Anaxa

Reimagining communication with quantum IoT and blockchain

Quantum x Blockchain

Security Hacks

More points of failure are opened, leading to vulnerability in security hacks

Bandwidth Latencies

Increased latency issues with network traffic, specifically in IoT

Data Breach Increases

Data breaches leading to identity theft and financial loss

Healthcare Industry

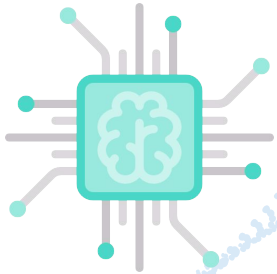
80,000 Cyber Attacks / Day

41 million Stolen Records / Year

$3.7 million USD / Breach

$6.2 billion USD Loss / Year

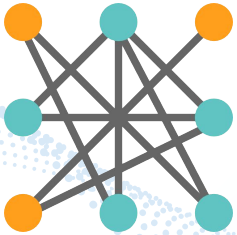
Solution



QKD Network

Quantum encryption with QKD for an unhackable, instantaneous network

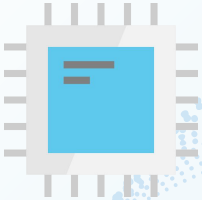
+



LBCP Layer

Blockchain-based platform with LBCP for decentralized trust

=

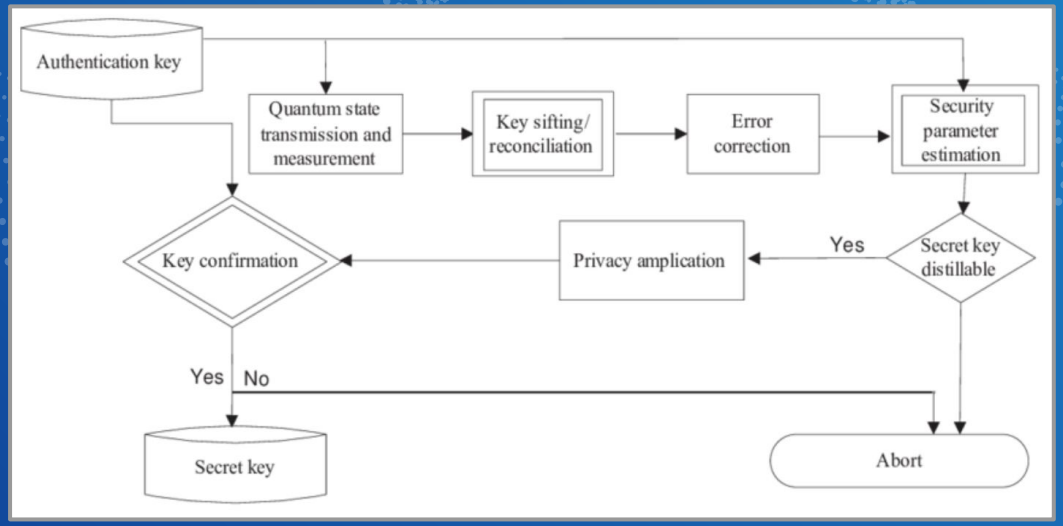


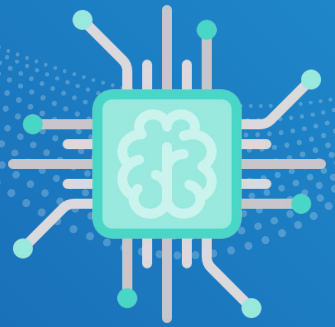
User platform containing secure storage system+ communication channels

Hardware

1 Implementable **Quantum Key Distribution** (QKD) Chips

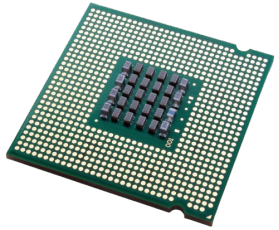
Secures Transmission Process





QKD Network

Uses quantum entanglement to generate an **unhackable, latent-free** key storing record information



