Nimbus-T™
Secure Identity & Authentication

WHITEPAPER

Secure Identity Management & Authentication with Blockchain integration for improved security.

Nimbus-T Global, GmbH / Switzerland
NT Coin (STO)

Date: February 15, 2019

Jose R. Bolanos MD, CEO

Disclaimer: *This document and others do not constitute a prospectus of any sort and are not a solicitation for investment. The NIMBUS-T token does not represent an ownership or share in ANY public or private corporation, or other entity in any jurisdiction. Ownership does not entitle you to any voting rights of the company. Purchasing a NIMBUS-T token is not an investment and should not be expected to have appreciation and in fact you may suffer a total loss in unexpected events. Acquisitions of NIMBUS-T tokens through the token sale are non-refundable. NIMBUS tokens are only to be used in connection with the future NIMBUS-T system and network under the terms and conditions. NIMBUS-T tokens are a new crypto-currency, a technology that uses the blockchain and distributed ledger technology to perform trustless transactions that remove intermediaries that in the past presented large costs with their usage. The technology allows for peer to peer transactions which are protected with encryption technologies. NT Coin or Nimbus-T Token is a payment token for healthcare and a planned STO (secure token offering) originating in Switzerland by Nimbus-T Global, GmbH.*

Background

Cryptocurrency Market

In January 2018 there were 200+ cryptocurrencies with a total market cap of over $750 Billion, a meteoric rise in valuation which sounded the bell for a new monetary system to shock the world. But a year later, a drop in valuation and an adjustment of expectations, there are over 1100 cryptocurrencies with a decreased market cap of $125 Billion. What we know today is that over 90% of these have failed and many were fraudulent. Globally, there is significant interest in the underlying technology of blockchain, encryption and distributed ledger technology. The top 5 cryptocurrencies have grown and remain stable despite the downturn. Big players are entering the market with investments because of the nature of the technology and its great promise of secure transactions that are more efficient and peer-to-peer. (www.coinmarketcap.com)

The advantage of crypto currencies over normal currencies is faster and cheaper transactions secured with distributed ledger technology. Today you can use Bitcoin, Ether or other to pay across the globe. In comparison, a merchant may pay 3.5% to accept credit card payments for transacting where-as the typical transaction on blockchains is a few cents. In the book, “The Truth Machine, the future of everything” by Michael J. Casey (https://www.amazon.com/Truth-Machine-Blockchain-Future-Everything/dp/1250114578), explains that the blockchain technology will revolutionize our society in a way the internet could not, truth in transactions, research, smart contracts, ownership validation, security around your access to information.

Technology for Secure Patient Identity Management.

Nimbus-T has received USPTO patent approval for its Nimbus-Key System technology for enhanced security around patient identities and access to your medical information across healthcare systems. Hospital information systems are behind the curve when it comes to security and it is your medical and personal information that is a risk. Our technology is in development and we have several pilots in the works. Ultimately we see your **Nimbus-Key** or encrypted global identity as the protection for aggregating all of your healthcare information in a secure manner. Imagine your doctor being able to see a new portal with an array of information from your digital health to your genomic data that you have control over. Then imagine having control of that information so that you may participate in clinical trials as a patient and getting paid for it? The new blockchain technology creates a distributed ledger on the Ethereum platform to secure that information as well as transactions across the platform. Currently the country of **Estonia** is the most digitally advanced e-government that is using a form of secure digital ID for it population to deliver government services such as renewal of driver’s license, starting a business, opening a bank account and paying taxes. The importance of a secure digital identity is significant, and it is just beginning to take shape. We are at the forefront of providing a secure patient identity that will have immense implications to allow people to have access to multiple services.

In the United States, healthcare transactions account for $3.5 Trillion! Health insurance carriers are very inefficient in orchestrating healthcare payment transactions, there is a 45% loss due to excessive paperwork, oversight, and adjudication. In Switzerland, the second most expensive health care system in the world, where the government mandates health insurers to pay for services. These two systems have problems with inefficiency, high costs, many intermediaries and have disconnected the patient from the process so expenses go unchecked.

What we are developing a secure identity system for healthcare which is backed by the blockchain and smart contracts to provide enhanced efficiency and transparency. Our NT Coin will provide an alternate healthcare payment system that removes such inefficient intermediaries and provides a peer-to-peer secure transaction architecture. Your Nimbus-Key ID will provide access to your medical records, setting up appointments, telehealth visits, and personalized healthcare intelligence. A cryptocurrency for healthcare providing peer-to-peer payments will save the healthcare systems 40% and enhance access for patients, you select your own doctor and not your insurance carrier.

