PitchBook

PitchBook Data, Inc.

John Gabbert Founder, CEO

Nizar Tarhuni Senior Director, Institutional Research & Editorial

Dylan Cox, CFA Head of Private Markets Research

Institutional Research Group

Analysis

Brendan Burke
Senior Analyst, Emerging Tech
brendan.burke@pitchbook.com

Data

Matthew Nacionales
Data Analyst

pbinstitutionalresearch@pitchbook.com

Publishing

Designed by **Joey Schaffer**

Published on June 13, 2022

Contents

EMERGING TECH RESEARCH

Hashing Out the Future of Encryption Algorithms

Innovations driving startup growth in cryptography

PitchBook is a Morningstar company providing the most comprehensive, most accurate, and hard-to-find data for professionals doing business in the private markets.

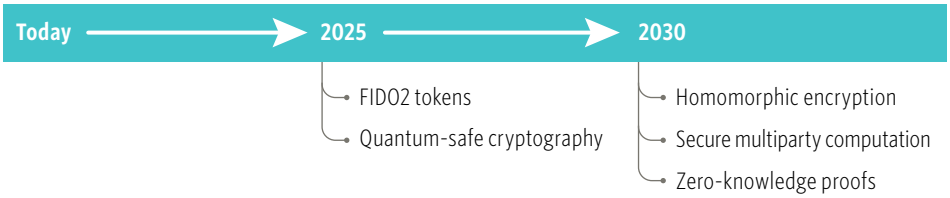
Key takeaways

- Public key infrastructure innovation led to a 30-year commercial runway that can be replicated in the modern cloud computing, quantum, and AI eras.
- Venture activity in companies commercializing the FIDO2 standard suggests that fundamental innovation in public key encryption can produce large companies.
- FIDO2 tokens and quantum-safe cryptography will likely gain mainstream adoption by 2025, while privacy-enhanced computing will likely require further research until commercializing around 2030.

Outlook

We see diverging timeframes for commercialization of encryption innovations based on research and development (R&D) and enterprise priorities across three key categories: FIDO2 authentication, quantum-safe cryptography, and privacy-enhanced computing. FIDO2 is becoming a standard for authentication with over 60% of enterprises using some form of passwordless multifactor authentication today.[1] Lightweight versions of passwordless authentication will likely become ubiquitous by 2023 while FIDO2 integrations are ongoing. The success of initial FIDO2 pilots by tech giants such as Apple will extend to broader enterprise adoption by 2025. Similarly, given enterprises' urgency surrounding quantum computing development by hostile actors, we expect quantum-safe cryptography to commercialize as soon as a National Institute of Standards and Technology (NIST) standard is finalized. Privacy-enhanced computing will likely take longer to develop due to the need for enhanced processing efficiency and research into compressed algorithms. We view these methods as unlikely to produce large companies until 2030. We may see winners emerge in each of these categories, producing companies at the scale of RSA Security and its spin-offs.

Indicative timelines for mainstream adoption of emerging encryption protocols



Source: PitchBook

Background

Encryption innovation has historically created large companies. Public key infrastructure (PKI) spawned a wave of large companies responsible for underpinning the security of the internet. Researchers at the Massachusetts Institute of Technology invented public key encryption technology in 1977 and subsequently founded the company RSA Data Security in 1982. RSA encryption became the standard for the fledgling internet by 1990, and RSA Data Security commercialized a derivative product called BSAFE public key encryption. The company sold for approximately $251 million in 1996 in a reverse merger to go public and scaled to a $2.1 billion acquisition to EMC in 2006. Two years later, domain name system (DNS) leader Verisign achieved a $282.1 million valuation in its IPO and remains a large publicly traded company that has exceeded a $28 billion market cap. The company was founded as a spin-off of RSA Security.

PKI emerged as a potential panacea for internet security that enabled companies to collect increasing rents on enabling technology. Early startups in the space integrated PKI in specific use cases, including DNS registry, payments, and identity

1: "The State of Workforce Passwordless Authentication," Ponemon Institute, October 2021.

authentication—retaining pricing power from their intellectual property over encryption algorithms. For example, Verisign currently charges $8.39 per ".com" address and $9.02 per ".net" annually to provide domain name services to internet nonprofits and the government.[2] RSA achieved long-term leadership in user authentication with its SecurID product before ceding ground around 2011 to a new wave of access management and endpoint protection platforms. PKI innovation led to a 30-year commercial runway that can be replicated in the modern cloud computing, quantum, and artificial intelligence (AI) eras.

Innovation opportunities

Startups are beginning to commercialize novel encryption techniques that can provide enduring value streams when addressing emerging types of IT communications. Encryption innovations are required across cloud computing, identity management, industrial networks, and data centers, among other IT functions. For this reason, we see encryption innovation opportunities across three key categories that can each establish protocols for the future of IT: Fast IDentity Online 2 (FIDO2) tokens, quantum-safe cryptography, and privacy-preserving computing. While incumbents are developing products in these spaces, we believe that startups will ultimately be formed to commercialize the most advanced breakthroughs from academia and as spin-offs from large companies. We are beginning to see incumbents make acquisitions in these areas to remain innovative.