QKD Transmitter Chip

Starts the entanglement

Produces the secure key

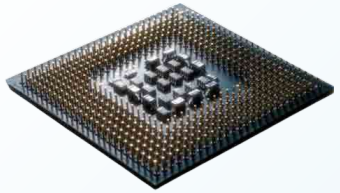
Material: Silicon Oxynitride

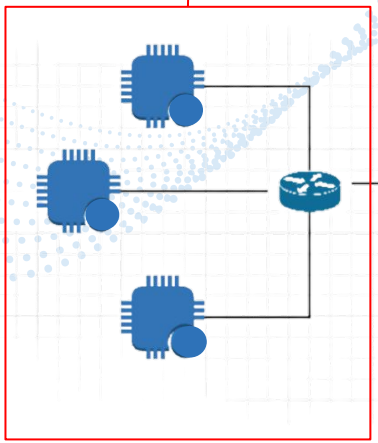
QKD Receiver Chip

Completes the entanglement

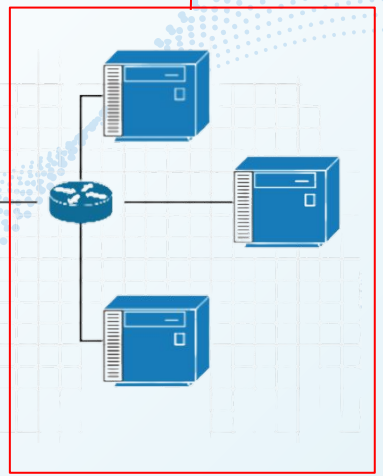
Receives/verifies the key

Material: Indium Phosphide





Data Transmission



qIoT device

Node

Datacenter

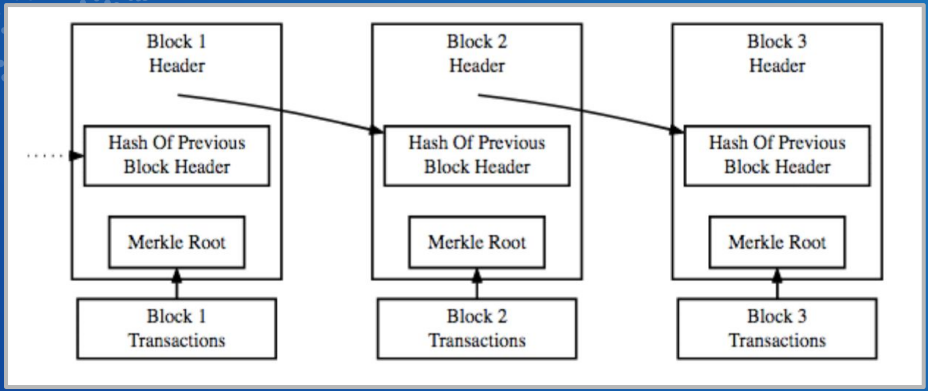
Anaxa

Software

1. Decentralized Storage with **Light Blockchain Communication Protocol** (LBCP)

Secures Storage Process

2. User Interface for Uploading Records



LBCP Layer

LBCP creates an **immutable, tamper-proof,** network with the user having **full ownership over** data

Device Scheme

Hospital

Data starts here

qIoT device

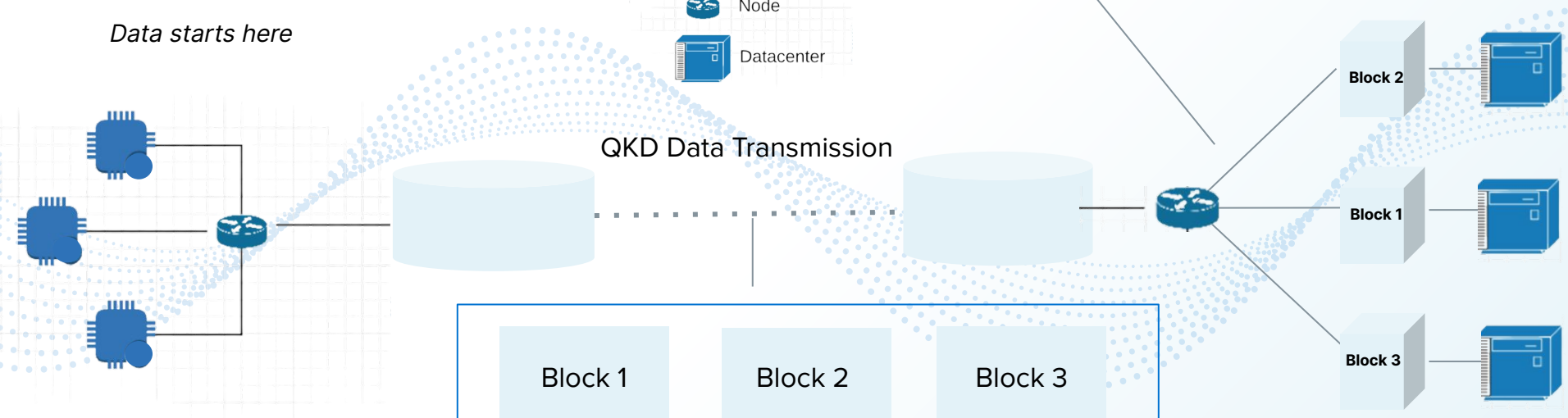
Node

Datacenter

Data is spread out across multiple nodes to reduce risk and prevent meaningful theft

