



Revolutionizing Digital Security
The Future of Digital Identity & Asset Protection

Business Plan & Overview

Q4/2025

Table of contents

About WiKey	5
Why invest in WiKey?	5
Investment Amount	6
WiKey's Market Opportunity & Industry Landscape	7
What specific problem does WiKey's solution solve?	7
What is the WiKey Product Proprietary Advantage	7
WiKey's Web2 Cyber Security Market Overview	7
WiKey's market opportunity	9
The Addressable and Obtainable Market	9
How fast this specific identity theft and key protection market is growing? What are the key trends driving its growth?	10
What regulatory changes might impact the industry?	10
The main competitors, and how is WiKey different?	11
What are the biggest barriers to entry?	12
Business Model & Revenue Generation	13
Overview	13
WiKey's revenue model	14
WiKey's plan to scale revenue over time	14
WiKey's unit economics	15
Partnerships or key client relationships	15
What is the expected break-even point?	15
Product & Technology	16
WiKey's Authenticator installation and login demo	16
Core technology	19
WiKey's authenticator development status	20
WiKey's proprietary technology and patents	20
Product roadmap for the next 12-24 months	20
What security measures and compliance frameworks are in place?	21
Is the technology scalable for global expansion?	21
Regulatory & Compliance Risks	22
What financial regulations apply to this Cyber security business?	22
WiKey's licenses and approvals	22
What are the biggest regulatory risks in different target markets?	23
WiKey's handle consumer data and privacy compliance	23
Financials & Capital Efficiency	24

What are the projected financials for the next 3-5 years?	24
How much funding has the company raised so far, and from whom?	26
How will the investment be allocated?	26
The expected return on investment (ROI) and exit strategy	28
Leadership & Team	29
Growth & Customer Acquisition	30
WiKey's go-to-market strategy	30
WiKey's customer acquisition channels	30
WiKey's cost of acquiring a customer (CAC) vs. customer lifetime value (LTV)?	31
Competitive Landscape & Defensibility	31
WiKey's unique selling proposition	31
What is the risk of new entrants or disruptive innovations?	32
Exit Strategy & Liquidity	32
What is the expected timeline for an exit?	32
The most likely exit options	33
Risks & Mitigation Strategies	33
The biggest risks	33
How does WiKey plan to mitigate these risks?	34
What contingency plans are in place for economic downturns or funding shortfalls?	34
Competitive analysis	35
Appendixes	36
External Links to Presentation Technical and Marketing Materials	37
Patents submissions	37

Disclaimer

This document and business plan contains forward-looking statements and projections about Wikey's future business, market opportunities, technological capabilities, and financial performance. These statements involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to differ materially from those expressed or implied. Key risk factors include: market projections and revenue forecasts based on current assumptions may change, technological development timelines may vary from estimates, the regulatory landscape for digital assets and security continues to evolve, the competitive environment may shift significantly, patent protection may face unforeseen challenges, actual customer adoption rates may differ from projections, and market conditions and funding environment may change. This document is for informational purposes only and does not constitute an offer to sell or solicitation of an offer to buy any securities. All financial projections are estimates and should not be regarded as guarantees of future performance. Investors should conduct their own due diligence and seek appropriate professional advice before making any investment decisions. None of the information contained herein has been verified by independent third parties.

About WiKey

As identity theft and AI-powered attacks increasingly bypass traditional security measures, both internet users and blockchain systems remain vulnerable through their reliance on passwords and private keys.

WiKey's ground breaking decentralized authentication platform provides total protection for both traditional and blockchain assets - with no use of personal data, no single point of failure, and no secret keys to hide or manage, just straightforward and reliable security that works seamlessly across Web2 and Web3.

Document summary

WiKey is an AI-resistant security platform that protects Web2 and Web3 assets. It uses a decentralized authenticator with zero-trust architecture, eliminating the need for seed phrases or personal data. The company aims to raise \$10M and projects reaching break-even within 18-24 months. WiKey's target market includes financial institutions, cryptocurrency funds, and enterprise organizations. The company's revenue model is based on a freemium SaaS model with enterprise tiers. WiKey differentiates itself by eliminating seed phrases and secrets, requiring no personal data for authentication, and using a decentralized architecture. The technology is designed for global scalability, and the company has filed for IP protection.

Why invest in WiKey?

Wikey presents a compelling investment opportunity by addressing a critical \$15T security vulnerability across both Web3 and Web2 markets, with perfect timing as AI threats and growing institutional crypto adoption drive urgent need for better security solutions.

The company's revolutionary zero-trust technology, protected by patents, eliminates fundamental key security risks without requiring seed phrases or personal data, creating significant barriers to entry while solving both crypto custody and AI impersonation challenges.

The business model demonstrates strong unit economics with scalable SaaS revenue generating 30-35% margins and impressive LTV/CAC ratios of 20-25x for enterprise clients, providing a clear path to hundreds of millions of dollars of revenue by 2030.

Led by a serial entrepreneur CEO with multiple successful exits and backed by a team with deep expertise in cryptography and security, Wikey is well-positioned for significant growth.

The exit potential is substantial, with a clear path to multi billion dollar valuation through either strategic acquisition or IPO, driven by strong market demand and growing security needs.

The rising costs of data breaches (averaging \$4.45M) and increasing regulatory pressures further strengthen the investment thesis.

Investment Amount

The company seeks to raise \$10M at TBD terms, which will lead the company to profitability

WiKey's Market Opportunity & Industry Landscape

What specific problem does WiKey's solution solve?

The digital world faces two critical security challenges. In Web3, every blockchain and wallet depends on secret keys that can be lost or stolen, while custodial solutions create massive central points of failure. This forces users to choose between risky self-management of seed phrases or trusting custodians who can't even insure appreciating assets like Bitcoin.

Meanwhile, in Web2, the rise of AI has supercharged identity theft and account takeover attacks. Traditional authentication methods rely on personal data, passwords, and recovery processes that are vulnerable to sophisticated impersonation attacks.

Wikey solves both challenges with a revolutionary zero-trust approach.

For Web3, we enable true self-custody without seed phrases to manage or back up, eliminating both key vulnerabilities and custodial risks.

For Web2, our authentication system removes personal data from the equation, making AI impersonation and social engineering attacks impossible.

Using decentralized technology and social recovery without collusion risks, Wikey provides enterprise-grade security that scales with asset value while remaining simple to use.

What is the WiKey Product Proprietary Advantage

At its core is the patent-protected Zero-Trust Key Swap technology that enables secure key regeneration without backups or central storage.

The company has filed patents covering its decentralized authentication methods, social recovery mechanisms, and zero-knowledge security protocols.

The AI-Proof Authentication Engine represents a significant technological breakthrough in preventing AI impersonation without relying on personal data, while the proprietary decentralized recovery protocol enables secure account recovery without collusion risks.

The technology stack has been developed by a team with deep expertise in cryptography and multiple successful exits, led by a CEO with dozens of security and blockchain patents. This combination of patents, proprietary technology, and network effects creates significant barriers to entry and provides sustainable competitive advantages.

WiKey's Web2 Cyber Security Market Overview

The digital identity and authentication market is experiencing significant growth and transformation. Here are key references to the market's current state and future projections:

Web2 Market Size, Growth and References

The digital identity solutions market is projected to grow substantially in the coming years: From \$33.36 billion in 2025 to \$65.61 billion by 2029, with a CAGR of 18.4% [1](#).

Another projection suggests growth from \$42.12 billion in 2024 to \$133.19 billion by 2030, at a CAGR of 21.2% [ref](#).

A different estimate values the market at \$27.9 billion in 2023, with an expected CAGR of over 16% between 2023 and 2032 [ref](#).

