



Making Everything  
Quantum-Safe



# Disclaimer

Certain statements in this presentation may constitute "forward-looking" statements which involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of the Company, or industry results, to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. When used in this presentation, such statements use such words as "may", "will", "expect", "believe", "anticipate", "plan", "intend", "are confident" and other similar terminology. Such statements include statements regarding the Company's ability to grow revenues and margins, the business prospects of the Company's products, the future of quantum computers and their impact on the Company's product offering, the functionality of the Company's products and the intended product lines for the Company's technology. These statements reflect current expectations regarding future events and operating performance and speak only as of the date of this presentation. Forward-looking statements involve significant risks and uncertainties, should not be read as guarantees of future performance or results, and will not necessarily be accurate indications of whether or not such results will be achieved. A number of factors could cause actual results to differ materially from the matters discussed in the forward-looking statements, including, but not limited to, a delay in the anticipated adoption of quantum computers and a corresponding delay in Q-Day, the ability for the Company to generate sales, and gain adoption of the Company's products, the ability of the Company to raise additional financing if required, competing products that provide a superior product, competitors with greater resources and the factors discussed under "Risk and Uncertainties" in the company's Management's Discussion and Analysis document filed on SEDAR. Although the forward-looking statements contained in this presentation are based upon what management of the Company believes are reasonable assumptions, the company cannot assure investors that actual results will be consistent with these forward-looking statements. These forward-looking statements are made as of the date of this presentation, and the company assumes no obligation to update or revise them to reflect new events or circumstances.

This presentation contains statistical data, market research and industry forecasts that were obtained from third party web sites, publications and reports or are based on estimates derived from such publications and reports and the Company's knowledge of, and experience in, the markets in which it operates. The third-party publications and reports generally indicate that they have obtained their information from sources believed to be reliable, but do not guarantee the accuracy and completeness of their information. Actual outcomes may vary materially from those forecasts in such publications or reports, and the prospect for material variation can be expected to increase as the length of the forecast period increases. While the Company believes this data to be reliable, market and industry data is subject to variations and cannot be verified due to limits on the availability and reliability of data inputs and other limitations and uncertainties inherent in any statistical survey. Accordingly, the accuracy, currency and completeness of this information cannot be guaranteed. The Company has not independently verified any of the data from third-party sources included in this presentation or ascertained the underlying assumptions relied upon by such sources.



# Post-Quantum Cybersecurity

**June 2026**

We developed advanced post-quantum cryptographic technology that protects digital systems from the growing threat of quantum computers. Our patented and patent-pending IronCAP™ technologies provide long-term resilience against quantum-enabled attacks. By integrating our technologies into everyday products, from AI applications to remote access, email and digital-asset platforms, we deliver practical, quantum-safe products organizations can rely on today.

## **Stock Information**

<https://money.tmx.com/en/quote/ONE>

(TSXV: ONE | OTCQB: OONEF)

## **Company Website**

<https://www.01quantuminc.com/>



# Management and the Board



**Andrew Cheung**

President/CEO



**William Train**

Chairman &  
Board Member



**Brian Stringer**

CFO



**Tyson Macaulay**

Board Member/COO



**Alex Shpurov**

CTO



**Gary Kissack**

Board Member



**Professor Edoardo  
Persichetti**

PQC Advisor

# Q-Day Threat

## What is Q-Day?

Q-Day, moment quantum computers become powerful enough to break today's public-key cryptography (e.g. RSA, ECC), which protects all global communications, financial systems, and government infrastructure.