Datacenter

Destination



Block 1	Block 2	Block 3
64KB	64KB	64KB

Light Blockchain Communication Protocol

Data is partitioned into equal sized “blocks” in sequential order, to put data in a decentralized platform

Anaxa

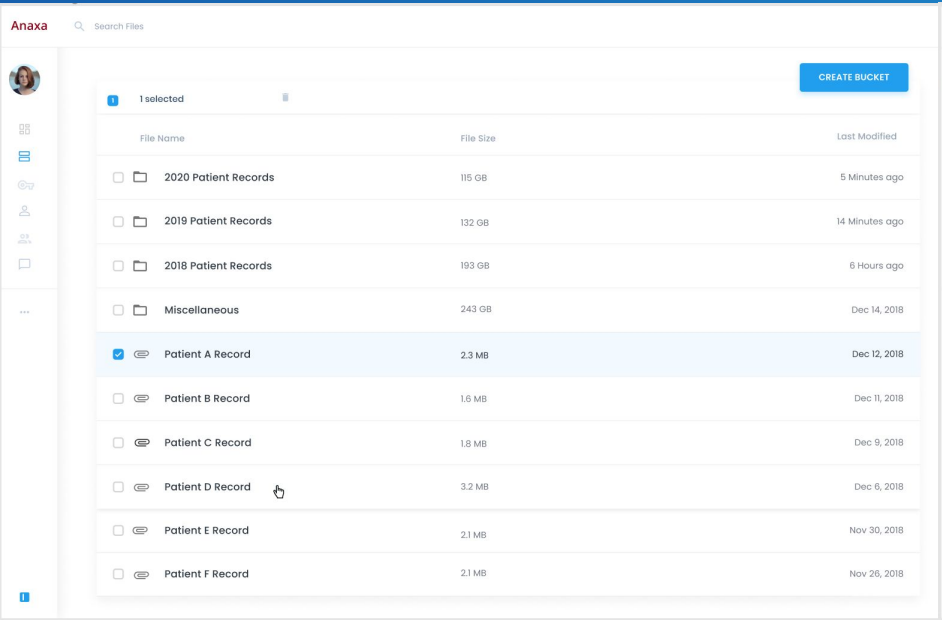
Platform Walkthrough

Sample User: Sarah

- Works at a **small-sized hospital** (<100 beds) affiliated with the UnitedHealth Group
- Position: **Medical Records Specialist** within Administrative and Support Staff
- Hospital relies on **EHR** digital records; Sarah organizes, maintains and updates health info on databases