Key Drivers and Trends

Several factors are driving the growth of this market:

1. Increased cybersecurity concerns: Rising incidents of identity fraud and data breaches are fueling demand for robust identity verification solutions [ref](#), [ref](#).
2. Technological advancements: Integration of AI, machine learning, and blockchain is creating new opportunities in the market [ref](#).
3. Biometric authentication: There's a growing adoption of biometric devices and advanced authentication techniques across various sectors [ref](#).
4. Regulatory compliance: Stringent data protection regulations are driving organizations to implement robust digital identity solutions [ref](#).
5. Digital transformation: The rapid digitalization across sectors, especially in Asia Pacific, is contributing to market growth [ref](#) [ref](#).

Regional Insights

Asia Pacific is experiencing the highest growth rate in the digital identity solutions market, driven by increased digital transformation and rising incidents of cyber fraud [ref](#).

The market is expected to continue its growth trajectory, with several trends shaping its future:

- Complex biometric verification and liveness detection [ref](#).
- Multi-layered defense systems [ref](#).
- Increased use of AI and machine learning in identity verification [ref](#).
- Potential obsolescence of physical IDs in favor of digital identity verification technologies [ref](#).

As the digital landscape evolves, the digital identity and authentication market is poised to play a crucial role in ensuring secure and seamless digital interactions across various sectors.

WiKey's market opportunity

The combined market opportunity for Wikey spans both digital asset security and digital identity authentication sectors, presenting a significant growth potential.

The digital asset security market encompasses \$3T in assets requiring protection, growing at 35% CAGR, driven by increasing institutional adoption and regulatory requirements, with \$3.8B lost to hacks in 2023 highlighting the urgent need for better solutions.

The digital identity and authentication market currently stands at \$26B (2024) and is projected to reach \$70B by 2027, growing at 25% CAGR, fueled by rising AI threats, remote work adoption, and digital transformation, with data breaches costing an average of \$4.45M per incident. Within these markets, Wikey targets an enterprise security segment of \$10B and a consumer protection market of \$5B, focusing on key growth sectors including financial institutions, cryptocurrency funds, enterprise organizations, and high-net-worth individuals. The market shows a clear trend away from centralized custody solutions and traditional authentication methods, aligning with Wikey's decentralized, zero-trust approach.

The Addressable and Obtainable Market

We will analyze the total addressable market (TAM), the serviceable addressable market (SAM), and serviceable obtainable market (SOM)

The digital security market presents a massive opportunity with a Total Addressable Market (TAM) of approximately \$3.026 trillion, combining the \$3 trillion Web3 security market for cryptocurrency assets and the \$26 billion Web2 digital identity market, which is projected to reach \$70 billion by 2027.

Within this, our Serviceable Addressable Market (SAM) is approximately \$310 billion, consisting of \$300 billion in institutional and high-net-worth crypto holdings requiring enhanced security, plus \$10 billion from enterprises needing advanced authentication solutions.

Our initial Serviceable Obtainable Market (SOM) targets \$5 billion, focusing on four key segments: financial institutions handling digital assets, cryptocurrency funds and exchanges, enterprise organizations with critical authentication needs, and high-net-worth individuals with significant crypto holdings.

Our revenue model is built on a freemium service with enterprise tiers, averaging \$5-20 per user per month, with enterprise licensing scaled based on security needs and user volume.

How fast this specific identity theft and key protection market is growing? What are the key trends driving its growth?

The digital security market is experiencing unprecedented growth, driven by converging trends in both Web3 and Web2 spaces.

In the Web3 sector, institutional Bitcoin adoption is accelerating through ETFs and corporate treasuries, while the overall cryptocurrency market cap has reached \$2.5T and continues to rise.

The increasing frequency and sophistication of crypto hacks (\$3.8B stolen in 2023) alongside regulatory pressure for better custody solutions is forcing the industry to seek more secure solutions.

Meanwhile, in the Web2 space, AI-powered attacks are growing 300% annually, while remote work expansion and digital transformation are increasing authentication needs.

With data breaches now costing \$4.45M per incident (2023), organizations are rapidly shifting from traditional password-based to more secure authentication methods.

The combined market is projected to grow at 35% CAGR over the next five years, driven by rising cybersecurity insurance costs, stricter regulatory compliance requirements, evolving AI threats, accelerating digital asset adoption, and ongoing enterprise digital transformation.

What regulatory changes might impact the industry?

The digital security and cryptocurrency industry faces a complex and evolving regulatory landscape that's driving significant changes in both custody and authentication requirements.

The SEC is pushing for stricter custody standards for digital assets, while the FDIC's inability to insure appreciating assets like Bitcoin creates challenges for traditional custodians.

In Europe, MiCA regulations are demanding enhanced custody solutions, alongside a global push for clear separation of customer assets and proof-of-reserve requirements.

On the authentication front, the EU Digital Identity Framework and US FedNow are mandating stronger security measures, while GDPR and privacy laws are limiting personal data usage in verification processes.

NIST guidelines are increasingly favoring passwordless authentication, reflecting a broader shift away from traditional security methods.

These regulatory changes are making it difficult for traditional custodians and banks to maintain compliance while highlighting the growing need for self-custody solutions that can protect against AI-driven threats.

Wikey's decentralized, zero-trust approach aligns with these regulatory trends by providing compliant security without personal data exposure or central points of failure.

The main competitors, and how is WiKey different?

The digital security landscape is divided between Web3 custody solutions and Web2 authentication providers, each with significant limitations.

In the Web3 space, hardware wallets like Ledger and Trezor rely on vulnerable seed phrases, while custodial services such as Coinbase and BitGo create central points of failure.

Multi-sig solutions like Casa and Unchained offer enhanced security but require complex setup and still need key backup, and smart contract wallets like Argent and Safe remain dependent on specific blockchain networks.

In the Web2 authentication market, password managers like LastPass and 1Password remain vulnerable to breaches, while 2FA providers such as Google and Authy can be bypassed through recovery processes.

Biometric solutions like Clear and Apple require personal data, and identity providers such as Okta and Auth0 operate through centralized systems.

Wikey differentiates itself by eliminating seed phrases and secrets entirely, requiring no personal data for authentication, and using a decentralized architecture that removes single points of failure.

This unique approach makes it AI-proof by design, as there's no data available for impersonation, while working seamlessly across both Web2 and Web3 environments with a simple user experience despite its advanced security features.

Web2 - Why current solutions are inadequate and how WiKey solves it

Web2 security faces critical vulnerabilities as authentication and account recovery relies on personal information that can be stolen, bought on dark web, or gathered from social media - data that once compromised can't be changed.

Password-based systems are vulnerable to phishing, cracking, and data breaches, while password recovery depends on the same compromised personal data.

Password managers create central points of failure, and 2FA via SMS/email can be intercepted.

Some Android or iOS apps act maliciously by sending incoming text messages to hackers, to initiate and intercept the recovery process.

The rise of AI makes impersonation attacks increasingly sophisticated through deepfakes and convincing phishing, with personal data feeding these AI attacks.

WiKey fundamentally changes this by requiring no personal information or passwords in its authentication process and at any other period of time - there's nothing to steal, buy, or gather, no central database to hack, and no fuel for AI impersonation.

WiKey also does not use database to store any critical information, which means that the platform is protected from hacking or changing the user's configurations.

By removing what attackers target rather than building better walls around vulnerable information, WiKey delivers true zero-trust security that's inherently resistant to both current and emerging threats.

Web3 - Why current solutions are inadequate and how WiKey solves it

Hardware Wallets:

While hardware wallets like Ledger or Trezor provide better security than software wallets, they don't solve the fundamental problem: you still need to backup your seed phrase.

This backup becomes the critical vulnerability - a single point of failure that could compromise all digital assets.

If someone finds your seed phrase backup, they can bypass the hardware wallet entirely.