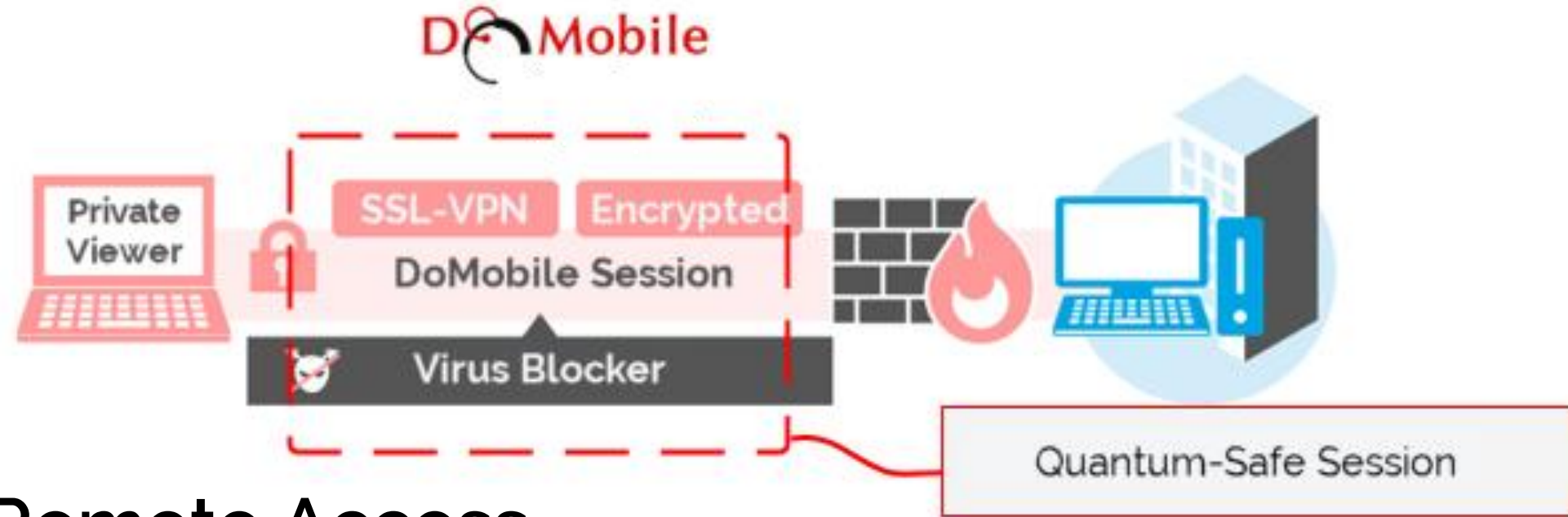
## Why Q-Day Matters?

- Shor's algorithm on quantum computer defeats RSA, ECC, etc.
- Everything on the Internet is vulnerable and must be protected before Q-Day – retroactive fixes won't work
- **Apple, Google, Microsoft, etc.:** Upgrading the infrastructures
- **US Government:** Issued NSM-10 formal warning against HNDL
- **Howard Lutnick, US Secretary of Commerce:** The worldwide cybersecurity will be totally broken by quantum computers if we don't act immediately
- **Jensen Huang of Nvidia:** "We are at the inflection point"
- **Vitalik Buterin of Ethereum:** "20% chance of Q-Day in 2029"



## Current Revenue Generators

1. Quantum-Safe Remote Access
2. Quantum-Safe Digital Assets
3. Quantum-Safe Email Security



Japanese patents  
4,875,094 | 5,832,027 | 7,328,969

## Quantum-Safe Remote Access

<https://www.hitachi-solutions-create.co.jp/solution/domobile.asp/>

**Remote access market:** \$0.8B in 2024 growing to \$1.4B by 2030 according to Grandview Research



### DoMobile Offering

- Agreement signed in June, 2025
- Commercial availability January 15, 2026
- First PQC remote access in Japan gives Hitachi a competitive edge in the Japanese remote access market
- Created by 01 Quantum for Hitachi



### Addressable Market

- HNDL attack is the biggest threat for remote access
- Server version (from ~USD5,000) | SaaS (~USD130 per year)
- TAM: **\$45M** in 2025 to **\$72M** in 2030 (assuming 5% of total)
- 01 Quantum received engineering fees plus ongoing royalty revenue sharing