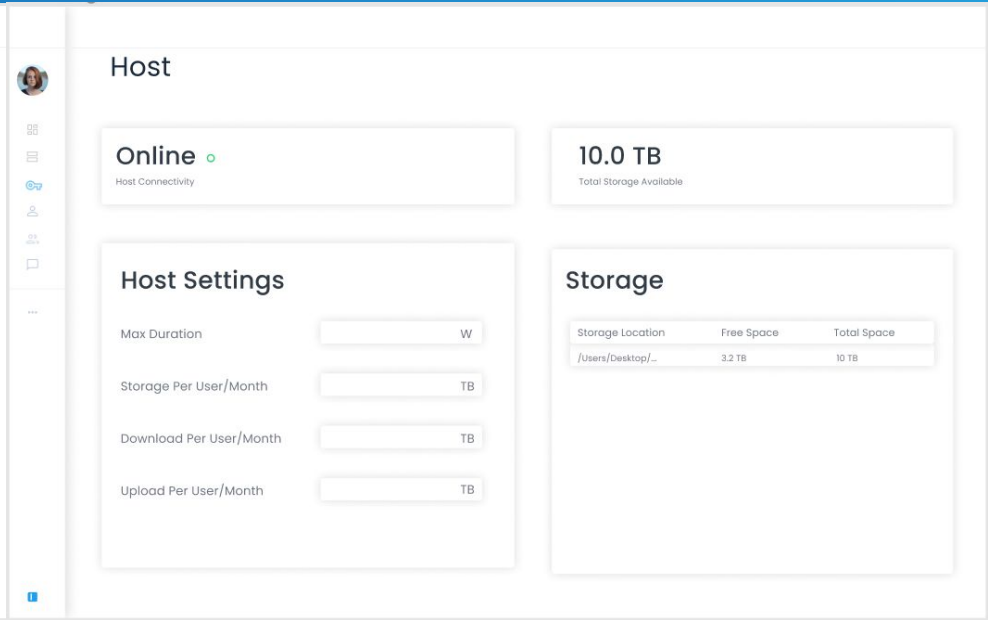
User Mockup

Home Page



- Hosting Settings for storing files
- Integrating QKD Chip onto device through a cryptographic API