2: "Company Report: We Expect Verisign to Provide Uninterrupted DNS Services Despite Elevated Cyber Risk," Morningstar, Emma Williams, April 2022.

This market map, including a full list of vendors, is available to PitchBook clients in the Information Security Analyst Workspace on the PitchBook Platform.

Encryption innovation ecosystem market map

Privacy-enhanced computing

Homomorphic encryption

IBM, Duality, Enveil, Inpher, Datafleets, Cryptolab

Secure multiparty computation

baffle, unbound security, IXUP, LiveRamp, cryptonumerics, ZIROH Labs, Cybernetica

Zero-knowledge proofs

toposware, qedit, DECO, Origo, evernym

Authentication tokens

FIDO2 token specialists

HYPR, Giesecke+Devrient, yubico, nok nok, RAON SECURE, SAMSUNG SDS, TRUSONA, Secret Double Octopus, Entersekt, boloro, Forticode, FEITIAN

Diversified authentication token providers

Microsoft, Cisco, Entrust, RSA, okta, THALES, OneSpan, LinOTP, KOBIL

Quantum-safe cryptography

Quantum-safe cryptography

ABOUT, Quintessence Labs, QUANTUMXCHANGE, ISARA, MagiQ, IDQ, SPEQTRAL, Aliro, KETS, Q→NU

Source: PitchBook | Geography: Global

Note: Companies are allocated to a single category based on primary value proposition. This list sorts companies by total VC raised and may exclude some market leaders.

FIDO2 tokens

PKI is receiving an overhaul from the Fast Identity Online (FIDO) Alliance, a consortium of tech and financial services companies sponsoring standards development for authentication. The Alliance's FIDO2 protocol combines public key encryption with a separate private key that can take the form of a software or hardware validator. The purpose of the private key is to create a universal second factor to supplant the range of secondary authentication factors including SMS, email, and phone calls. The key can be embedded on a device, such as a smartphone, with an app, making the device itself a factor. The private key system is based on cryptographic login credentials that reset for every session without intervention by the user. The protocol has gained support from tech giants including Google, Apple, and Microsoft, and can be embedded in applications via the Web Authentication (WebAuthn) application programming interface (API). Integration of FIDO2 in web applications remains low, limiting startups' ability to build comprehensive access management solutions across enterprise IT environments.

Venture activity in FIDO2 suggests that fundamental innovation in public key encryption can produce large companies. Transmit Security received a patent for a private authentication key in 2014 and scaled a business organically to a $2.7 billion post-money valuation in 2021. The company offers FIDO2-based passwordless authentication without a requirement to download an app. At an earlier stage, passwordless startup Stytch makes the WebAuthn protocol available via an API. We believe that implementing this protocol in various use cases can produce a similar volume of large companies to the first wave of public key encryption technology. These tokens have begun implementation and we expect mainstream adoption by 2025.

Key recent FIDO2 token VC deals*

Company name	Close date	Deal size ($M)	Post-money valuation ($M)	Deal type	Lead investor(s)	Valuation step-up
Transmit Security	June 22, 2021	$543.0	$2,743.0	Series A	General Atlantic, Insight Partners	N/A
Stytch	November 18, 2021	$90.0	$1,100.0	Series B	Coatue Management	5.2x
HYPR	March 30, 2021	$35.0	$135.0	Series C	Advent International	1.9x
Trusona	January 14, 2020	$19.4	$130.0	Series C	Georgian	2.2x

Source: PitchBook | Geography: Global
*As of March 31, 2022

Quantum-safe cryptography

Quantum computing presents fundamental challenges to legacy encryption technologies that must be proactively addressed with novel algorithms. The NIST runs a competition for quantum-safe algorithms that can provide the next iteration of RSA encryption. The competition selects among novel approaches to public key encryption that can protect IT systems from quantum systems sufficiently advanced to hack any RSA-encrypted database. The competition has narrowed to three finalists for digital signatures that can withstand quantum computer attacks—Dilithium, Falcon, and Rainbow. Given ongoing testing, NIST recommends against creating commercial products before the standard is developed. The selection of a

winning algorithm is scheduled for 2024, and we believe this will be a catalyst for mainstream commercial adoption within two years after selection.

Most quantum-safe encryption startups remain at the seed and early stages and rely on grant funding, showing the long path to commercialization in this space. Startups can continue R&D on techniques that are not likely to be selected by NIST yet may ultimately be viable in limited use cases. The outlier has been ArQit, which achieved a special purpose acquisition company (SPAC) merger at a $1.0 billion valuation, with forecasts to grow revenue from $14.0 million in 2021 to $660.0 million in 2025. The company is pursuing a method called symmetric encryption instead of NIST's preferred latticed-based architectures (represented by Dilthium and Falcon). We believe that the ultimate winners in encryption will come from the founders of the industry standard, much like RSA encryption. The vehicle by which this will be delivered is not likely to become clear for several years, increasing the risk of bets in the short term.