# qVAULT

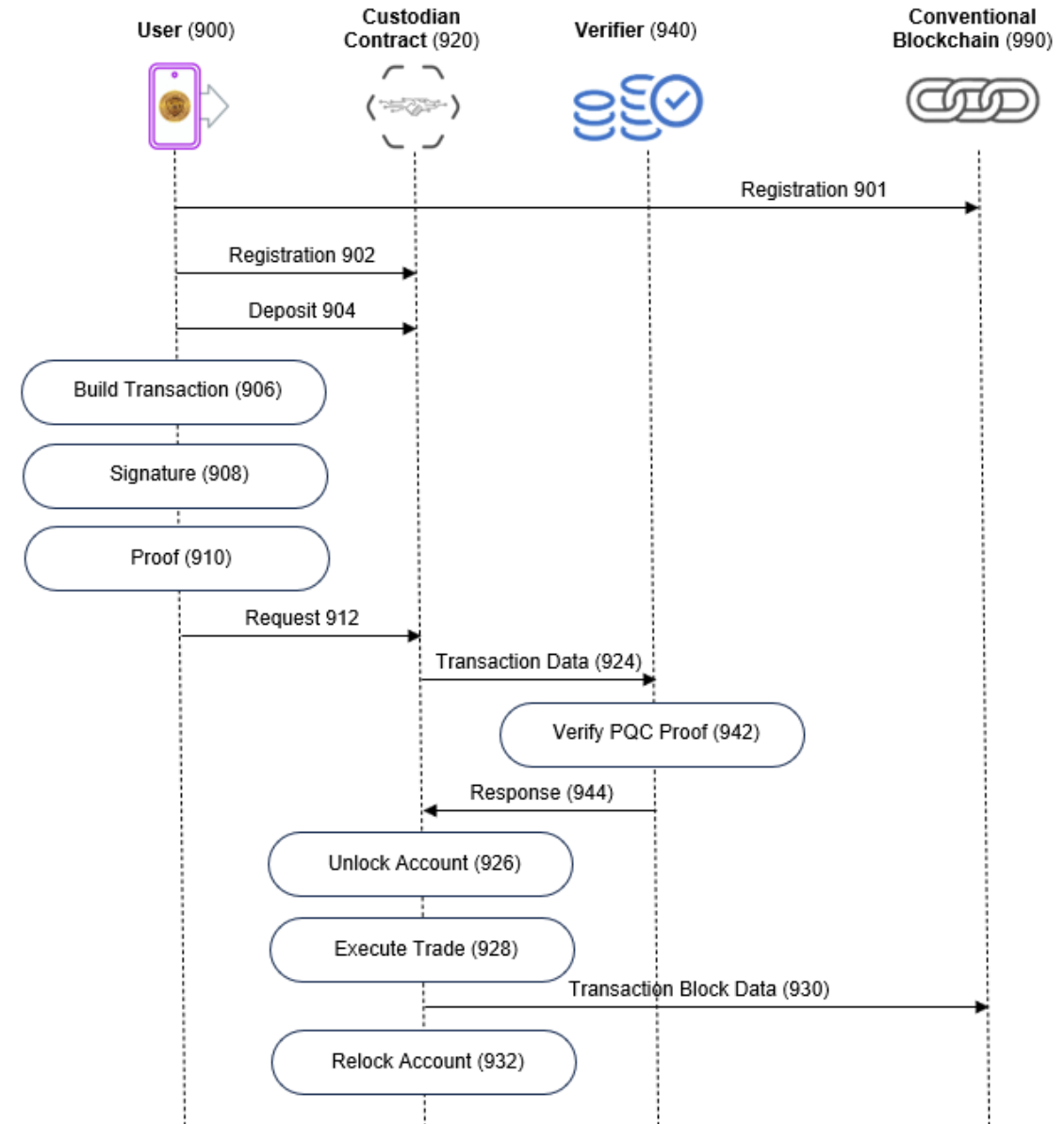
<https://www.qvault.qonetoken.io/>

## Quantum-Safe

- **HNDL**: A perfect storm brewing for global digital assets
- qONE tokens created by 01 Quantum for qLabs Foundation are based on our patent-pending QCW (19/344,357) and QDW (19/396,202) technologies

## Addressable Market

- \$qONE Token: Feb 2026 | qVAULT: June 2026
- \$4T digital assets must be quantum-safe before Q-Day
- \$qONE is the world's first "Quantum Gas Fee" utility token that users pay to **quantum lock/unlock** existing cryptos (e.g. ETH, SOL, HYPE, etc.)
- 01 Quantum receives development fees + ongoing royalty revenue + 22.5m \$qONE tokens