Status of Corporation

Nimbus-T, Inc is a United States Delaware C corp since 2014. The company has developed a patented technology (USPTO 2018) for creating a global patient and provider identity, double encrypting it and output as a QR code, known as the Nimbus-Key. This encrypted identity can be used as a security token in a two-factor authentication schema such as registering at a kiosk. This digital ID is the basis for delivering numerous services to consumers while ensuring proper authentication, decreasing fraud and decreasing costs to the healthcare system. Our Nimbus Identity System is a SAAS platform that is scalable and manages other identities securely across disparate data systems allowing for better record matching and preventing input errors as well as duplicate records. We have several pilots in discussion. I first major customer is Penn Highlands Healthcare (USA) with 4 hospitals, 100 locations, 4,000 employees, 400 doctors and over 250,000 patients. We have an MOU in place.

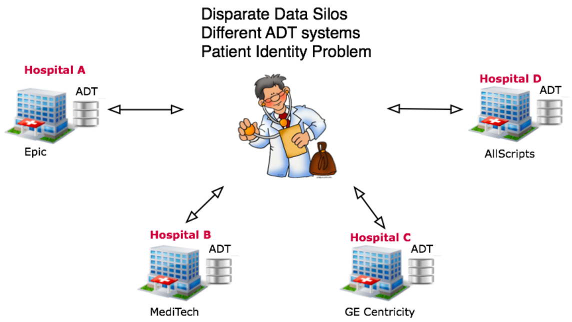
In Switzerland, we have created **Nimbus-T Global, GmbH**. We are planning a securities token offering (STO) from here and focus on blockchain technologies for healthcare. We are working with our legal team to get SEC and FINMA approval. Nimbus-T inc is exclusively licensing the patented Nimbus-Key technology to Nimbus-T Global for outside the USA. We will be using the proceeds of the STO for creating the technology of an alternate payment system in healthcare, blockchain transactions, smart contracts and other solutions to improve the information architecture to ensure patient safety and improved care.

The two companies are separate technologies with cross-licensing, and each will be seeking independent funding from their base countries of operations. Each will use the same branding and logo as they function in collaboration internationally.

Problem

Healthcare Identity Problem

In many countries throughout the world, identity management is a significant problem that prevents the proper access to a patient's medical information that may be scattered throughout numerous healthcare facilities, hospitals, clinics, labs, doctor's offices, etc. Now that medical records are digital and a patient will have a different identity (ID) or medical record number (MRN) at each of these touch points, records are at different places and there is no good access to view and aggregate them. Think about how many healthcare facilities you have been to in your life, do you have access to all of your medical records? The difficulty that I describe is called an interoperability problem, or the inability to have systems communicate your information because there is no single source of truth in identity. Our Nimbus-Key ID is the "single source of truth" connecting all other IDs to you.



The status regarding **identity theft** has been a significant problem across all industries. *"The latest account from the Identity Theft Resource Center (ITRC) reports that there has been a total of 641 data breaches recorded through November 3, 2015, and that nearly* ***176 million records have been exposed****. The annual total includes 21.5 million records exposed in the attack on the U.S. Office of Personnel Management (OPM) in June and 78.8 million health care customer records exposed at Anthem in February."(Source: 247 Wallist | By Paul Ausick November 5, 2015)*

The **Equifax breach** exposed over 140 million American's social security numbers and today the IRS is receiving the brunt of those fraudulent tax returns. Attackers got their hands on names, Social Security numbers, birth dates, addresses, some driver's license numbers, and about 209,000 credit card numbers. This massive breach occurred to one of the most respected credit reporting agencies, **Equifax!** *Source: Wired Magazine* . Does this mean that Equifax had not encrypted their database information? Identity theft is a huge problem for all governments.

Identity theft in healthcare has been a very big problem. In 2015, there were more than 150 million medical identities stolen from insurance companies and hospitals. The hackers find greater rewards for stealing medical identities over credit card numbers. A credit card can be cancelled with a single phone call, whereas a medical identity usually encompassed private personal information including SSN which allows the criminals the opportunity to take out fake credit card accounts in your name. A stolen medical identity can be so painful for the victim that it may cost up to $15,000 and 18 months to clear it up. Meanwhile, medical institutions do not want to change back erroneous information or billings that were done falsely in your name! Your FICA credit score can take a big hit and you are left wondering which way to turn. Needless-to-say, protecting your medical identity is one of the most important functions for anyone involved in delivering medical care. This includes hospitals, insurance brokers, health plans, ACOs, Labs, clinics and doctor's offices. Significant fines are being issued for security violations, HIPAA violations.