Additionally, if you lose the backup, you lose access to all your assets.

Multi-Signature Wallets:

Multi-sig seems to improve security by requiring multiple keys for transactions. However, it actually multiplies the backup problem.

Instead of protecting one seed phrase, you now need to securely store multiple keys, often for years. Each key needs to be backed up and protected from collusion, loss and theft. The more keys you need to protect over time, the higher the risk that one will be compromised or lost.

How WiKey Solves This:

WiKey takes a fundamentally different approach by eliminating the need for seed phrases or key backups entirely.

Instead of trying to help users protect secret keys (which will always be vulnerable), WiKey's decentralized system generates keys when needed without ever requiring storage or backup. This removes the core vulnerability - there are no secrets to steal or lose in the first place.

What are the biggest barriers to entry?

The barriers to entry in secure digital authentication and asset protection can be broken down into a focused paragraph:

Developing a secure, decentralized authentication system requires significant technical expertise in cryptography, zero-trust architecture, and blockchain technology - areas where experienced talent is both rare and expensive.

The solution must also achieve regulatory compliance across multiple jurisdictions while maintaining a delicate balance between institutional-grade security and user-friendly operation.

Building trust in the financial sector is particularly challenging, as institutions require extensive proof of security through audits, certifications, and proven track records before adopting new technology for critical authentication or asset protection.

WiKey filed for IP protection.

Patent protection for key technological innovations creates another significant barrier, as does the need for substantial capital to fund development, security audits, and go-to-market strategies.

Additionally, the complex network effects in both Web2 and Web3 markets mean that any new solution must achieve user adoption to become viable, while competing against established players with deep pockets and existing market relationships.

Business Model & Revenue Generation

Overview

Wikey employs a multi-tiered revenue model starting with a freemium base that offers basic authentication features and limited digital asset protection to individual users at no cost, driving initial adoption and network effects.

The premium tier, priced at \$5-\$50/user/month, provides enhanced features like collusion prevention, increased number of helpers, priority support, and additional security options, targeting a 5-15% conversion rate from free users.

Enterprise offerings are structured in three tiers: Standard Enterprise (\$15-25/user/month) providing full security features and basic integration support for up to 1,000 users; Advanced Enterprise (\$25-50/user/month) offering custom integrations and enhanced SLA for up to 10,000 users; and Financial Institution Tier (\$100+/user/month) delivering custom security features, dedicated support, premium SLA, and unlimited users with pricing based on assets under protection.

Additional revenue streams include API access fees, integration services, custom development, and security consulting, creating a comprehensive monetization strategy that scales with client needs and usage.

WiKey's revenue model

Wikey employs a multi-tiered revenue strategy centered on a freemium SaaS model. The basic tier is free for individual users, with low demand, driving initial adoption and network effects, while premium features are available through subscription tiers averaging \$5 per user per month.

Enterprise clients are served through customized licensing agreements based on user volume, security requirements, and integration needs, with pricing typically ranging from \$15-50 per user per month.

For financial institutions and cryptocurrency funds, custom enterprise solutions include additional security features and dedicated support, commanding premium pricing of \$100+ per user per month or custom pricing based on assets under protection.

Additional revenue streams come from API access fees for developers integrating Wikey's authentication system into their applications, and consulting services for enterprise-level implementations.

The model is designed to scale with client growth while maintaining high margins due to the automated, decentralized nature of the technology, requiring minimal incremental costs per user.

This approach allows for predictable recurring revenue while capturing value proportional to the security risks being mitigated.

WiKey's plan to scale revenue over time

Wikey's revenue scaling strategy follows a carefully planned three-phase approach.

The initial phase (Years 1-2) targets high-value early adopters such as crypto funds and financial institutions, focusing on enterprise clients with critical security needs while building API partnerships and launching a freemium model to drive user adoption.

The growth phase (Years 2-3) expands the enterprise customer base across industries, increases average revenue per user through premium features, scales Web2 authentication market penetration, and develops strategic partnerships with financial institutions.

In the acceleration phase (Years 3-5), Wikey plans to roll out institutional-grade features for mass adoption, enter new geographic markets with localized solutions, launch additional security services based on core technology, and integrate with major enterprise authentication systems.

Key revenue scaling metrics include targeting 100% year-over-year enterprise customer growth,

increasing premium user conversion from 5% to 15%, expanding average contract value from \$50K to \$500K, and achieving 40% annual revenue growth through upselling, all while driving adoption through network effects.

WiKey's unit economics

We will analyze the CAC, LTV, churn rate, payback period.

Wikey's unit economics demonstrate strong potential for sustainable growth and profitability.

Customer Acquisition Costs vary significantly by segment:

We estimate that cost of acquisition should range from \$15,000-25,000 for enterprise clients, \$50-100 for premium users, and \$5-10 for freemium users, with blended CAC trending downward as network effects take hold.

We estimate that the lifetime Value with enterprise clients will be at \$500,000+ over 3-5 year contracts and premium users at \$1,000+ with average 3-year retention, resulting in LTV/CAC ratios of 8:1 for enterprise and 10:1 for premium customers.

Churn rates should be low at under 5% annually for enterprise clients and 15% for premium users, primarily due to deep security integration and increasing network effects.

The payback period is efficient at 6-8 months for enterprise clients and 4-6 months for premium users, driven by high margins and improving with scale and automation.

In our freemium model aims for a 5% conversion rate to premium, contributing to overall user growth and network effects.

Partnerships or key client relationships

The company is in planning initial beta in Q2/2025 and is in the process of obtaining distributors. The product can be currently downloaded from the Android and iOS app stores and be enabled for select customers

What is the expected break-even point?

Wikey projects reaching break-even within 18-24 months, targeting Q4 2026 based on current financial projections and unit economics.

The monthly cash burn is planned to consist of \$200K for R&D and development, \$150K for

sales and marketing, and \$100K for operations and support, totaling \$450K monthly.

The path to break-even relies on securing 10-15 new enterprise clients per quarter at an average annual contract value of \$200K, alongside growing the premium user base by 1,000+ users per month at \$5 per user monthly.

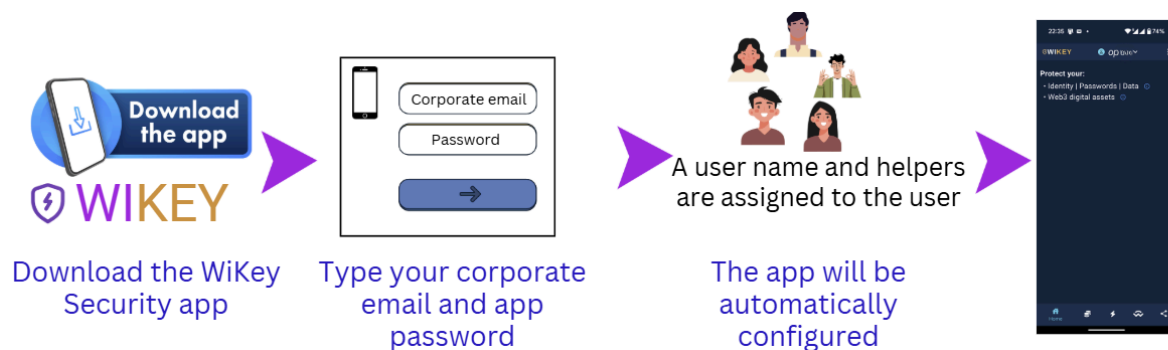
To achieve break-even, Wikey needs to reach approximately 50 enterprise clients (generating \$10M ARR) and 20,000 premium users (contributing \$1.2M ARR), for a total required ARR of \$11.2M.

This goal is achievable due to the scalable nature of the technology, which requires minimal incremental costs per user thanks to its automated, decentralized architecture.