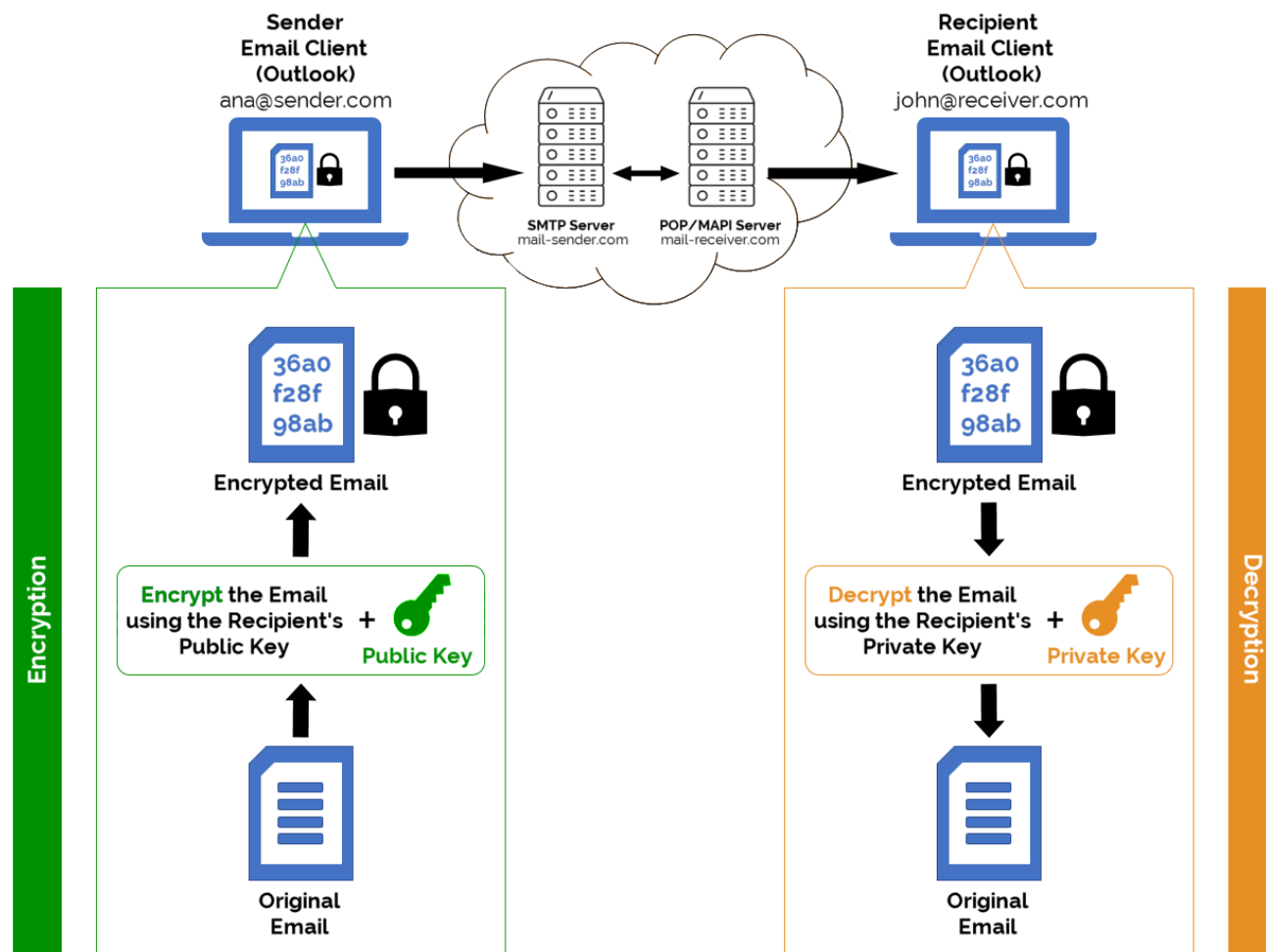
(TSXV: ONE | OTCQB: OONEF)





# Quantum-Safe Email Security

## End-to-End Encryption Model



## End-to-End Email Security

- Comply with FIPS-203 / FIPS-204 – **NIST endorsed!**
- End-to-End Quantum-Safe signature – **phishing killer!**
- End-to-End Quantum-Safe encryption – **true privacy!**
- Operates as an Outlook plugin – **mainstream ready!**



## Addressable Market

- MSLP: \$9.95 per month
- Channel: \$3 per month
- 730M business email addresses worldwide
- 10% paying \$3 per month = **\$2.6b** annual recurring revenue



# Quantum-Safe AI Security (2026-2027)





# AI Security Business Opportunity (pain points)



## Prompt Security & Privacy

Users ask questions that may be highly sensitive with personal or confidential business information, market, or proprietary basis. Risks include compliance risks, fiduciary risks, and potentially national security risks.



## AI Model Security

Exfiltration attacks threaten the intellectual property and know-how contained in specialized models.