Key recent post-quantum cryptography deals*

Company name	Close date	Deal size ($M)	Post-money valuation ($M)	Deal type	Lead investor(s)	Valuation step-up
ArQit	September 3, 2021	$415.0	$1,000.0	Reverse merger	Centricus Acquisition	N/A
QuintessenceLabs	September 17, 2021	$19.3	$105.9	Series B	Main Sequence Ventures, TELUS Ventures	N/A
SpeQtral	July 19, 2021	$8.3	N/A	Early-stage VC	Xora Innovation	N/A
KETS Quantum Security	June 8, 2021	$5.4	$15.8	Series A	Quantonation, Speedinvest	2.4x

Source: PitchBook | Geography: Global
*As of March 31, 2022

Privacy-enhanced computing

Homomorphic encryption

Homomorphic encryption is the "holy grail" of the encryption market and is beginning to launch commercially viable solutions. The protocol allows third parties to operate on encrypted data, thus removing the need to manage encryption keys, which is a vulnerability in data security platforms. However, the products suffer in practice from excessive compute requirements, and they are ill suited to large databases given the processing power requirements. A startup's ability to define use cases for the technology while its compute requirements decline will determine its commercialization pathway. Partial homomorphic encryption limits the types of calculations that can be conducted on the encrypted data, such as multiplication or addition. Most commercial applications limit the calculations to only those that are necessary for the use case, freeing computing resources.

A variety of open-source projects, incumbent offerings, and startups develop homomorphic encryption solutions, illustrating the immaturity of the market. Leading open-source projects include HElib, Homomorphic Encryption for Arithmetic of Approximate Numbers (HEEAN), Microsoft SEAL, PALISADE, and Torus-FHE. Startups including Enveil, Duality Technologies, and Fortanix—which refers to the technology as

A note on blockchain:
The fundamental innovations underlying blockchains for security use cases include privacy-preserving computing technologies covered in this section, including ZKP and secure multiparty computation. Startup innovations in the space have largely become entangled with cryptocurrency support, leaving them outside the scope of this note. For a comprehensive survey of innovation in blockchain, see our related Vertical Snapshot.

runtime encryption—have developed commercial prototypes. Startups are benefiting from strategic investment, showing the long-range investment proposition. Financial services enterprises—including USAA Corporate Development, Capital One Ventures, Bloomberg, and Mastercard—have invested in this space via Enveil's Series A and B rounds because of use cases in customer data protection. Both Fortanix and Duality have raised from Intel Capital, demonstrating a strategic focus on the future of homomorphic encryption. Financial investors may be missing long-term opportunities in this space.

Zero-knowledge proofs (ZKP)

ZKP refers to an encryption protocol that enables privacy-preserving messaging for both parties in a communication to verify that knowledge shared is accurate without exposing the underlying data. This technology is more limited than homomorphic encryption since it only allows answers to binary questions with trust that the underlying data is accurate. This can serve the transfer of sensitive information that does not require complex processing, such as anti-money laundering and know your client registries and payments. ZKP remains primarily at an academic stage, though Avast recently acquired Evernym, a sovereign identity innovator that relies on ZKP. The company sees opportunities for consumer privacy technologies to rely on ZKP since it can eliminate the need for companies to collect third-party data. We expect academic innovations to translate to startup business models over the next several years.

Secure multiparty computation (sMPC)

sMPC offers a less compute-intensive alternative to homomorphic encryption that relies on distributed computing to offer a trusted environment for encrypted operations. The protocol enables third-party computation on encrypted data. Startups in this space have achieved limited traction. Cryptocurrency platform Coinbase acquired sMPC startup Unbound Security to improve its transaction security. Unbound Security previously raised a $20.0 million Series B, demonstrating rapid progress in the niche.

Key recent privacy-enhanced computing deals*

Company name	Close date	Deal size ($M)	Post-money valuation ($M)	Deal type	Lead investor(s)	Valuation step-up
Enveil	April 27, 2022	$25.0	$305.0	Series B	USAA Corporate Development	7.7x
Evernym	December 17, 2021	N/A	N/A	Acquisition	Avast (LON: AVAST)	N/A
Unbound Security	November 30, 2021	N/A	N/A	Acquisition	Coinbase (NYSE: COIN)	N/A
DataFleets	February 17, 2021	$67.2	$67.2	Acquisition	LiveRamp Holdings (NYSE: RAMP)	N/A
Unbound Security	November 17, 2020	$20.0	$158.6	Series B	Evolution Equity Partners	3.7x

Source: PitchBook | Geography: Global
*As of March 31, 2022