

originator of the message is who he or she claims to be.

To illustrate, Alice (the sender) first computes the hash value of her message. Next, she encrypts the hash value with her private key, a process analogous to signing a document, generating a digital signature of the message's hash.³ Alice then sends the message and its digital signature to Bob (the receiver).

Upon receipt of the message, Bob can recover the hash value for the message that Alice purportedly sent and compare that value to his own computation of the hash value. If these match, Bob can be assured that the message has not been altered in transmission and also that Alice was the party who sent it, since only Alice could have used her private key to create a digital signature of the message's hash.

FIGURE 3.1 How public-key cryptography works



Messages can also be digitally time-stamped. A known authoritative time and date server—such as the Internet Time Service, operated by the National Institute of Standards and Technology—accepts a message, appends the current date and time, and then provides a digital signature for the stamped message.

Blockchain

Blockchain is a technology that enables multiple parties to coordinate when there is no central trusted party. This often comes up in financial settings. A blockchain records transactions so that they cannot be altered retroactively without detection. Because the entire blockchain can be distributed over thousands of computers, it is always accessible; anyone can deploy an application for it, and no one can prevent any such deployment. Moreover, anyone can interact with this application, and no one can prevent such an interaction. Finally, data cannot be erased. Later transactions may indicate that corrections are necessary, but the original data remain.

A blockchain can be visualized as a chain of blocks where each block contains a single transaction and a cryptographic hash of the previous block. This creates a chain in which every block except the first is linked to the previous block. As more transactions occur, the blockchain gets longer because more blocks are added to the chain.

The distributed nature of blockchain also increases security. A new transaction is broadcast to every party in the network, each of which has a replica of the entire blockchain (see figure 3.2). Each party tries to validate the new transaction. It could happen that these replicas may not be fully synchronized; some might have received the new transaction while others have not. To ensure that all replicas are identical, blockchains have mechanisms for coming to consensus on the correct information. Ethereum, for example, accepts transactions that have been validated by two-thirds of the participants. Blockchains are designed with economic incentives for replicas to behave honestly.

Applications that run on a blockchain are called smart contracts. These are computer programs that are always available and whose execution cannot be reversed—once a smart contract processes an incoming request, that processing cannot be rolled back. Smart contracts can be used to implement financial instruments, to record ownership of digital assets, and to create marketplaces where people can buy and sell assets. Smart contracts are composable—one smart contract can use another—thus creating a vibrant ecosystem of innovation where one project can make use of a service developed by another project. Once deployed, they are available forever, running whenever someone interacts with them. By contrast, cloud computing applications are inherently transient—as soon as the application developer stops paying the cloud fees, the cloud provider kills the application.