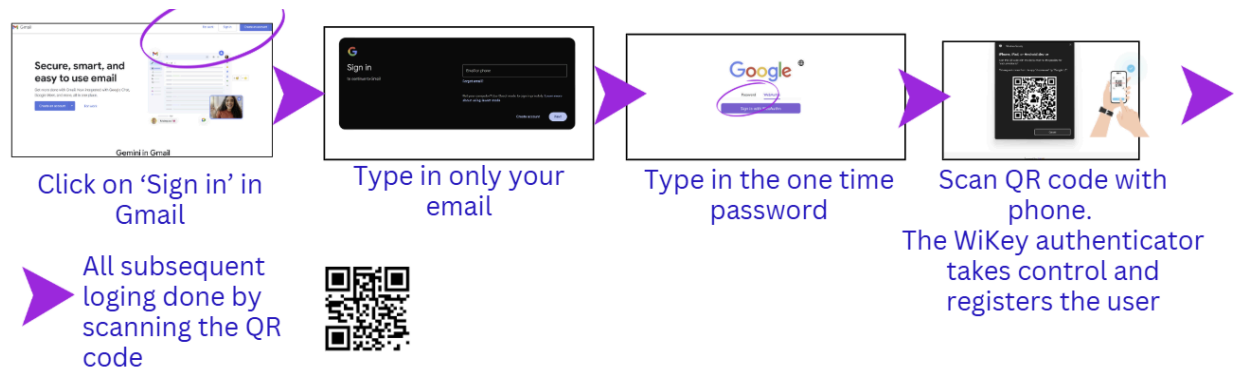
Product & Technology

WiKey's Authenticator installation and login demo

Installation & Configuration

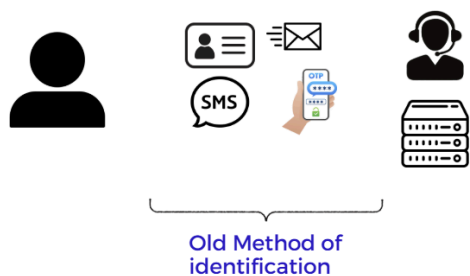


Example: Register user to GMail Service



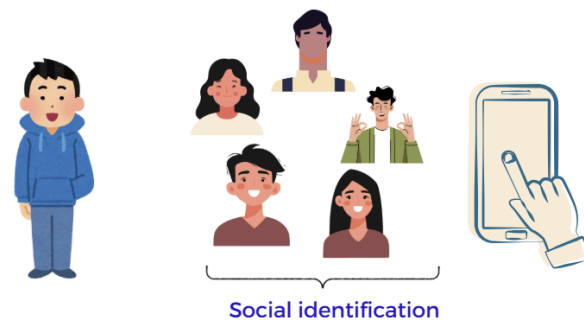
Recovery Old vs. WiKey's consensus recovery

On Password Loss



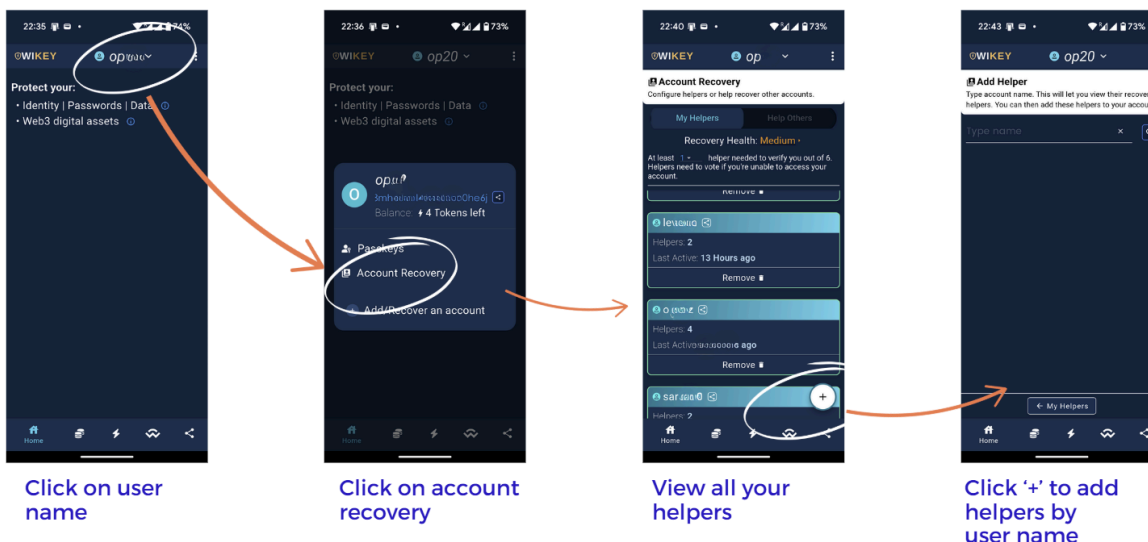
User (or impersonator) contact customer support or a remote computer to identify himself via text, email or ID

Activated On Phone Loss

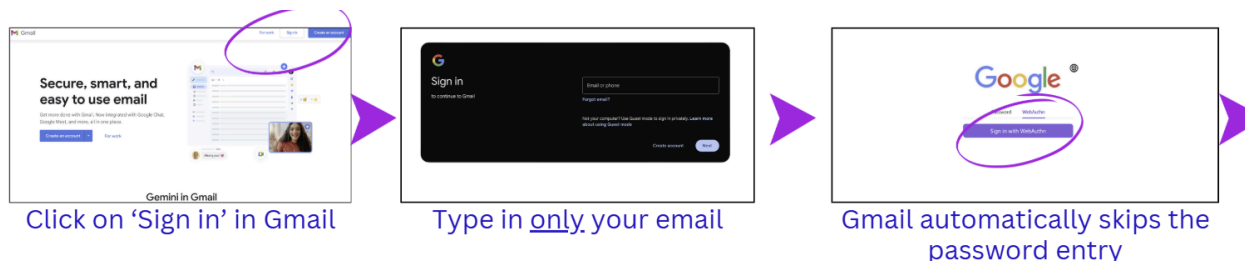


Friends or co-workers identify the user, Click on his name in their app to authorise the new secret key

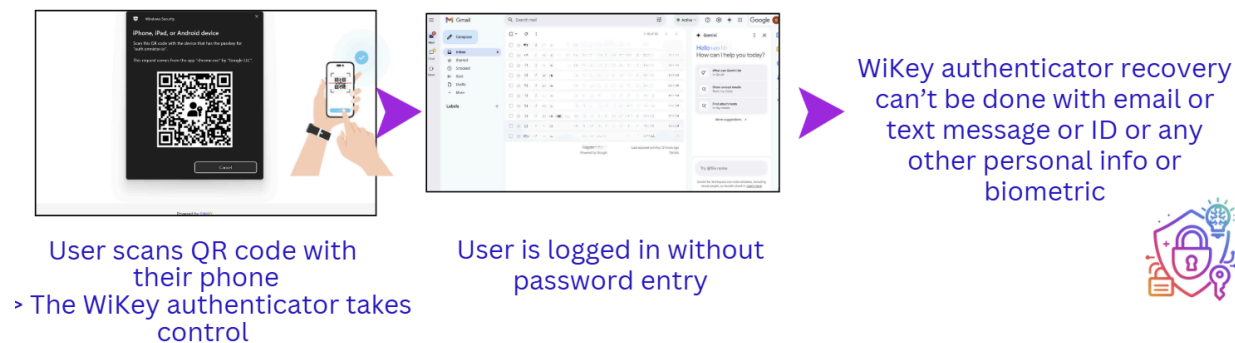
How to add a helper with the WiKey app



Example: Login to Gmail



Example: Login to Gmail (2)