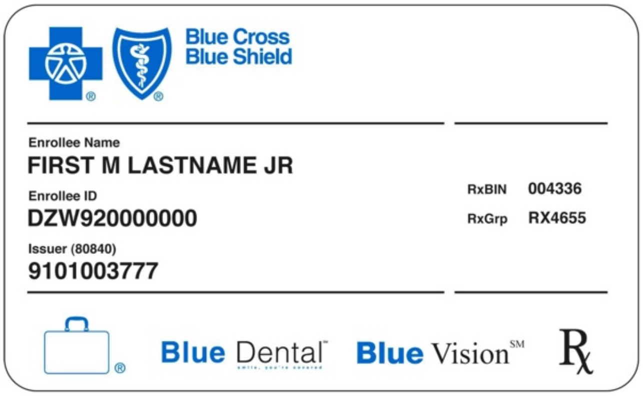
World Health Organization

"***Statement of Problem and ImPact***: *Throughout the health-care industry, the failure to correctly identify patients continues to result in medication errors, transfusion errors, testing errors, wrong person procedures, and the discharge of infants to the wrong families. Between November 2003 and July 2005, the United Kingdom National Patient Safety Agency reported 236 incidents and near misses related to missing wristbands or wristbands with incorrect information (1). Patient misidentification was cited in more than 100 individual root cause analyses by the United States Department of Veterans Affairs (VA) National Center for Patient Safety from January 2000 to March 2003 (2). Fortunately, available interventions and strategies can significantly reduce the risk of patient misidentification* ". *Source: WHO paper on Patient Identification.*

Healthcare Authentication Problem

Authentication is the function of determining if you are, who you say you are. Strict identification is performed by many companies before setting up your private identities, such as governments and banks when they ask you for picture ID, passport, copy of a phone bill or a tax return. In today's social media world, there is no prior identification of a person and anyone can set up an account. Facebook has over 25% fake accounts without identifying the identity of the person and then it has an authentication service to allow a person to log into other accounts and systems. You are essentially authenticating to a potential fraudster.

The problem in healthcare is again the absence of authentication in the delivery of healthcare and payment transactions. For example, In the USA, Medicare and Medicaid is plagued with a massive **healthcare fraud amounting to over $120 Billion annually**, as stated by ex-attorney general Eric Holder in 2015. Authentication deficiency is rampant in the healthcare industry, insurance cards are paper based and identity is easily stolen or transferred to another to defraud the system. There is no authentication mechanism, no picture, no check of other IDs, no encryption or no biometric technology. Anyone family member of the same sex can use another one's card and obtain healthcare services. This brings up another problem in that a fraudster stealing your identity can then secure fraudulent access to healthcare under your name which will result in **inaccurate, diagnosis, medications and lab results in your medical record!** So the lack of proper patient authentication leads to the potential of massive fraud and placement of false information into the wrong medical record. The Nimbus-Key ID System will securely authenticate a person and provide quick and accurate access to your personal medical record and decrease fraud while saving $billions of dollars for the healthcare system.