# Solution: Quantum AI Wrapper (QAW)



## QAW Technology

- Encrypt both the user data and the AI model
- Using Full Homomorphic Encryption (FHE) technology
- Patent-protected (19/241,748)



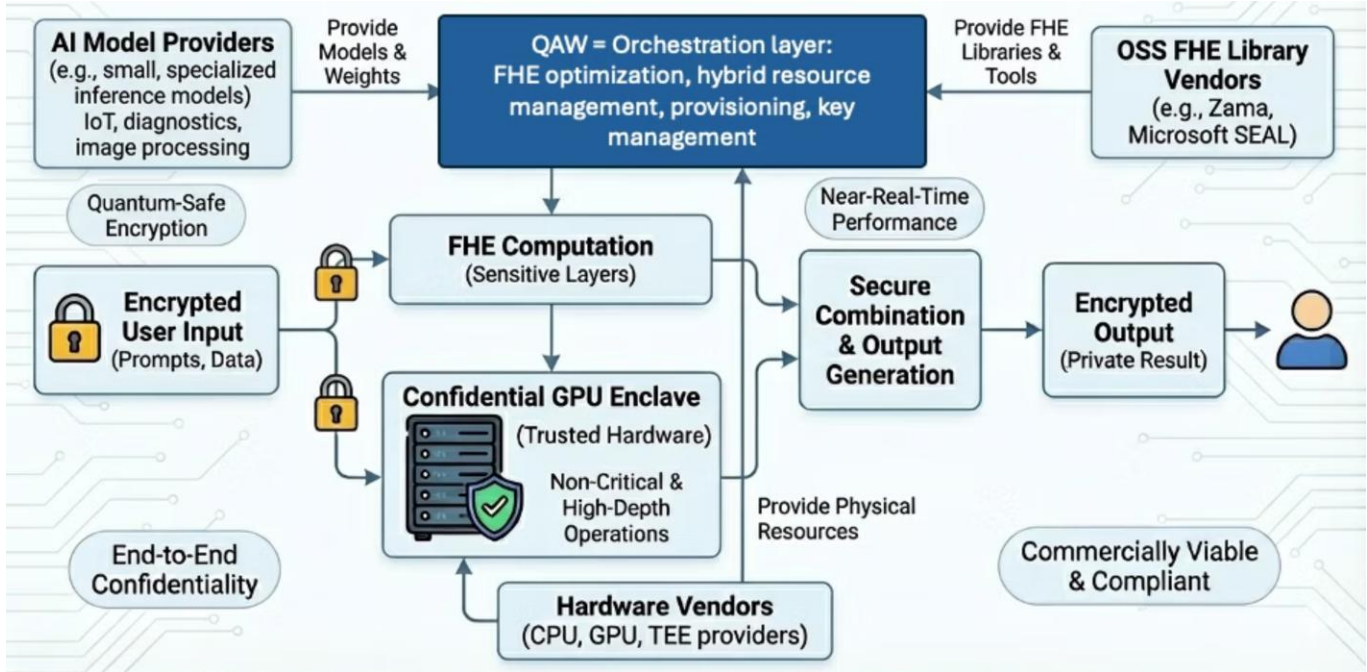
## Initial Addressable Market

- By 2027, companies will be 3x more likely to use SLM over LLM (source - Gartner) – amendable to FHE
- 2025 TAM for all AI models **\$0.9b** growing to **\$5.4b** by 2032 a 600% increase
- FHE is a subset – initial addressable market for FHE is **\$850m** through to 2028
- QAW target segments (Finance, Government, Health) represents **\$650m**



## Resulting Service Opportunity

- Open-Source Software (OSS) support SLA-agreement
- Professional Services
- Managed Services



(TSXV: ONE | OTCQB: OONEF)



# QAW: Product Positioning & Go-To-Market Strategy



## Value Proposition

- Model IP/User Privacy Protection via FHE
- Compliance & national security
- Dedicated / on-premise deployment
- AI Marketplace (SaaS)



## Business Model

- Community open-source (free)
- Professional/managed services
- Enterprise support
- AI Marketplace: **15%-25%** commission (similar to Amazon, eBay)



## Government Funding

- Provincial/Federal Innovation Funds
- Technology Procurement Program (e.g. Quantum Funds, Cyber Security Funds, AI Funds)