Core technology

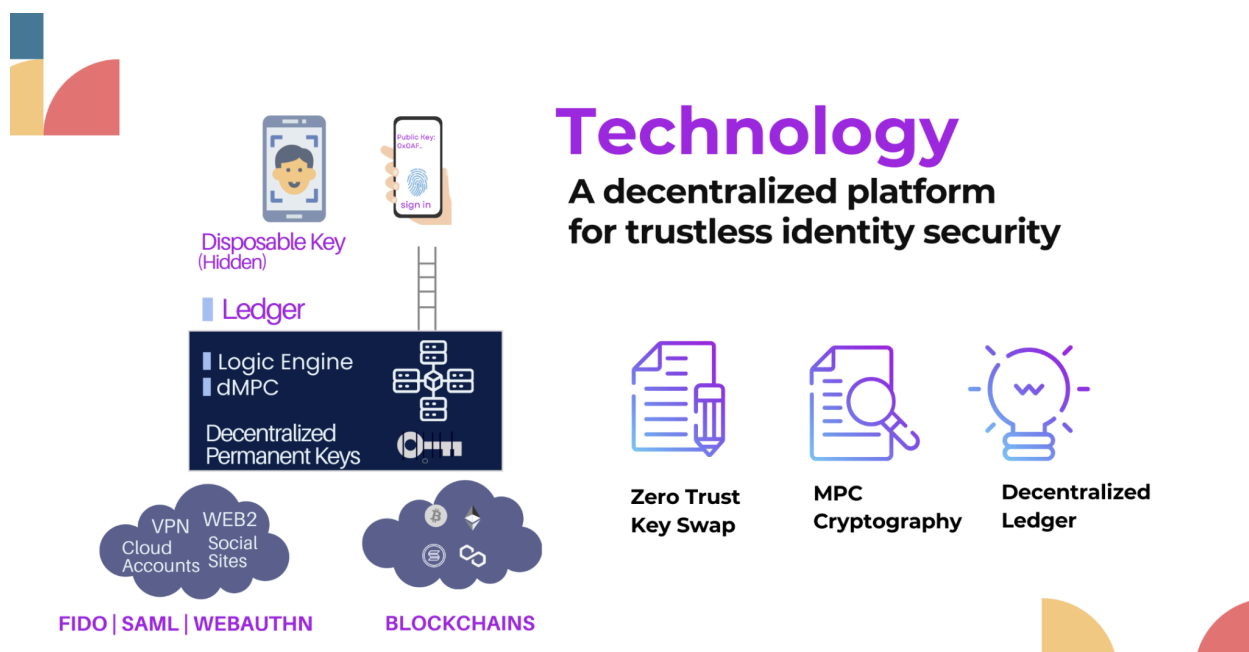
Wikey's core technology is built on three fundamental pillars that work in concert to deliver unprecedented security. At its heart is a proprietary Zero-Trust Key Swap Technology that eliminates the need for seed phrases or key backups, storing keys only on the user's device while enabling secure key regeneration if the device is lost, all without relying on personal data or central servers.

This works in conjunction with Multi-Party Computation (MPC) Cryptography, which distributes security across multiple parties, preventing single points of failure and enabling secure social recovery without risk of collusion attacks.

MPC by itself is vulnerable to man in the middle or impersonation attacks. WiKey solves it by shielding all communication to the MPC with messages that are signed with a temporary key

The third pillar is a Decentralized Ledger that provides transparency and immutability while ensuring secure key protection without relying on any single entity, recording authentication events without storing sensitive data.

Together, these technologies create a unique security solution that prevents AI impersonation attacks, eliminates key vulnerability risks, enables true self-custody, and maintains enterprise-grade security that scales without compromising protection.



WiKey's authenticator development status

WiKey's security solution has reached a significant milestone: a functional demo version ready for beta testing and limited enterprise deployment.

The core technology - including zero-trust key management, decentralized authentication, and AI-proof security - is operational and demonstrable.

While the fundamental security architecture is proven, we're actively addressing stability challenges in certain high-load scenarios and scaling optimizations needed for broader deployment.

These refinements will be crucial as we move from limited enterprise trials to wider market adoption.

WiKey's proprietary technology and patents

Wikey has developed and protected a robust portfolio of proprietary technology, with IP filed covering its core innovations.

The centerpiece is the Zero-Trust Key Swap technology, a patented pending system that enables secure key regeneration without backups, along with the AI-Proof Authentication Engine that provides secure verification without personal data.

The company has filed IP protection for its Decentralized Recovery Protocol, which enables social recovery without collusion risks.

These core technologies are protected through a combination of IP including proprietary algorithms for key management, unique implementation of MPC cryptography, custom decentralized ledger architecture, and anti-impersonation verification methods.

Additional patents are currently in process for decentralized authentication methods, social recovery mechanisms, and zero-knowledge security protocols, while the company continues to develop new IP to enhance the privacy and security of its users.

Product roadmap for the next 12-24 months

Wikey's 24-month product roadmap is structured in four strategic phases designed to ensure stable market entry and scalable growth.

The first phase (Months 1-6) focuses on beta launch and initial enterprise deployment, including stabilizing the core platform, addressing scaling issues, completing initial security audits, deploying first enterprise integrations, and refining user experience based on feedback.

In the second phase (Months 7-12), Wikey will expand market presence by launching the full enterprise solution, releasing Web2 authentication integration with more protocols (SAML and Passkey already working), expanding crypto wallet compatibility, introducing API for the developer ecosystem, and scaling infrastructure for broader adoption.

The third phase (Months 13-18) concentrates on feature enhancement, including institutional-grade reporting, advanced compliance tools, enterprise management dashboard,

expanded social recovery options, and mobile SDK launch.

The final phase (Months 19-24) focuses on full-scale rollout with global expansion, advanced enterprise features, enhanced integration capabilities, additional authentication methods, and expanded platform support, positioning Wikey for comprehensive market coverage and sustained growth.

What security measures and compliance frameworks are in place?

The security architecture is built on multiple layers of protection, starting with zero-trust authentication that eliminates vulnerable personal data and secret keys.

Core security measures aim to include regular third-party security audits, penetration testing, and code reviews, also aiming for compliance frameworks cover SOC 2 Type II certification (in process), ISO 27001 alignment, and GDPR compliance.

The platform implements end-to-end authentication, secure key management without central storage, and AI-proof authentication protocols.

For financial institutions, Wikey aims to meet key regulatory requirements including SEC custody rules, European MiCA guidelines, and relevant KYC/AML frameworks.

The decentralized architecture ensures no single point of failure, while the social recovery system prevents unauthorized access through sophisticated verification protocols.

Enterprise deployments include additional security layers such as dedicated infrastructure, custom security policies, and real-time audit logs, all while maintaining zero access to user keys or personal data.

Is the technology scalable for global expansion?

Wikey's technology is architected for global scalability through its innovative decentralized design that fundamentally differs from traditional authentication systems requiring central servers and database scaling.

The zero-trust approach distributes security load across the network, while automated key management and API-first design enable seamless integration with minimal infrastructure requirements.

The absence of central storage and no requirement for personal data or keys further enhances scalability potential.

However, current challenges include the need to optimize performance under high-load scenarios, stability improvements for larger deployments, and infrastructure scaling for enterprise-level demands, along with addressing various regional compliance requirements.

The global deployment strategy involves an initial focus on key financial and high risk enterprises, followed by a phased regional rollout supported by local partnerships with cyber security vendors for market penetration.

While the technology is fundamentally designed for global scale, certain stability and performance aspects require refinement before full-scale international deployment can be achieved.

Regulatory & Compliance Risks

What financial regulations apply to this Cyber security business?

Wikey's operations intersect with multiple regulatory frameworks across both cybersecurity and financial services.