Blue Cross Blue Shield

Enrollee Name
FIRST M LASTNAME JR

Enrollee ID
DZW920000000

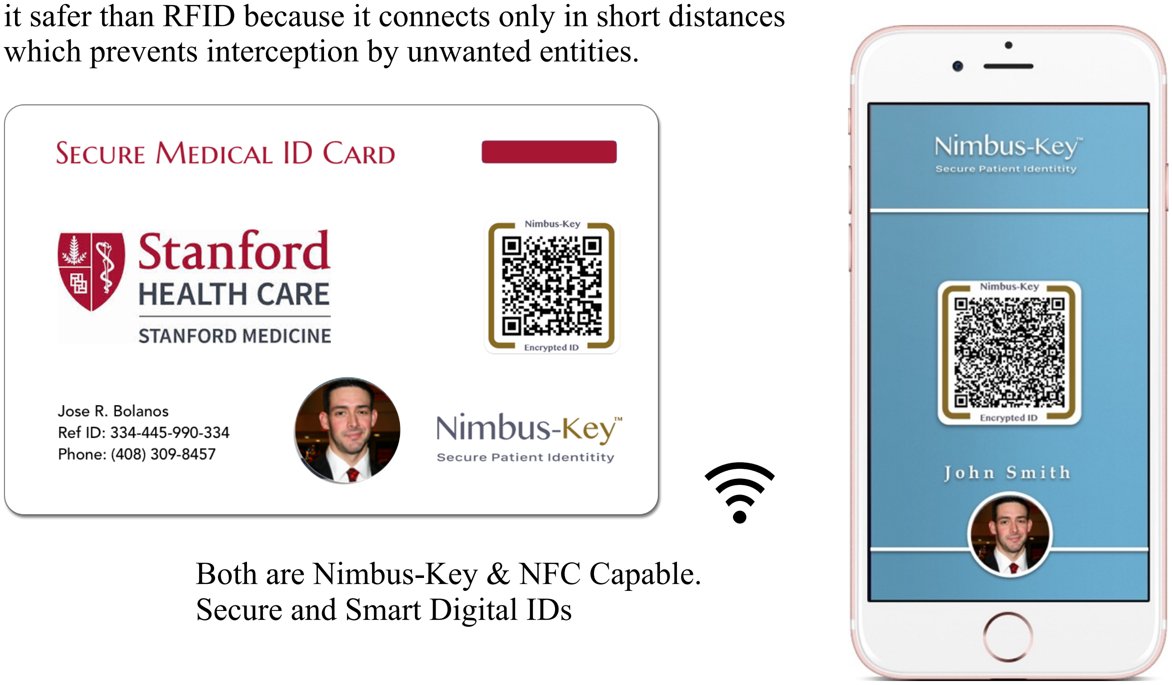
Issuer (80840)
9101003777

RxBIN 004336
RxGrp RX4655

Blue Dental Blue Vision Rx

Solution that includes Blockchain technology.

Nimbus-T has a patented technology called the Nimbus-Key System which is a cloud based solution, on the Amazon Cloud, we are connecting to the distributed ledger on the **Ethereum Blockchain Platform.** Our system creates a "**Global Identifier**" for each person and this is then encrypted and output as a QR-code for print or a Smart Digital ID. No one can read or access it because it is encrypted. We provide two-factor authentication of healthcare providers and patients making it a secure platform for communicating sensitive information. The encrypted QR-code is called the **Nimbus-Key** and can be displayed on an identity card or an app on your mobile phone. Also, each of these, as seen below, has the ability to transmit the encrypted identity using NFC communication making it safer than RFID because it connects only in short distances which prevents interception by unwanted entities.



Both are Nimbus-Key & NFC Capable.
Secure and Smart Digital IDs

Every hospital uses different software to manage operations such as: registration, billing, lab, xray, and other internal systems and each one provides each patient with a different ID number. Managing these disparate information systems with different IDs is fraught with potential errors. The hospital's ADT systems (Admissions, Discharge, and Transfer) use an MPI (Master Patient Index) to manage those disparate identities within the hospital system. In today's healthcare world, many hospital systems are merging in order to decrease costs, but this creates enterprises with different EMRs (electronic medical records). So a patient now has many identities across systems and information integrity becomes more difficult without a single source of truth, a global ID. This is what the Nimbus-Key ID is meant to solve.

Across the USA, HIEs (health information exchanges) have been created to help with system interoperability or communication of a patient's information across different systems. They use algorithms to determine if two records belong to the same person. Unfortunately, this is prone with errors up to 20% of the time, meaning **improper patient record matching** which is a catastrophic problem. You do not want to have another person's medical information within your medical record.

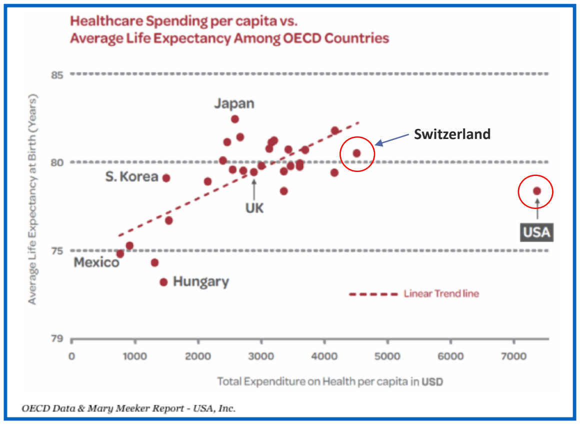
Our **Nimbus-Key System** provides every patient and provider with a **unique global identifier encrypted**, a secure and smart digital ID, then our system links other identities from many disparate systems to your global ID or Nimbus-Key. This provides the opportunity for doctors to have SSO (single sign on) to their multiple systems within the enterprise. This provides patients with the ability to view and aggregate their medical information across multiple systems on a dashboard on their laptop or mobile device. Doctors similarly have the ability with our system to view patient data quickly and efficiently. This is especially important as more and more information systems come online and we all start signing up, systems like digital health programs, quantified-self initiatives and genomic data. We can aggregate this information in one place so your healthcare provider can use it to the fullest benefit in delivering your care. Our aim is to have a broader picture of your healthcare information available to you and your doctor.

Our target customers are governments, health insurance companies, hospital systems, ACOs (accountable care organizations) and medical groups. Our identity platform is the foundation of all transactions, communications, information integrity and productivity for the entire healthcare system.

Our blockchain solutions can solve the opioid crisis using smart contracts to prevent over prescribing and fraud. Our telehealth solutions can help expand the reach and efficiency of healthcare providers for healthcare systems, student health centers, mental health facilities and rural health initiatives.

An Global Alternate Healthcare Payment System. Our NT Coin, a new healthcare cryptocurrency can provide a more efficient delivery mechanism for transactions with smart contracts and distributed ledger technology. Currently healthcare transactions undergo a myriad of processes regarding oversight, adjudication, re-pricing, contract verification, patient eligibility and more, which causes a 40% loss from inefficiency. Yes, **40% of the healthcare dollar is being wasted**. We would be in a great position to streamline the payment processing using the blockchain technology for all governments. A secure identity platform with faster and a more efficient payment system.