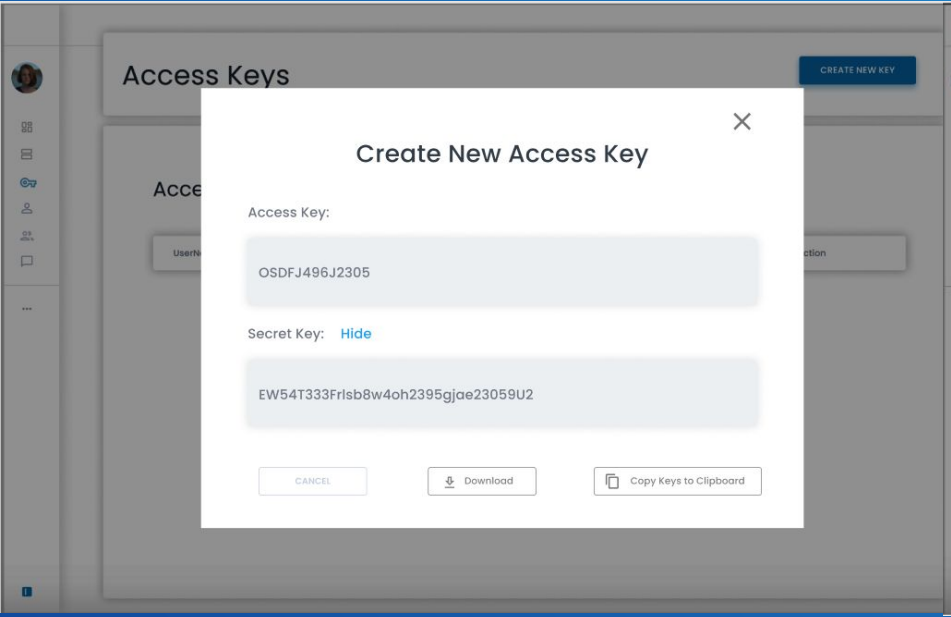
Record Upload & Storage



- Uploaded by medical personnel
- Stored to the platform with LBCP

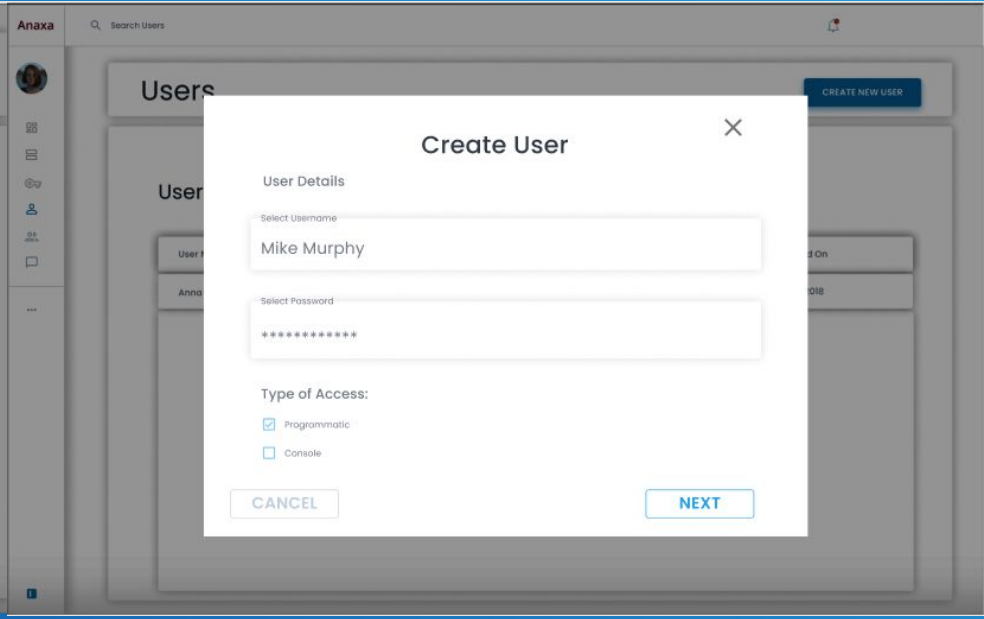
User Mockup

Access Key



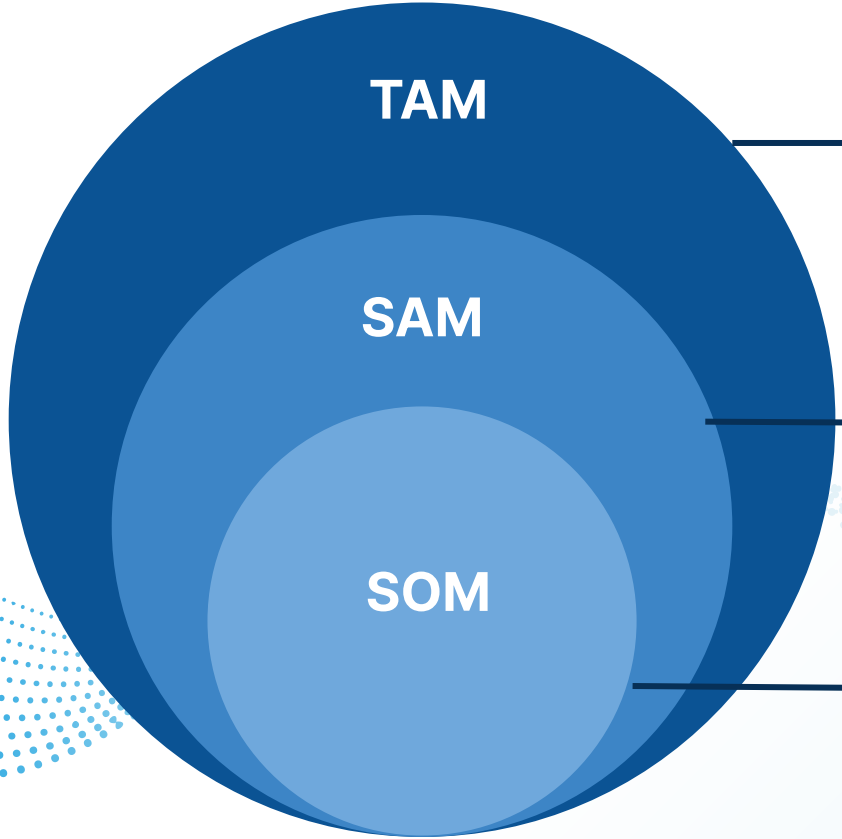
- User can be added to be part of the network
- Gains access to the record

Adding User



- Access key is created
- Starts the QKD link to ensure the secure transmission of data to another node

Current Market



$22 Billion

Health data security & analytics industry

$3.2 Billion

Healthcare agencies and services affected by data breaches in North America

$58 Million

Health insurance agencies and hospitals affected by data breaches in the New England hub

Anaxa

Current Market

Classical vs. Quantum Network Potential

5G	QG
• *Encryption Speed* 10 Gbps	• *Encryption Speed* **100 Gbps**
• *Latency* 1 ms	• *Latency* **0 ms**
• *Spectrum Efficiency* 30 bits/hz	• *Spectrum Efficiency* **60 qubits/hz**

Business Model

Model

Quantum Hardware

Transmitter and receiver chips to enable for quantum encryption and a quantum key distribution (QKD) link during the data transmission process

Decentralized Storage

SaaS-based with a minimum of 20 nodes for the storage of data and the communication channel

User Platform

SaaS-based model with a cost per user each year

50 Users

(Years 1-5 of complete product launch to market)

➔ Projected Revenue: = $2.7 million

➔ ARPA: $4,500

Anaxa

Business Model

Product Breakdown

1. User data gathered
2. Data processed by client, prepare to send/save in decentralized storage nodes
3. QKD Transaction completes, data encrypted + sent using Light Blockchain Communication Protocol (LBCP)