For digital asset security, the company must comply with SEC custody requirements, CFTC guidelines for digital asset protection, and evolving stablecoin regulations.

On the authentication and identity front, key regulations include SOC 2 compliance for service organizations, GDPR and privacy laws governing personal data protection, NIST cybersecurity frameworks, and regional regulations like California's CCPA.

For financial industry clients, Wikey must address Basel requirements for operational resilience, FINRA cybersecurity guidelines, and banking regulations around third-party risk management.

The company's zero-trust architecture actually simplifies compliance in many areas since it doesn't store personal data and doesn't store keys centrally, but still requires ongoing monitoring of evolving regulations, particularly around AI security and digital asset custody.

International expansion brings additional requirements such as EU's DORA for financial sector cybersecurity, MiCA regulations for crypto-assets, and country-specific data protection laws, all of which must be continuously monitored and incorporated into the compliance framework.

WiKey's licenses and approvals

Wikey currently operates under standard business licenses and, due to its unique technological approach, does not require specific financial services licenses since it doesn't hold, custody, or transfer customer assets or funds.

The company's is planning to have the following regulatory status includes standard technology service provider agreements and information security certifications in process, including SOC 2 Type II audit underway, ISO 27001 certification planned, and verified GDPR compliance.

The decentralized, non-custodial nature of Wikey's technology deliberately avoids many complex licensing requirements that typically apply to traditional financial or cyber security

services providers.

Near-term licensing and certification plans focus on international business licenses for expansion, regional technology service certifications, industry-specific security attestations, and partner agreement frameworks.

What are the biggest regulatory risks in different target markets?

Wikey's regulatory risk landscape across different target markets presents several key challenges:

In the United States, the primary regulatory risks stem from evolving SEC and CFTC frameworks around digital asset security, potential new AI regulations affecting authentication systems, and varying state-level cybersecurity requirements.

The absence of clear federal guidelines for non-custodial security solutions creates regulatory uncertainty, while rapid changes in AI-related regulations could impact authentication protocols.

In the European Union, the main challenges come from strict GDPR enforcement, upcoming AI Act requirements, MiCA regulations for crypto-asset services, and DORA compliance for financial sector technology providers.

The EU's complex regulatory landscape requires careful navigation, particularly around data protection and AI usage in security systems.

Each jurisdiction presents unique compliance challenges for security technology deployment.

WiKey's handle consumer data and privacy compliance

Wikey's approach to consumer data and privacy is built on a fundamental "zero-data" principle that can be explained here:

The company's core technology is designed to operate without collecting or storing personal data, significantly simplifying privacy compliance.

No personally identifiable information (PII) is needed for authentication or recovery processes - users' keys are stored only on their devices, and the recovery process uses zero-knowledge proofs rather than personal information.

This architecture eliminates many traditional privacy compliance concerns since there's no central database of personal information to protect.

For enterprise deployments, all data is decentralized, ensuring that no one, even Wikey cannot access user secret key data.

The platform is inherently GDPR-compliant by design, as it collects no personal data to begin with, and meets CCPA requirements through its data-minimalist approach.

In cases where enterprise clients require audit logs, these are stored with zero-knowledge authentication, ensuring compliance without compromising privacy. This unique approach means that even in the event of a security breach, there would be no personal data exposure since none is stored in the first place.

Financials & Capital Efficiency

What are the projected financials for the next 3-5 years?

Wikey's financial projections over the next 5 years start with Year 1 (2026) targeting \$3M in revenue, split between enterprise clients (\$2.5M) and premium users (\$0.5M), while operating at a loss during market entry with a burn rate of \$250K/month.

Year 2 (2027) projects growth to \$15M, with enterprise revenue reaching \$12M and premium users contributing \$3M, aiming for break-even by Q4.

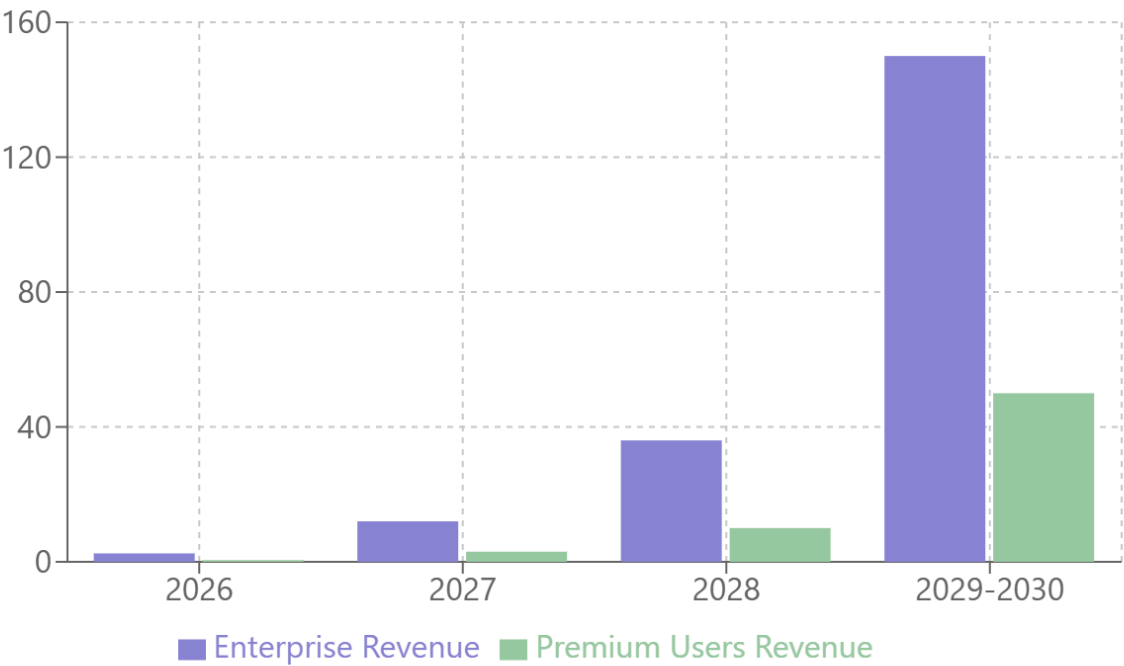
Year 3 (2028) forecasts significant scaling to \$45M total revenue (\$35M enterprise, \$10M premium users), marking the first profitable year.

Years 4-5 (2029-30) project substantial growth to \$120M-\$200M (\$90M-\$150M enterprise, \$30M-\$50M premium), with profit margins reaching 30-35%. Cash flow projections show break-even in Q4 2027, followed by positive cash flow in 2028, with 40% of revenue allocated to growth investment and 25% to R&D to maintain technological leadership and market expansion.

Wikey's financial projections over the next 5 years are structured as follows:

Year	Burn rate/month	Revenue Projections	Enterprise clients	Premium users
2026	\$250K	\$3M	\$2.5	\$0.5M
2027	\$250M	\$15M	\$12M	\$3M
2028		\$45M	\$36M	\$10M
2029-2030		\$120M-\$200M	\$90M-\$150M	\$30M-\$50M

WiKey Revenue Projections (USD Millions)



How much funding has the company raised so far, and from whom?

The company has raised so far ~\$1M from Ofir Paz

How will the investment be allocated?