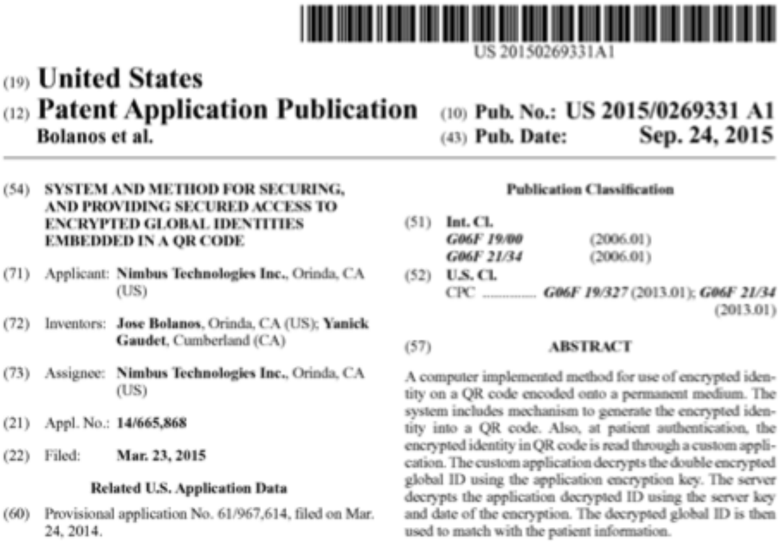
The graph on the right reveals that the US and Swiss Healthcare systems are the most expensive per capita of the developed world. You can clearly see that for the amount of money spent on healthcare, both of these governments the population's average life expectancy does not increase in relationship to the amount spent. Both of these governments need help in finding better solutions that provide a return on investment. The overall health of the population is the basis for the productivity of the nation.



OECD Data & Mary Meeker Report - USA, Inc.

Intellectual Property – Patent approved and Issued.

System and method for securing, and providing secured access to encrypted global identities embedded in a QR code. Google Patents. PDF



US 20150269331A1

(19) **United States**
(12) **Patent Application Publication**
Bolanos et al.

(10) **Pub. No.: US 2015/0269331 A1**
(43) **Pub. Date: Sep. 24, 2015**

(54) **SYSTEM AND METHOD FOR SECURING, AND PROVIDING SECURED ACCESS TO ENCRYPTED GLOBAL IDENTITIES EMBEDDED IN A QR CODE**

(71) Applicant: **Nimbus Technologies Inc.**, Orinda, CA (US)

(72) Inventors: **Jose Bolanos**, Orinda, CA (US); **Yanick Gaudet**, Cumberland (CA)

(73) Assignee: **Nimbus Technologies Inc.**, Orinda, CA (US)

(21) Appl. No.: **14/665,868**

(22) Filed: **Mar. 23, 2015**

Related U.S. Application Data

(60) Provisional application No. 61/967,614, filed on Mar. 24, 2014.

Publication Classification

(51) **Int. Cl.**
G06F 19/00 (2006.01)
G06F 21/34 (2006.01)

(52) **U.S. Cl.**
CPC *G06F 19/327* (2013.01); *G06F 21/34* (2013.01)

(57) **ABSTRACT**

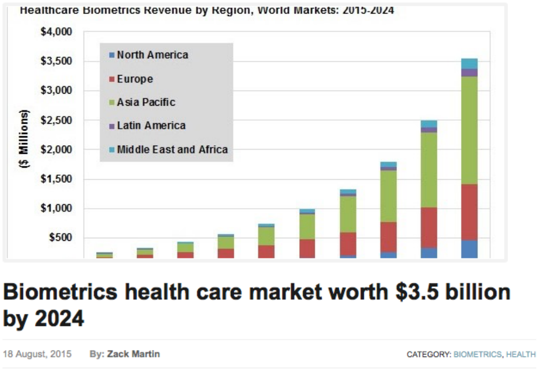
A computer implemented method for use of encrypted identity on a QR code encoded onto a permanent medium. The system includes mechanism to generate the encrypted identity into a QR code. Also, at patient authentication, the encrypted identity in QR code is read through a custom application. The custom application decrypts the double encrypted global ID using the application encryption key. The server decrypts the application decrypted ID using the server key and date of the encryption. The decrypted global ID is then used to match with the patient information.

Note: Patent application was made by Nimbus Technologies, Inc which we later changed the company name to Nimbus-T, Inc

We have the ability to use the Nimbus-Key (encrypted global id into a QR code) as a **security token**. This new security token when combined with PIN code, biometric, image, and other security measures enhances the overall security and access using multi-factor authentication. We have partnered with Identazone to create an interoperable identity system which will allow our Nimbus-Key and Biometrics to cover all aspects of identity management that a customer may require.