Key Developments

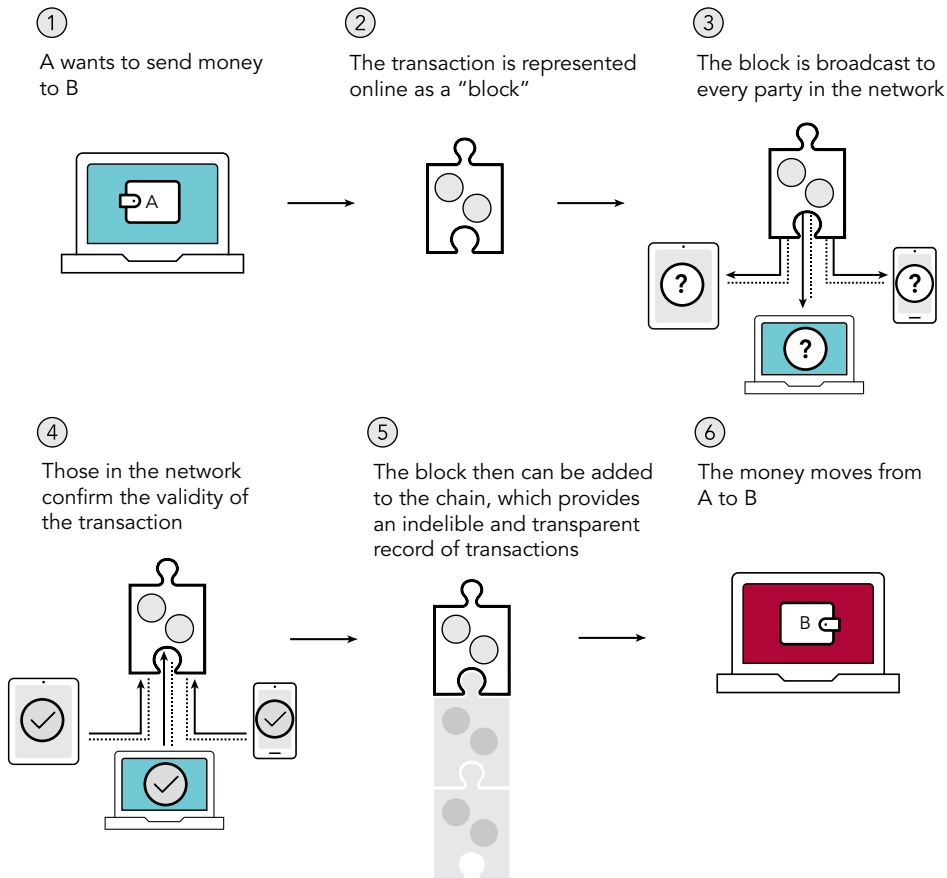
A Host of Blockchain Applications

Blockchain technology was developed decades ago but has recently been used for a variety of applications. All those listed below have been implemented in some form and are operational today, though perhaps not on particularly large scales.

Time-stamping and data provenance Because data written to a blockchain cannot be modified or removed, blockchains provide a good mechanism for data provenance and time-stamping. An artist or an author who creates a new work of art can post a hash of the work to the chain, thereby proving the time at which the object was created. If later someone else claims authorship of the creation, the artist can point to the chain to prove its provenance.

Identity management A blockchain stores all the data from a person's important documents—diplomas, healthcare and financial records, tax returns, birth certificate—in encrypted form. These

FIGURE 3.2 How a blockchain manages transactions



original records are saved digitally, signed by their original providers, and, when made available through the blockchain, provided with provenance and time-stamping. Blockchain also facilitates selective revelation: Upon request, the person can authorize release of data only to the minimal extent necessary to satisfy the request. For example, people can prove that their age is above some legal minimum, like twenty-one, but not have to reveal their date of birth. A woman can allow a healthcare researcher to look at her records for specific data—for example, whether she has ever had an abortion—without revealing her name. Applications of blockchain for identity management, such as SpruceID, are already being deployed.⁴

Supply chain management Blockchain can provide a transparent and secure way to track the movement of goods and their origin and quantity. This can be particularly valuable for high-value industries, such as the diamond industry; industries with significant counterfeit issues, such as luxury goods (see figure 3.3); or industries where the true source of goods is important, such as organic or vegan food. Blockchain can greatly simplify the job of forensic accountants trying to trace transactions.

Transactional records Many kinds of transactional records can be stored on a blockchain, thereby streamlining the process of buying and selling items by reducing fraud, increasing transparency, cutting

FIGURE 3.3 Blockchain helps tackle counterfeiting in the luxury goods industry



Source: Shutterstock / TY Lim

paperwork, and generally making the process more efficient.

Cryptocurrencies Cryptocurrencies are digital instruments that many people use as a medium of exchange. Well-known ones include Bitcoin, Ethereum, Avalanche, and Polygon, each of which has its own unique features and applications. Because they are not issued by any central authority, they are not subject to the same national regulatory regimes that govern traditional currencies (i.e., so-called fiat currencies). Cryptocurrencies use a blockchain structure to ensure the integrity and immutability of transaction data, making it resistant to fraud and counterfeiting and reducing its susceptibility to government interference or manipulation. Contrary to a common belief, cryptocurrencies can, but do not have to, support private or secret transactions—indeed, the most popular cryptocurrencies deliberately do not hide the details of their transactions. Those who transact in cryptocurrencies often wish to exchange their instruments for fiat currency (e.g., real dollars) and generally use a cryptocurrency exchange to do so. In the United States, such exchanges are regulated financial institutions and are presently

under the jurisdiction of the Securities and Exchange Commission.

Secure Computation

The field of cryptography has also expanded in scope to include secure computation, a well-established subfield that enables multiple parties to contribute inputs to a function that they jointly compute in such a way that the specific inputs from each party are kept secret from the others. Secure computation enables data privacy during computation, ensuring that no party learns more information about the other parties' inputs than what can be inferred from the result alone. Secure computation also allows users to prove they possess knowledge of a statement without having to disclose the actual content of that statement.