Here's the detailed allocation plan for the \$10M investment:

Core Investment Areas:

Product Development: \$4M (40%)

- * Core technology optimization and scaling
- * Enterprise features development
- * Security enhancements and audits
- * User interface refinement

Team Expansion: \$3M (30%)

- * Engineering team growth
- * Sales and business development
- * Customer success team
- * Security specialists

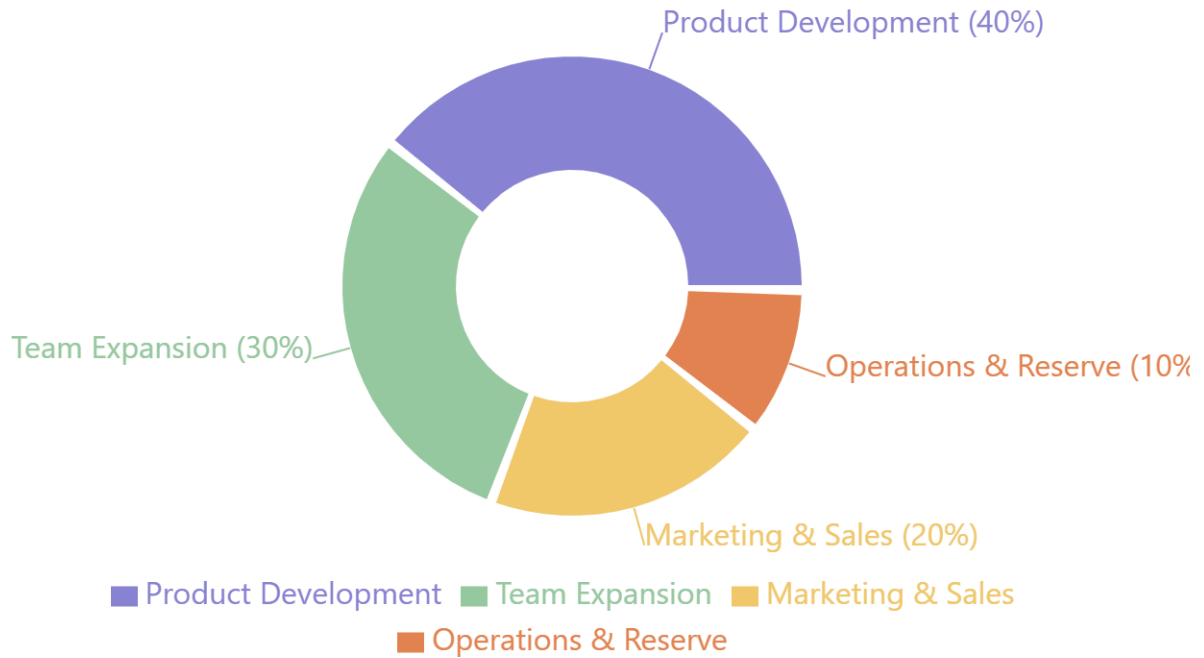
Marketing & Sales: \$2M (20%)

- * Enterprise client acquisition
- * Brand development
- * Industry partnerships
- * Market expansion initiatives

Operations & Reserve: \$1M (10%)

- * Infrastructure scaling
- * Office operations
- * Legal and compliance
- * Working capital reserve

Investment Allocation (\$10M)



18-Month Deployment Timeline:

Immediate: Security audits and core tech optimization

Months 1-6: Key hires and infrastructure scaling

Months 7-12: Market expansion and enterprise features

Months 13-18: Scaling operations and additional hiring

The expected return on investment (ROI) and exit strategy

Wikey's ROI and exit strategy analysis projects significant value growth from the initial \$10M investment, with break-even expected by Q4 2027.

The company's valuation is projected to scale from current \$30M (2024) to \$200M by 2026, reaching \$400M-\$800M by 2028, and potentially \$4B-\$5B+ by 2030.

The primary exit strategy focuses on strategic acquisition within 4-5 years by major financial institutions, enterprise security companies, or cloud service providers, with expected valuations at 8-10x revenue.

A secondary path considers IPO potential in 5-7 years, requiring \$200M+ annual revenue, strong growth metrics, and market leadership position.

Key value drivers include Wikey's proprietary technology portfolio, enterprise client base, recurring revenue model, high margins (30-35%), and growing market demand in both Web3 and Web2 security sectors.

Leadership & Team

Ofir Paz - CEO

- Serial entrepreneur with 2 successful exits (Microsoft acquisition and IPO)
- Hundreds of patents in security, operating systems, and blockchain
- Deep expertise in cryptography, operating systems and system architecture

Dr. Sara Alon Paz - Founder & Business Development

- One successful exit (NSPR)
- Proven track record in sales
- Extensive industry relationships

Levi Schechter - VP R&D

- Former Amdocs background
- Network security expertise
- Extensive experience in secure authentication systems

Key Advisors:

- David Schwed: Former Global Head of Digital Assets at BNY Mellon, CISO at Galaxy Digital
- Uri Stav: Cryptography expert, government and startup experience
- Shalev Keren: Cryptography researcher, MPC/ZK and Blockchain specialist

Technical Leads

- Ron Masuari and Kehat Megisidh: Technical experts in blockchain and smart contracts

Marketing Leads

The company is planning to hire top marketing experts to lead its B2B business

Growth & Customer Acquisition

WiKey's go-to-market strategy

The go-to-market strategy follows a dual-track approach targeting both Web3 and Web2 sectors, starting with high-value early adopters in the cryptocurrency and financial services industries.

The initial focus is on enterprise clients with significant digital asset holdings and critical authentication needs, leveraging the urgent demand for secure key management and AI-proof authentication.

Market entry begins with direct enterprise sales targeting crypto funds, financial and high risk institutions, and organizations facing AI-driven security threats, supported by strategic partnerships with key technology providers and system integrators.

A freemium model drives broader adoption and creates network effects, while API availability enables integration with existing enterprise systems.

The strategy emphasizes education about key security vulnerabilities and AI impersonation risks, positioning Wikey as the solution to these critical challenges.

Growth expansion targets include government agencies, healthcare institutions, and large enterprises requiring enhanced authentication security, with geographic expansion focusing initially on major financial centers before broader global rollout.

Sales efforts are supported by thought leadership content, industry event participation, and strategic advisory board relationships, while technical partnerships with major platform providers ensure seamless integration capabilities.

WiKey's customer acquisition channels

Wikey's customer acquisition strategy operates through multiple complementary channels, each targeting specific market segments with distinct efficiency metrics.

Direct enterprise sales serves as the primary channel for high-value clients, particularly crypto funds and financial institutions, achieving 30-40% conversion rates on qualified leads with a 3-4 month average sales cycle.

Partnership channels, including system integrators, technology partners, and financial service providers, generate 25-35% success rates through referrals, while digital marketing efforts through thought leadership content, security industry events, and technical webinars maintain a 15-20% lead conversion rate at lower cost.

The developer community channel, supported by comprehensive API documentation, developer portal, and open source software, drives ecosystem adoption and integration.

Channel economics show enterprise CAC at \$15,000-25,000, partner-driven CAC at \$8,000-12,000, and digital marketing CAC at \$50-100 per premium user, with overall acquisition

costs trending downward as network effects take hold and the product gains market recognition.

WiKey's cost of acquiring a customer (CAC) vs. customer lifetime value (LTV)?

Wikey's customer economics demonstrate strong unit metrics across both enterprise and premium segments.

In the enterprise segment, CAC ranges from \$15,000-25,000 per client, while delivering an LTV of \$500,000+ over 3-5 year contracts, resulting in an impressive LTV/CAC ratio of 20-25x.

With average enterprise contract values of \$200K annually and low churn rates under 5%, the enterprise payback period is 6-8 months.

The premium user segment shows equally strong metrics, with CAC of \$50-100 per user generating an LTV of \$1,000+ over a three-year average retention period, yielding an LTV/CAC ratio of 10-15x.

Premium users generate average revenue of \$60/year with 15% annual churn and a quick 4-6 month payback period.

Channel efficiency continues to improve as partner-driven CAC is 40% lower than direct acquisition, while network effects are steadily reducing overall CAC.

High retention rates are maintained through deep product integration, while strong upsell potential and growing contract values further enhance the long-term economic profile.