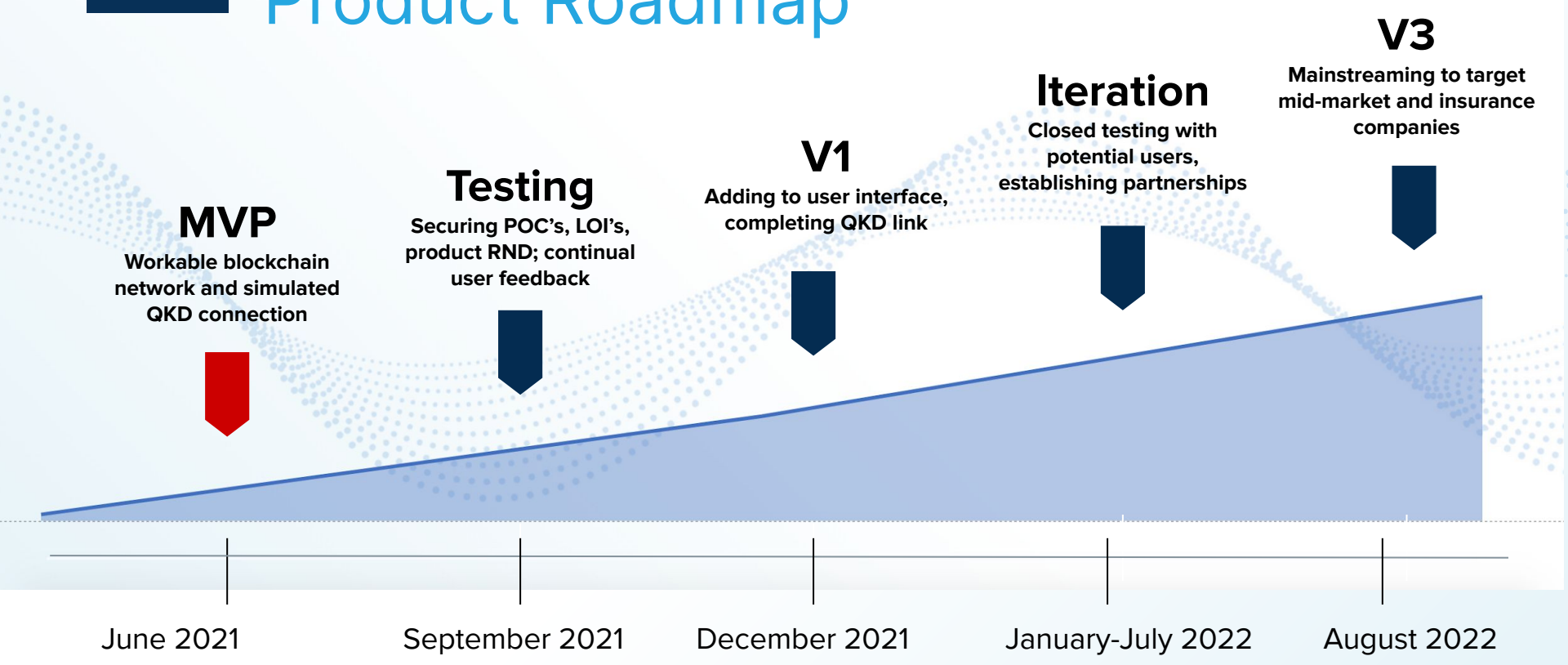
Pricing by Component

Quantum Hardware
- Manufacturing cost: ~$20,000
- Profit Margin: 30% (17% industry average)
- 5 minimum user devices allotted
- “Pay as you go”

Decentralized Storage
- Manufacturing cost: ~$50 per TB + qHardware
- Profit Margin: 30% (17% industry average)
- 20 nodes minimum (2TB each, $100)
- SAAS model for maintenance
- $28,100 upfront cost, $26,000 afterwards (annually)