To illustrate secure computation, consider the problem of determining the collective wealth of three people while keeping the individual wealth of each person secret. Alice chooses a large random number and in secret adds her wealth to that number. Alice then gives the sum to Bob privately, who adds his wealth secretly to the number received from Alice. Bob secretly passes the total to Charlie, who does the same computation and then passes the result to Alice. Alice then in secret subtracts her original random number from the number received from Charlie and reveals the result to everyone else. That revealed number is the sum of each party's wealth but at no time does anyone learn of anyone else's wealth.⁵

This example is oversimplified but is offered to suggest how computation on secret data might be accomplished. The example is not exactly how a real-world secure computation works (in fact, there is a subtle flaw in the procedure described); true secure computation protocols use more complex mathematics to defend against malicious behavior and to guarantee the privacy of each person's input during the computation process.

In addition, the example is somewhat artificial compared to more realistic examples (with more complex mathematics) such as tallying vote counts or bidding in an auction. For example, at an auction, three bidders each have a secret bid in mind, and the goal could be to determine which bid is the highest without publicly revealing information about the other bids.

Applications of secure computation allow data analytics to be performed on aggregated data without disclosing the data associated with any individual element of the dataset. Banks can detect fraud without violating the privacy of individual customers. A group of workers can calculate their average salary without revealing their colleagues' personal pay. A Stanford system called Prio allows for a network of connected computers to work together to compute statistics, with clients holding their individual data privately.⁶ This was deployed, for example, on mobile phones during the COVID-19 pandemic to calculate how many people were exposed to COVID-19 in aggregate, without learning who was exposed.

Zero-Knowledge Proofs

A zero-knowledge proof is a cryptographic method that allows Paul (the prover) to prove to Vivian (the verifier) that Paul knows a specific piece of information without revealing to Vivian any details about that information. The term *zero knowledge* indicates that Vivian gains zero new knowledge about the information in question, apart from the fact that what Paul is saying is true.

Consider a simplified example that demonstrates the logic: two people dealing with a locked safe. Let's say Paul wants to prove to Vivian that he knows the combination to the safe, but he doesn't want to reveal the combination to Vivian. With a zero-knowledge proof, Paul can convince Vivian that he knows the combination without exposing the combination itself.

To do so, Paul has Vivian write something on a piece of paper without showing it to him. Together, they put the paper into the safe and spin the combination lock. Vivian now challenges Paul to say what is on the paper. Paul responds by asking Vivian to turn around (so that Vivian cannot see Paul) and then enters the combination of the safe, opens it, looks at the paper and returns it to the safe, and closes it. When Vivian turns around, Paul tells her what was on the paper. Paul has thus shown Vivian that he knows the combination without revealing to Vivian anything about the combination.

In practice, of course, zero-knowledge proofs are more complex, yet they already have seen real-world implementations:

Banking A buyer may wish to prove to a seller the possession of sufficient funds for a transaction without revealing the exact amount of those funds. This capability has been implemented in the Zcash cryptocurrency.⁷

Provenance for digital images Cameras can provide a digital signature for every photo, capturing an image and information about the time, date, and location. But such photos can then be digitally cropped, resized, or converted from color to black-and-white. Zero-knowledge proofs have been implemented in the standards of the Coalition for Content Provenance and Authenticity to ensure that the original photo was properly signed and that only permissible edits were made to the original without having to trust the editing software that was used.⁸

Cooperative tracking and verification of numbers of tactical nuclear warheads A zero-knowledge proof methodology has been developed to cooperatively provide updates on the movement and status changes of warheads in accordance with a political agreement to do so without revealing other sensitive information. This approach has not yet been implemented in any real arms control agreement, but its feasibility has been demonstrated in principle.⁹

Over the Horizon

Impact of Cryptography

The applications described above suggest a broad range of possibilities for cryptographically enabled data management services. Whether we will see their widespread deployment depends on complicated decisions about economic feasibility, costs, regulations, and ease of use.

Misaligned incentives can affect how fast innovations are deployed. Some of the applications described above provide significant benefits for the parties whose data can be better protected and kept more private. But existing companies, having built their business models on legacy systems that ingest all their customers' data, have no incentive to change their practices. They are the ones who would have to pay for these privacy-protecting capabilities, yet they would not benefit from their adoption.

