

# 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 IronCAP X™, 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, IronCAP X™, the ability of the Company to raise financing to pursue its business plan, 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.



## Investor Summary (Spring 2022)

- **Encrypted remote communications for 20 years**
- **World leader in quantum-safe data encryption**
- **Multi-billion-Dollar Untapped Verticals**
- **Accepted and Endorsed by World-class Partners**



Tomorrow's Cyber Security, Today

**I R O N C A P**

# Remote communications Insecure

- ❑ Working from home has dramatically increased our remote access business user-base in Japan.
- ❑ 20 years long partners, Hitachi.
- ❑ Our remote access product is effectively paving the in-road for our IronCAP™ engine to be integrated, creating the world's first quantum-safe remote access product.

# Cyber Threats **we Solve**

## 1. Phishing and ransomware

- ❑ "57% of organizations experienced a successful phishing attack in 2020." - Proofpoint
- ❑ "Ransomware attacks cost an average of \$4.62 million (more than the average data breach costs)." - IBM
- ❑ "Cyberattacks are now the foremost risk to the global financial system..." - U.S. Fed Reserve Chair, Jerome Powell

# Cyber Threats **we Solve**

## 2. Nation state hacking and Blockchain

- ❑ “Securing NATO's communications for the quantum era is paramount to our ability to operate effectively without fear of interception.”  
- NATO's Cyber Security Centre
- ❑ \$330m worth of Solana was stolen.
- ❑ “Yes, most systems relying on cryptography in general are, including traditional banking systems.”  
- Bitcoin.org opensource

# Quantum Threat **has Arrived**

Quantum Computers are commercially available

- ❑ IBM released Q in **Jan 2019**
- ❑ Google Sycamore claimed Quantum Supremacy in **Oct 2019**
- ❑ Amazon launched Braket quantum service in **Dec 2019**
- ❑ Honeywell predicted x10/year **June 2020**
- ❑ UST of China released JiuZhang-2 in **October 2021**

“Quantum Race” between the open and the closed world

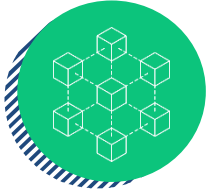
- ❑ Open world: IBM, Google, Honeywell, D-Wave, etc.
- ❑ Closed world: Billions have been invested by many nations

Grab-and-wait strategy presents serious threat

- ❑ Hackers seize data and incubate it pending future attack



# Addressable Market



## Blockchain Security (Token, DeFi, Metaverse)

- ❑ Tokens, NFTs, DeFi, Smart Contracts
- ❑ Token market size alone = **\$3 trillion**



## Financial Transactions

- ❑ E.g. 2b credit cards VISA/Master combined
- ❑ \$1 per year = **\$2b per year**



## Email Security (stop phishing)

- ❑ 730m active business email accounts globally
- ❑ \$10 per year = **\$7.3b per year**



- Website Security**
- Remote Access Security**
- IoT Devices Security**
- Digital Identity**



# IronCAP is the Solution



## Patent-Protected Innovative Technology

- ❑ Years of R&D with millions invested to create patent-protected, best-in-class, first-to-market, quantum-safe encryption technology



## Proven Technology

- ❑ Built on the 50-year time-tested Goppa code-based cryptography theory which has no cracking theory
- ❑ Survived 2 global hackathons in 2019-2021



## Seamless Integration

- ❑ IronCAP is compliant with the OpenSSL, PKCS#11, and OpenPGP industry standards that can be seamlessly integrated into existing PKI infrastructure

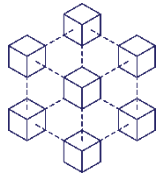




# Partnerships



# IronCAP Use Cases



## World's First Quantum-Safe Blockchain

- ❑ Engineering fees + 10% of token issued to validators
- ❑ To be completed in May/June



## Integration with Thales HSM

- ❑ Thales: Largest HSM manufacturer in the world
- ❑ Customers: Central banks, SWIFT, Defense, etc.



## World's first Quantum-Safe Bitcoin ATM

- ❑ Launched by a partner
- ❑ Completed in Jan 2021



## IronCAP X™ Email Security (killer of phishing)

- ❑ Free personal version: Available on [www.ironcap.ca](http://www.ironcap.ca)
- ❑ Business version (Summer): \$10/year/user



# Market Cap (USD) Comparison

Fully Diluted Shares	100m
Market Cap (in USD)	\$25m
52 Week High/Low	\$0.42 / \$0.20

Vertical	Name	Market Cap	Notes
Crypto Engine	Arqit	\$2,700m	Nasdaq
Email Security	Mimecast	\$5,000m	Nasdaq
Email Security	ZIX	\$500m	Nasdaq
Website Security	RSA	\$2,000m	Acquired (Mar/2020)
Remote Access	LogMeIn	\$4,300m	Acquired (Aug/2020)



# Timing is Everything

## Technology Leader

- ❑ Patent-protected and Commercially available
- ❑ Cybersecurity is front and center of every business
- ❑ World's first true quantum-safe end-to-end email security

## Inflection Point

- ❑ Rolling out globally with partners: CGI, PwC, Thales, Hitachi
- ❑ Cash burning stage behind us