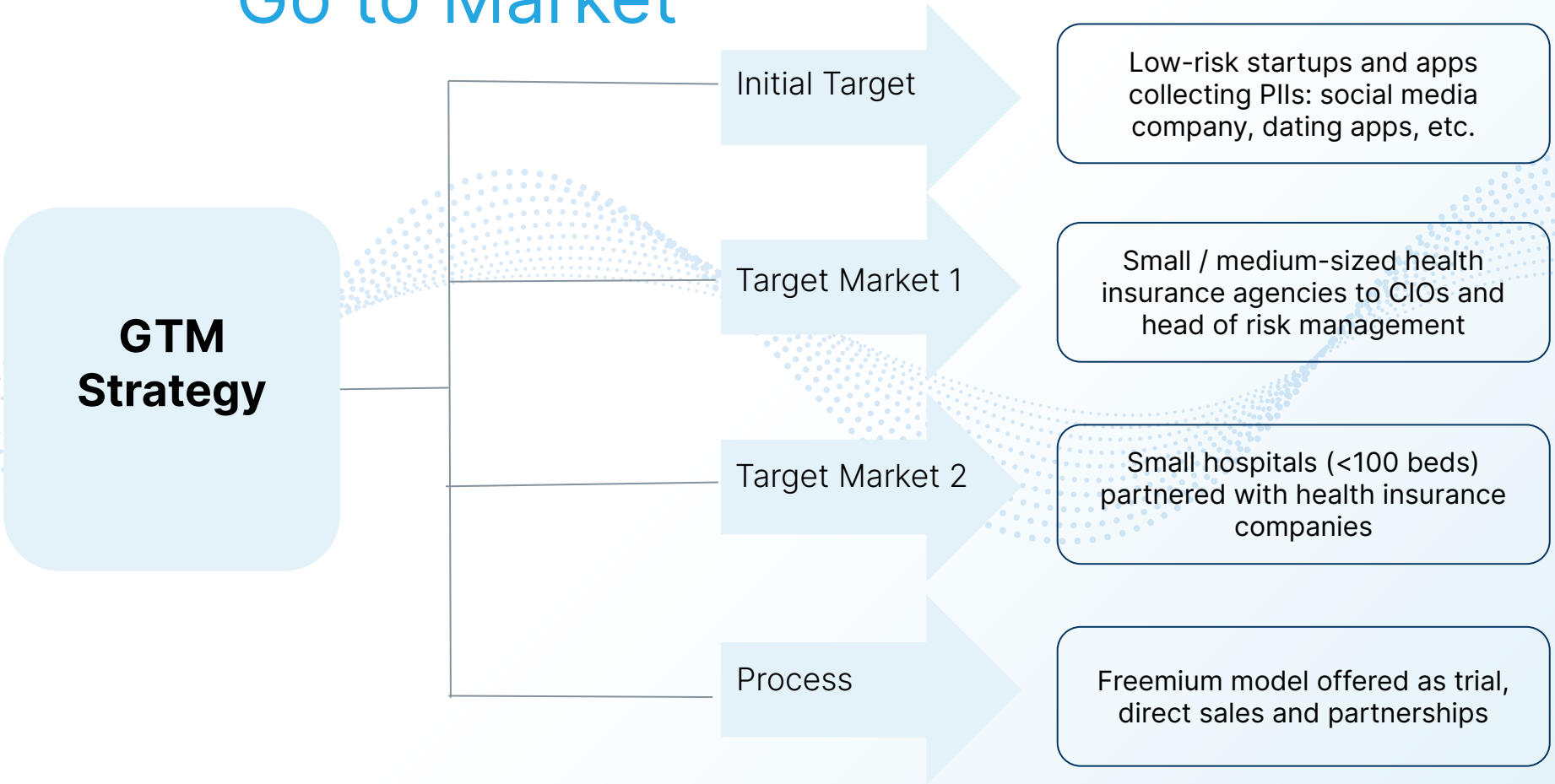
User Platform Software
- SAAS Model
- $200 per user (medical staff/personnell)
- 5 users minimum tier
- Pay for maintenance + upkeep
- Optional, depending on need of client

Product Roadmap



Anaxa

Go to Market


GTM Strategy
Initial Target
Low-risk startups and apps collecting PIIs: social media company, dating apps, etc.
Target Market 1
Small / medium-sized health insurance agencies to CIOs and head of risk management
Target Market 2
Small hospitals (<100 beds) partnered with health insurance companies
Process
Freemium model offered as trial, direct sales and partnerships

Team and Contact

Alice Liu; Co-founder

aliceliu2004@gmail.com

Saad Mufti; Co-founder

saadmuf10@gmail.com

Affiliations:

Biomedical Zone

DMZ

BACE Accelerate

Website: anaxa.tech

Anaxa