Market Opportunity

https://www.secureidnews.com/news-item/biometrics-health-care-market-worth-3-5-billion-by-2024/



Biometrics health care market worth $3.5 billion by 2024

18 August, 2015 By: Zack Martin CATEGORY: BIOMETRICS, HEALTH

“Starting from a base of $250 million in 2015, the firm forecasts that global health care biometrics revenue will reach $3.5 billion by 2024, with cumulative revenue for the 10-year period totaling $12.5 billion. Key health care use cases, which will drive adoption of biometrics hardware and software in the industry, will include home/remote patient access, care provider authentication, patient identification and tracking, and pharmacy dispensing.”

https://www.linkedin.com/pulse/biometric-market-trends-2016-identity-verification-finance-scholz/

The Biometric Market Trends of 2016: Identity Verification, Healthcare, Finance, IoT
Published on February 3, 2016 by Clair Sholtz

"Biometrics is a quickly growing industry. The global market for biometric technologies, which totaled $14.9 billion in 2015, is expected to ***reach $41.5 billion by 2020****, reflecting a five-year compound annual growth rate (CAGR) of 22.7% (MarketWired). The need for unique credentials to authenticate an individual that are much less prone to theft or loss is facilitating the shift from traditional authentication methods to biometrics."*

http://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp
Biometric System Market worth $32.73 Billion USD by 2022
"The biometric system market is expected to reach USD 32.73 Billion by 2022 at a CAGR of 16.79% between 2016 and 2022. The base year considered for the study is 2015 and the forecast is for the period between 2016 and 2022."

http://www.biometricupdate.com/201502/market-for-healthcare-biometrics-to-reach-5-billion-by-2020
Market for healthcare biometrics to reach $5 billion by 2020. By Stephen Mayhew
"In a white paper issued this week, Biometrics Research Group, Inc., the parent company of BiometricUpdate.com, estimates that the entire global marketplace for biometric solutions in the healthcare market will reach approximately US$5 billion by 2020."

Blockchain in Healthcare

"Blockchain technologies enable the creation of a digital database which is rendered extremely secure through its reliance on mathematical consensus achieved by the operation of a distributed network of computers which store identical copies of the database. In this way, Blockchain technologies provide the foundation for trust between strangers without the need for a trusted third-party intermediary to guarantee the security of transactions."
https://www.blockchain-healthcare.org

Our Nimbus-Key ID system in the cloud hybridized with the Ethereum blockchain will enable a secure transaction platform for the following use cases:

1. Secure prescriptions and accurate mediation lists
2. Smart contracts to limit opioid quantity prescribed by provider
3. Peer-to-peer payment systems improving efficiency and cost of transaction
4. Secure supply chain in healthcare with improved identity management of products
5. Reducing fraud in transactions, payments and products
6. Improving information collection, accuracy and validity in clinical trials.
7. Providing ownership of medical information for patients
8. Improving authentication and record integrity.

These are just the tip of the information possibilities. Many hospital systems are committing to blockchain solutions in the attempt to advance processes.

A Cryptocurrency for Healthcare

Our NT coin will be a form of payment for the healthcare sector. Employers will be encouraged to provide their employees with our wallet and issuance of a certain amount of NT coin for spending with doctors, dentists, hospitals and other healthcare services. We aim to deliver a network of providers that will offer a 30% discount off of set prices. The average family spends $3500 annually in out-of-pocket medical expenses.

We will also provide an app for consumers that will deliver the following benefits:

1. Basic information, including demographic, and insurance plans
2. Medical history and medication lists for improved accuracy of diagnostics
3. Secure messaging with our community of patients and doctors
4. Telehealth platform for quick access to a provider
5. Secure identity management and fast registration at hospitals and clinics
6. Control who has access to your medical information
7. Linking your Nimbus-Key ID to other medical identities
8. Linking your Nimbus-Key ID to Digital Health and Genomic Health
9. Access to a marketplace of healthcare services for preventive health.
10. News and information regarding important health issues.

Secure Token Offering – STO

The ICO market has changed dramatically, no longer is it fashionable to create a white paper and an idea, then to seek funding for a concept. Those have passed and failed. Today, the regulatory environment requires a more robust offering with integrity throughout the entire process. KYC/AML processes (know your customer / anti-money laundering) are a must and regulatory compliance with different governments. We are in the process of getting SEC and FINMA approval and are planning an STO for Nimbus-T Global GmbH toward the middle to end of 2019.