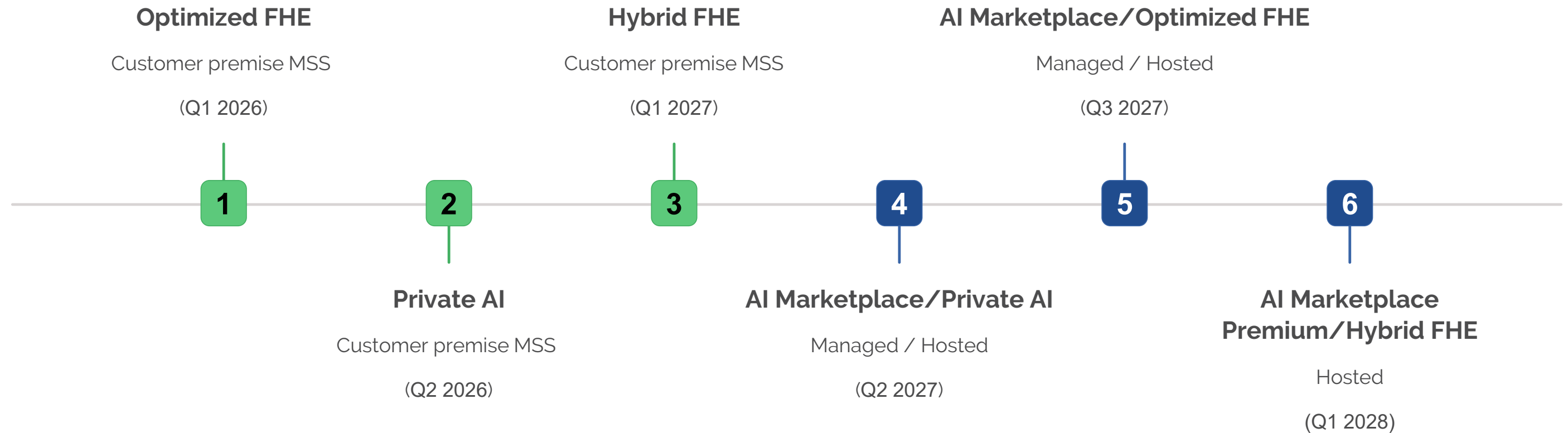
## Sales & Marketing

- PR, Contents, and Demand Generation
- Partner/Enablement/Field Events (e.g. TMLS)
- Direct sales: Financials | Government Procurement | Health
- Channel sales: Partner ecosystem | International

# QAW Roadmap (Q1 2026 - Q1 2027)

Dedicated instances / customer premise deployment

Hosted / SaaS



Assumption: Hybrid FHE is the most complex and last product variation to be introduced.

Assumption: Infrastructure comes from Data Centre partner (or we buy a Data Centre operator).

(TSXV: ONE | OTCQB: OONEF)





# Conclusion



# Global Partnerships

- We are their SME (Subject Matter Expert)
- Our partners have global customers with cybersecurity vulnerability
- Revenues: Engineering fees and/or royalty revenue sharing



# Market Value

## 01 Quantum

	Amount
Market Cap	\$70,000,000
52 Weeks High/Low	\$1.39 / \$0.19
Cash / Debt	\$3.1m / \$0

	Amount
Basic Shares	108,366,386
Options/Warrants	8,955,000 / 6,247,917
Cash burn (quarterly avg)	\$200,000

Comparison (Jun 3, 2026)	Market Cap
01 Quantum (ONE)	\$70m
Quantum eMotion (QNC)	\$1.0b
BTQ Technology (BTQ)	\$500m

## Stock Chart (01 Quantum – ONE.V) – June 3, 2026



(TSXV: ONE | OTCQB: OONEF)



# Timing = EVERYTHING!



Technological Ready



Commercial Ready

- Quantum market at its inflection point = AI market 2 years ago
- **Large TAM:** Quantum Threat must be addressed now (HNDL + NSM-10) with global PQC market expected to grow from \$0.4B in 2025 to over \$2.8B by 2030 (46% CAGR)
- **Under-Valued vs. peers:** Our Go-To-Market strategy is dev fees + rev sharing (no downside) – Revenue started in 2025
- **Leverage to a multi-segment:** First mover with practical, quantum-safe products across high-value segments like AI, Remote Access, Digital Assets, Email, etc.
- **World-class partners:** Hitachi, CGI, Thales, PwC, and others
- **Backed by strong IP:** Proprietary patent-protected/patent-pending technologies engineered to withstand Q-Day and aligned with NIST PQC FIPS standards



(TSXV: ONE | OTCQB: OONEF)