Competitive Landscape & Defensibility

WiKey's unique selling proposition

Wikey provides the first truly secure solution to the fundamental vulnerability in digital security: the management of secret keys and personal data.

Unlike traditional solutions that require users to protect vulnerable seed phrases or trust centralized custodians, Wikey's revolutionary zero-trust technology eliminates the need for key backups or personal data storage altogether.

This addresses two critical market needs: for Web3, it enables true self-custody of digital assets without key management risks; for Web2, it prevents AI-driven impersonation attacks by removing personal data from the authentication process.

The solution is unique in its ability to provide enterprise-grade security without secrets to protect, offering decentralized protection that scales with asset value while maintaining simplicity for users. No other solution in the market combines these features - elimination of seed

phrases, protection against AI impersonation, true self-custody, and enterprise scalability - in a single platform.

What is the risk of new entrants or disruptive innovations?

Wikey's defense against new entrants and disruptive innovations is built on multiple layers of protection, starting with patent-protected key swap technology and significant technical complexity in its zero-trust architecture.

The company builds competitive moats through network effects from its growing user base, deep enterprise integration barriers, and first-mover advantage in true keyless security.

However, potential vulnerability areas exist, including quantum computing breakthroughs, large tech companies entering the space and open-source alternatives.

To mitigate these risks, Wikey maintains a strong focus on R&D investment (25%-40% of the proceeds or revenue), actively monitors emerging technologies, rapidly integrates security enhancements, builds deep enterprise relationships, and maintains a defensive patent portfolio.

While the core technology enjoys significant protection through patents and technical complexity, the fast-evolving nature of security technology requires constant innovation and adaptation to maintain market leadership.

Exit Strategy & Liquidity

What is the expected timeline for an exit?

Wikey's exit strategy timeline can be outlined in a focused paragraph:

The company projects a 4-5 year path to exit, primarily targeting a strategic acquisition by 2028-2029. At this point, revenue projections of hundreds of millions and established market leadership in both Web3 and Web2 security sectors should attract strategic buyers including major financial institutions, enterprise security companies, or cloud service providers at valuations of 20-50x revenue (\$10B+ potential exit value).

This timeline aligns with market maturity projections for digital asset adoption and AI security needs.

A secondary path considers IPO potential in years 5-7 (2029-2031), requiring strong growth metrics, and clear market leadership.

The exit timeline is supported by projected milestones including break-even in Q4 2027, profitability in 2028, and significant enterprise client acquisition.

Key value drivers for exit include the proprietary technology portfolio, established enterprise

client base, recurring revenue model with 30-35% margins, and growing market demand for secure digital asset and identity protection solutions.

The most likely exit options

Wikey's exit strategy prioritizes three potential paths, with strategic acquisition in 2028-2029 as the most probable outcome.

This primary exit option targets major financial institutions seeking digital asset security capabilities, enterprise security companies expanding into blockchain/crypto, or cloud service providers adding security infrastructure, with expected valuations at 20-50x revenue (\$5B+ at projected revenue), driven by proprietary technology and enterprise client base.

A secondary IPO path in 2029-2031 would require achieving considerable annual revenue, demonstrated market leadership, and strong growth metrics, offering maximum value potential and independence but demanding more stringent performance metrics.

A tertiary option involves secondary sale to private equity firms, strategic investment funds, or larger security companies, potentially occurring prior to full exit but at lower multiples than a strategic sale.

The strategic acquisition path remains most compelling due to the high strategic value of Wikey's technology and enterprise relationships, coupled with the growing demand for secure digital asset and identity protection solutions.

Risks & Mitigation Strategies

The biggest risks

We will analyze the market, regulatory, technical and operational risks

Wikey faces interconnected risks across multiple dimensions that require careful management and mitigation strategies.

Market risks include cryptocurrency market volatility affecting adoption, enterprise hesitation in adopting new security technology, competition from large tech companies, changing customer preferences in authentication methods, and potential market slowdowns impacting enterprise spending.

Technical challenges center on addressing current stability and scaling issues, protecting against quantum computing threats to cryptography, preventing zero-day vulnerabilities in core technology, managing integration with legacy systems, and keeping pace with evolving AI threats.

The regulatory landscape presents risks through evolving digital asset custody regulations, changing authentication compliance requirements, cross-border data protection laws, new AI regulations affecting authentication, and regional licensing requirements. Operational risks involve meeting enterprise service level agreements, scaling customer support efficiently, maintaining security standards during growth, retaining key personnel, and managing rapid international expansion. The company's success depends on effectively balancing and addressing these interconnected risks while maintaining focus on core technology development and market expansion.

How does WiKey plan to mitigate these risks?

Wikey addresses its multi-faceted risks through a layered mitigation approach. Market risks are managed through diversification across both Web3 and Web2 sectors, ensuring revenue stability even during crypto market volatility, while building strong enterprise relationships to overcome adoption hesitation. Technical risks are addressed through significant R&D investment (25%-40% of proceeds or revenue), continuous security audits, and maintaining a robust testing environment for stability and scaling improvements.

The zero-trust architecture inherently mitigates many security risks by eliminating central points of failure and personal data storage.

Regulatory compliance is managed through a proactive approach, with the technology designed to be regulation-agnostic, requiring minimal adjustments for new requirements due to its data-minimal approach.

Operational risks are mitigated through automated processes, strategic hiring of key personnel with competitive packages, and a phased approach to international expansion.

What contingency plans are in place for economic downturns or funding shortfalls?

The primary defense is a lean operational structure with a relatively low burn rate (\$250K/month) and the ability to reduce non-essential spending by 30-40% if needed. The business model's high margins (30-35%) provide flexibility during downturns, while the recurring revenue from enterprise clients offers stable cash flow. Specific contingency measures include a 6-month cash reserve policy, pre-negotiated bridge financing options with existing investors, and

the ability to accelerate revenue through prepaid enterprise contracts.

The company can also implement a staged reduction plan if necessary: first reducing marketing spend (20%), then slowing hiring (maintaining critical technical teams), and finally scaling back non-core development while maintaining essential security and stability work.

Competitive analysis

Wikey's competitive landscape spans both Web3 security and Web2 authentication sectors, with distinct advantages over traditional solutions in each space.

In the Web3 sector, hardware wallet providers like Ledger and Trezor offer strong brand recognition but remain dependent on vulnerable seed phrases and physical devices, while custodial services like Coinbase and BitGo provide ease of use but create central points of failure. Multi-sig solutions such as Casa and Unchained enhance security but require complex setup and key backup.

In the Web2 authentication space, traditional 2FA providers (Google, Authy) face vulnerabilities to social engineering and SMS hijacking, password managers (LastPass, 1Password) risk central database breaches, and identity providers (Okta, Auth0) maintain vulnerable centralized architectures, AI threats and personal data risks.

Wikey differentiates itself through four key advantages: revolutionary technology that eliminates seed phrases entirely with patent-protected innovations; superior security architecture with no central point of failure or personal data exposure; simplified user experience that works seamlessly across Web2 and Web3; and unique market positioning that serves both individual and enterprise needs while remaining future-proof against emerging threats.

Appendixes

External Links to Presentation Technical and Marketing Materials

Link to this document	https://bit.ly/3X9L7yG
------------------------------	---

Website	wikey.io
----------------	---

WiKey for Web2 - Cyber Security

Presentation	https://bit.ly/3TExp44
---------------------	---

One Pager	https://bit.ly/4awFrm0
------------------	---

WiKey for Powering the Unbanked	https://bit.ly/4iQV2LL
--	---

WiKey for Web3 - Protecting Digital Assets

Web3 Presentation	https://bit.ly/3wNG5O8
--------------------------	---

Web3 Whitepaper	https://bit.ly/42gvqqE
------------------------	---

Patents submissions

2024	https://bit.ly/3X9L7yG
-------------	---