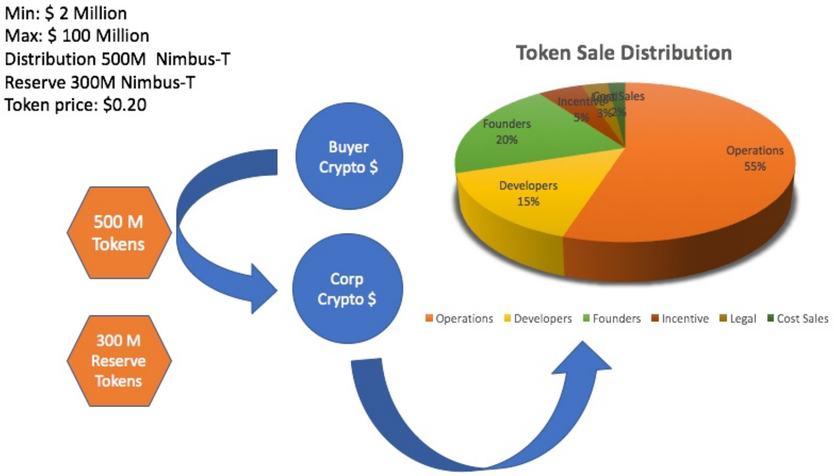
Our Token Private Sale will entertain accredited investors, family offices, hospital systems and institutional investors.

- Minimum $2 Million / Max: $100 Million
- Tokens to be distributed or sold: 500 Million / Reserve 200 Million
- Token Price: $0.20 per Nimbus-T Token

Cryptocurrency to be accepted with be Ether and Bitcoin. Also Fiat currency.
Use of proceeds:

- Operations 55%
- Founders 20%
- Developers 15%
- Incentives and bug bounties 5%
- Legal 3%
- Cost of Sales 2%

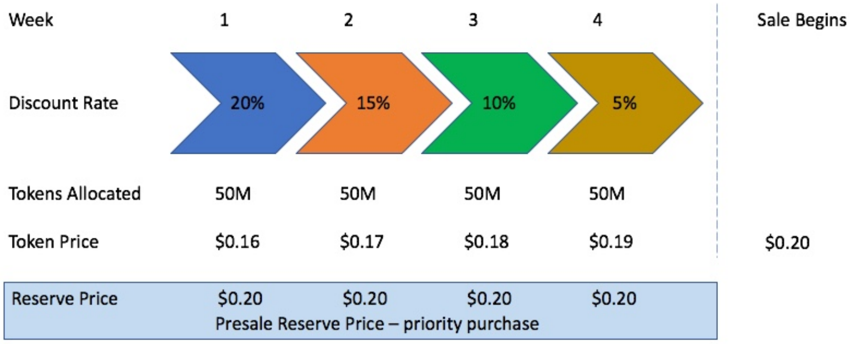
Nimbus-T Token Sale Strategy



Discount Pre-Sale Logistics

Our discount sale will last 4 weeks prior to actual sale date. As described below, a purchaser of the NT Coin may avail themselves to the discount rate that varies week by week, starting with a 20% on week 1 and decreasing to 5% on week 4. During this pre-sale we will also have a Reserve Price / Priority Purchase event where a buyer may take advantage of the presale by locking in their request to buy at full price. We plan to limit each week to 50 million tokens on the discounted rate, but no limit on the Reserve Priority Purchase.

Nimbus-T Token Pre-Sale Discount



Week	1	2	3	4	Sale Begins
Discount Rate	20%	15%	10%	5%	
Tokens Allocated	50M	50M	50M	50M	
Token Price	$0.16	$0.17	$0.18	$0.19	$0.20
Reserve Price	$0.20	$0.20	$0.20	$0.20	
	Presale Reserve Price – priority purchase				

Security around the ICO is very important to us. We do not want anyone to make a mistake and lose their money by sending money to a smart contract address or a fake website with a wrong account. www.nimbus-t.io is the only authorized site.

Executive Team & Advisory Team

Jose Bolanos MD
CEO / Founder
USA/Suisse

Andrew Snyder MD
Operations
CMO Evolent Health

Nick Gaich
Operations
Silicon Valley, USA

Alexandria Combs
Operations
Silicon Valley, USA

Phillip Pellerin
Supply Chain
Silicon Valley, USA

Michael Innes
Identity Systems
Silicon Valley, USA

Brad Furber Esq
Securities Law
Advisor

Govinda Babu GBJH
Technology
Advisor

Yanick Gaudet
Engineer
Advisor

Sebastian Pelletier
Engineer
Advisor

Hennie Cloete
Engineer
Advisor

Thomas Johnson
CIO Penn Highland
Advisor

Vassil Dimitrov PhD
Professor Encryption
Calgary University

Avinish Dixit
Technology
Advisor

Adrian Rich Esq
Corporate Attorney
Perkins Coi

Mark Koo Esq
Patent Attorney
Credere Law

1. **Jose R. Bolanos MD, CEO -**
   Stanford medical alumnus, 20+ years in clinical medicine, managing director of Venture-Med Angel group helping innovative healthcare startups for past 8 years. Past strategic advisor for Lifemed-ID. Present advisor for FACT-Encryption, Dynosense, Physiocue, Spirometrix, Bioxiness and Precise Light Surgical.
   * Past researcher at UC Davis in human sperm cryopreservation and fertilization.
   * Past Chief Strategist for LifeMed ID which focused on patient identity management using Smart Card technologies and Cloud based infrastructure.
   * His emphasis on managing patient healthcare data for hospitals, HIEs and ACOs.
   * Past CEO of New Americas Medical Group, a physician IPA dealing with managed care solutions for Hispanic patient healthcare delivery.