A second point is that widespread deployment will require confidence that proposed innovations will work as advertised. That is, would-be users of these innovations must have confidence in them. But concepts such as secure computation and zero-knowledge proofs are math heavy and counterintuitive to most people. Expecting policymakers, consumers, and regulators to place their trust in these applications will be challenging.

Challenges of Innovation and Implementation

Although cryptography is fundamentally a mathematical discipline, it requires both human talent and substantial computing resources to examine the efficiency of new techniques, write software that is computationally expensive such as zero-knowledge provers, and conduct comprehensive scans of the internet. Progress also relies on interdisciplinary centers that bring together faculty from different fields

to share problem sets and understand the potential benefits that cryptographically enabled techniques and approaches could provide.

Research is funded by both the US government and private industry, but funding from the US government is subject to many requirements that increase the difficulty of proposal submission manyfold (as much as by a factor of sixty). Thus, research faculty often prefer arrangements with the private sector, which tend to be much simpler. On the other hand, only the US government is able to fund research that may not pay off for many years (as in the case of quantum computing).

Policy, Legal, and Regulatory Issues

As a rule, public policy considerations are application specific; there has been no push to regulate basic research in cryptography for several decades.

EXCEPTIONAL ACCESS

Exceptional access regulations would require communications carriers and technology vendors to provide US law enforcement agencies access to encrypted information (both data storage and communications) under specific legal conditions. Opponents of exceptional access argue that implementing this capability inevitably weakens the security afforded by encryption to everyone. Supporters of exceptional access do not debate this technical assessment: It is true that exceptional access, by definition, weakens encryption. However, they argue that even if lower security is the result of implementing exceptional access, that price is worth the benefits to law enforcement.¹⁰

CRYPTOCURRENCY REGULATORY CONCERNS

Particularly considering the 2023 FTX trading scandal, in which the FTX cryptocurrency exchange went bankrupt and founder Sam Bankman-Fried was subsequently convicted of fraud, many have questioned the extent to which cryptocurrencies should

The lack of a regulatory framework for cryptocurrency affects many American users, consumers, and investors who are often confused about the basic workings of cryptocurrencies and their markets.

be exchangeable for national currency and whether they are better regulated as investment instruments or as currency. The lack of a regulatory framework for cryptocurrency affects many American users, consumers, and investors who are often confused about the basic workings of cryptocurrencies and their markets. It may also prevent entrepreneurs from implementing their ideas in the United States or inadvertently incentivize them to move offshore.

ENERGY CONSUMPTION

Bitcoin, an older and today the dominant cryptocurrency, consumes an enormous amount of energy; Bitcoin mining uses more energy than the Netherlands.¹¹ For this reason, newer blockchains— notably Ethereum—are designed to use far less energy, and today Ethereum’s annual energy use is less than a 10,000th of YouTube’s annual consumption. But Ethereum’s market capitalization is less than half that of Bitcoin, and it remains to be seen whether any less energy-intensive cryptocurrency will displace the latter.

QUANTUM COMPUTING AND CRYPTOGRAPHY

Current public-key cryptography is based on the extraordinarily long times (times comparable to the age of the universe) required with today’s computers to derive a private key from its public-key counterpart. When realized, quantum computing (discussed more fully in chapter 8 on semiconductors) will pose a significant threat to today’s public-key algorithms. Experts disagree on how long it will take

to build quantum computers that are capable of this, but under the May 2022 National Security Memorandum 10, Promoting US Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, the US government has initiated the transition to quantum-resistant public-key algorithms. Many experts in the field expect quantum-resistant algorithms will be widely available by the time quantum computing comes online.

At the intersection of quantum computing and cryptography are two important issues. The first is that support for the transition to a quantum-resistant encryption environment should continue with urgency and focus.

A second issue is that messages protected by pre-quantum cryptography will be vulnerable in a post-quantum world. If those messages had been saved by adversaries (likely in the case of parties like Russia), those bad actors will be able to read a host of old messages. Containing secrets from the past, they may reveal embarrassments and dangers with potentially detrimental policy implications.¹²

CENTRAL BANK DIGITAL CURRENCIES AND THE EROSION OF US FINANCIAL INFLUENCE

A central bank digital currency (CBDC) is a type of cryptography-based digital currency issued and regulated by a country’s central bank, with legal tender status and value equivalent to the country’s traditional currency—that is, digital assets backed by

central banks. A CBDC can be designed with any number of the functional characteristics of cryptocurrencies and thus can be regarded as a national cryptocurrency. However, a CBDC could be implemented in a centralized manner to improve performance and efficiency instead of using distributed blockchain technology.