2. **Yanick Gaudet, CTO -**
   Healthcare Information Technology Consultant, HL7 Specialist for over 20 years. Focused on connectivity within the healthcare system, integration, encryption and co-developer on the Nimbus-T technology patent.

3. **Andrew Snyder, MD, CMO –**
   Executive Vice President, Chief Clinical Integration Officer & President, Mount Sinai Health Partners, IPA. Past Chief Medical Officer for Brown and Toland IPA in San Francisco. Dr Snyder has a vast experience in managed care and population health management of large patient populations.

4. **Vassil Dimitrov, PhD, Professor Encryption -**
   Professor at University of Calgary Teaching numerical analysis, complexity of algorithms, cryptography, VLSI designs, computer arithmetic.
   Research works - hardware implementation of cryptographic algorithms, image

compression algorithms and their VLSI implementation, digital watermarking, computer arithmetic algorithms, computational number theory, computational geometry. He has published several papers on encryption technologies.

5. **Sebastian Pelletier, Cloud Architecture-** in
   Software Engineer/Architect, Java/JEE technology specialist. Accomplished software engineer/architect with over 16 years of relevant industry experience where a combination of programming skills, creativity and continuous learning contribute to new and innovative system development with shorter development cycles. Proven expertise in design and development of scalable and real-time architectures, distributed systems, legacy systems integration on the Web and JAVA development.

6. **Nick Gaich, Operations -** in
   Nick Gaich is the founder and CEO of Nick Gaich and Associates, a firm dedicated to providing executive coaching, leadership development, strategic planning, and operational performance. He also serves as a Senior Advisor to Venture-Med an Angel Investment Firm dedicated to funding and mentoring new healthcare start-ups.
   Nick Gaich retired in 2012 as Assistant Dean of Clinical and Translational Research Operations, Stanford Center for Clinical and Translational Research and Education at Stanford University School of Medicine.

7. **Alexandria Combs, Global Health -** in
   Healthcare Catalyst ▸Consulting: Strategy & Clinical Transformation | Start-ups & New Market Entry | Global Health. She consults on strategy and clinical transformation as well as with start-ups and companies focused on new market segments. With a strong commitment to improving health and health care systems globally, particularly focusing on countries with lean economies, I actively volunteer with medical missions in Africa and Asia, assisting with strategic planning, fundraising, and operational execution.

8. **Phillip Pellerin, Supply Chain -** in
   SCM Systems SME / Strategic Sourcing , Procurement / Contracting / Sequencing , Genomics / Value Analysis. Verity Health System he is director of sourcing and supply chain management. Mr Pellerin has vast experience in supply chain dynamics and operational efficiencies.

9. **Michael Innes, Digital ID systems -** in
   Michael is currently a consultant in Slalom’s Delivery Leadership practice and helps clients deliver on projects where Technology and Supply Chain Operations intersect. He has deep experience with ‘End to End’ visibility projects at a variety of life science, retail and healthcare clients. His engagements have impacted client operations in the following ways: Agile transformation, ‘Big data’ Visualization, legacy system migration onto ‘the Cloud' and successful IBM, Oracle, JDA, SAP and PeopleSoft Supply Chain package implementations.

References

Contact: Jose R. Bolanos MD, CEO / jose@nimbus-t.com / skype: jbolanosmd

Disclaimer: *This document and others do not constitute a prospectus of any sort and are not a solicitation for investment. The NIMBUS-T token does not represent an ownership or share in ANY public or private corporation, or other entity in any jurisdiction. Ownership does not entitle you to any voting rights of the company. Purchasing a NIMBUS-T token is not an investment and should not be expected to have appreciation and in fact you may suffer a total loss in unexpected events. Acquisitions of NIMBUS-T tokens through the token sale are non-refundable. NIMBUS tokens are only to be used in connection with the future NMBUS-T system and network under the terms and conditions. NIMBUS-T tokens are a new crypto-currency, a technology that uses the blockchain and distributed ledger technology to perform trustless transactions that remove intermediaries that in the past presented large costs with their usage. The technology allows for peer to peer transactions which are protected with encryption technologies.*