An important benefit of a CBDC is the marriage of convenience and lower costs of digital transactions—by cutting out intermediaries—and the regulatory oversight of traditional banking. In 2021, nearly six million Americans had no access to a bank account. Lower transaction costs would improve financial inclusion and enable many more people to have access to a well-regulated financial system. Those lower costs would also apply to cross-border transactions, therefore reducing the costs of international commerce.

The United States is considering issuing its own CBDC.¹³ Although the dollar is the currency most used in cross-border transactions, the development of CBDCs by others could reduce global dependence on the US currency and on a financial infrastructure largely controlled today by the United States (e.g., the Society for Worldwide Interbank Financial Telecommunication, or SWIFT, which is used by banks and other institutions to send secure messages to each other about financial transactions). This could significantly undermine the effectiveness of US economic sanctions and other financial tools. Today, more than ninety nations are researching, piloting, or deploying CBDCs, with several already testing cross-border transactions. China is the first major country to deploy a CBDC, the digital yuan, widely within its own economy.¹⁴ America may lag China and some other countries, but it could benefit from a cautious, well-timed approach by learning from earlier adopters' experiences.

NOTES

1. National Institute of Standards and Technology, "Cryptography," US Department of Commerce, accessed August 15, 2023, <https://www.nist.gov/cryptography>.
2. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory* IT-22, no. 6 (November 1976): 644–54.
3. In this context, encrypting the hash value simply means running the encryption algorithm using as the input key a string of numbers that just happen to be Alice's private key. In most cases involving public-key cryptography, the private key is used only for decryption purposes, but nothing stops a user from using it in other ways.
4. SpruceID, "SpruceID," Spruce Systems, accessed October 13, 2024, <https://spruceid.com/>.
5. This example is inspired by Keyless Technologies, "A Beginner's Guide to Secure Multiparty Computation," *Medium*, February 22, 2020, <https://medium.com/@keylesstech/a-beginners-guide-to-secure-multiparty-computation-dc3fb9365458>.
6. See Stanford University, "Prio," accessed September 25, 2023, <https://crypto.stanford.edu/prio>.
7. Zcash, "What Are Zero-Knowledge Proofs?," accessed August 30, 2023, <https://z.cash/learn/what-are-zero-knowledge-proofs>.
8. Trisha Datta and Dan Boneh, "Using ZK Proofs to Fight Disinformation," *Medium*, September 29, 2009, <https://medium.com/@boneh/using-zk-proofs-to-fight-disinformation-17e7d57fe52f>.
9. Miles A. Pomper, William Alberque, Marshall L. Brown Jr., et al., *OP55: Everything Counts: Building a Control Regime for Nonstrategic Nuclear Warheads in Europe*, CNS Occasional Paper Series, James Martin Center for Nonproliferation Studies, May 10, 2022, <https://nonproliferation.org/op55-everything-counts-building-a-control-regime-for-nonstrategic-nuclear-warheads-in-europe>.
10. Office of Public Affairs, "Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cybersecurity," US Department of Justice, July 23, 2019, <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber>.
11. Digiconomist, "Bitcoin Energy Consumption Index," accessed September 16, 2023, <https://digiconomist.net/bitcoin-energy-consumption>.
12. Herbert Lin, "A Retrospective Post-Quantum Policy Problem," *Lawfare*, September 14, 2022, <https://www.lawfaremedia.org/article/retrospective-post-quantum-policy-problem>.
13. Board of Governors of the Federal Reserve System, "Central Bank Digital Currency (CBDC): Frequently Asked Questions," accessed August 15, 2023, <https://www.federalreserve.gov/cbdc-faqs.htm>.
14. Darrell Duffie and Elizabeth Economy, eds., *Digital Currencies: The US, China, and the World at a Crossroads* (Stanford, CA: Hoover Institution, 2022), https://www.hoover.org/sites/default/files/research/docs/duffie-economy_digitalcurrencies_web_revised.pdf.

STANFORD EXPERT CONTRIBUTORS

Dr. Dan Boneh

SETR Faculty Council and Professor of Computer Science and of Electrical Engineering

Dr. David Tse

Thomas Kailath and Guanghan Xu Professor of Engineering

Neil Perry

SETR Fellow and PhD Student in Computer Science