White Paper

Our Vision and Mission

HealthCombix is a geographically distributed blockchain development team with members located in the United States, Europe, and Asia.

HCX PAY, a trusted **privacy-centric** healthcare payment network, is the first of many blockchain-inspired capabilities to be developed by HealthCombix to realize its long-term vision:

- Our *creation is* a **frictionless** healthcare **experience** at a **lower cost** for anyone, anytime, anywhere
- Our *vision* is to **enable decentralized** healthcare ecosystems around the globe
- Our *mission* is to **reinvent** the way healthcare is done
- Our *motivation* is to empower consumers

Our Core Beliefs

- A decentralized healthcare ecosystem framework enabled by a distributed or healthcare blockchain network ecosystem is needed to disrupt the existing market structure to create an open, meaningful, and fair system. Eliminate unnecessary intermediaries, enhance trust and privacy, and pave the way for advanced capabilities including data interoperability, digital identity, health data asset management, advanced payments, and disease prediction systems.
- Data interoperability remains a major problem in the United States and around the globe hampered by technical complexities, market forces, and jurisdictional regulatory differences and complexities. Open protocols have the potential to remove or significantly diminish these complexities.
- Blockchain-inspired technology will set the stage for health data and other healthcare assets to evolve into a *new asset class* giving rise to consumers controlling the brokerage of their data for research, improved pricing transparency, precision health, clinical trials, payment, and disease intervention and management.
- Meaningful healthcare industry disruption and new care economies and ecosystems will emerge from innovation related to open decentralized networks and convergence of advanced technologies including IoT and machine learning.
- Healthcare administrators, risk managers, and supply-chain trusted intermediates will be displaced or diminished.
- Closed, private blockchain, or shared infrastructure solutions may create incremental efficiencies but not the transformational effects that open blockchain networks will have on industry.

White Paper Table of Contents

Our Vision and Mission 1
Our Core Beliefs 2
The Problems to be Solved 4
Network Opportunities 8
- HCXP mining node operator network management and toolbox 8
- Cross-border healthcare markets 10
- Employer channel opportunity 11
- Virtual care and on-demand delivery 12
- Uberizing medical claims and patient adherence with anonymous witnessing 12
- Virtual underwriting (smart syndicates), medical cost sharing, and health trust networks 13
- Data fiduciaries and curators 13

HCX PAY Platform Capabilities 15
- HCXP mining, decentralization, and virtual nodes 15
- Tokenization and healthcare 15
- Data privacy, proxy re-encryption, and payment 17

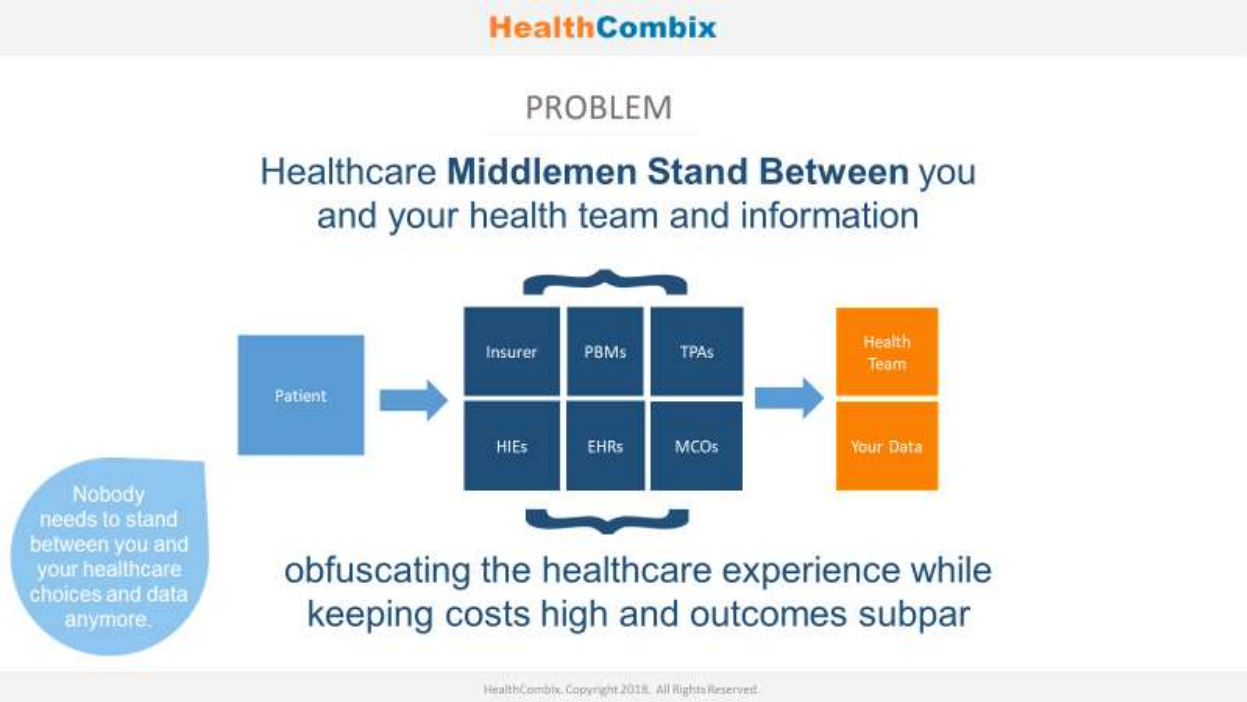
Blockchain and CryptoNote Algorithm Technology 18
- CryptoNote algorithm 18
- Untraceable payments and ring signatures 18
- Unlinkable transactions 19
- Standard CryptoNote transaction 20
- Adaptive limits 21
- Smooth emission 22
- Egalitarian proof-of-work 22

Roadmap 24
Network Condition and Token Economics 25
- The HCXP token 25
- HCX PAY network attributes 25
- Supply allocation 25

Core Team 26
Endnotes 35

The Problems to Be Solved

Healthcare middlemen stand between you and your health team and information, obfuscating the healthcare experience while keeping costs high and outcomes subpar. Whether in the United States, Asia, or Europe, these organizations including insurance companies, claims networks, pharmacy benefits managers, and managed care organizations, many with questionable value propositions, are poor stewards of your privacy and not necessarily aligned with you or your provider's best healthcare or economic interest.



Without the free flow of data or a data sharing mandate, the current healthcare actors, especially large digital incumbents seeking to enter the healthcare market (Google, Apple, Amazon), are effectively preventing the advancement of artificial intelligence in healthcare and disease prediction systems due to design bias resulting from competitive data hoarding.

More importantly, these digital silos are putting consumers and patients at national security threat risks from state and non-state actors seeking to weaponize healthcare data and future algorithms regarding civilian populations.

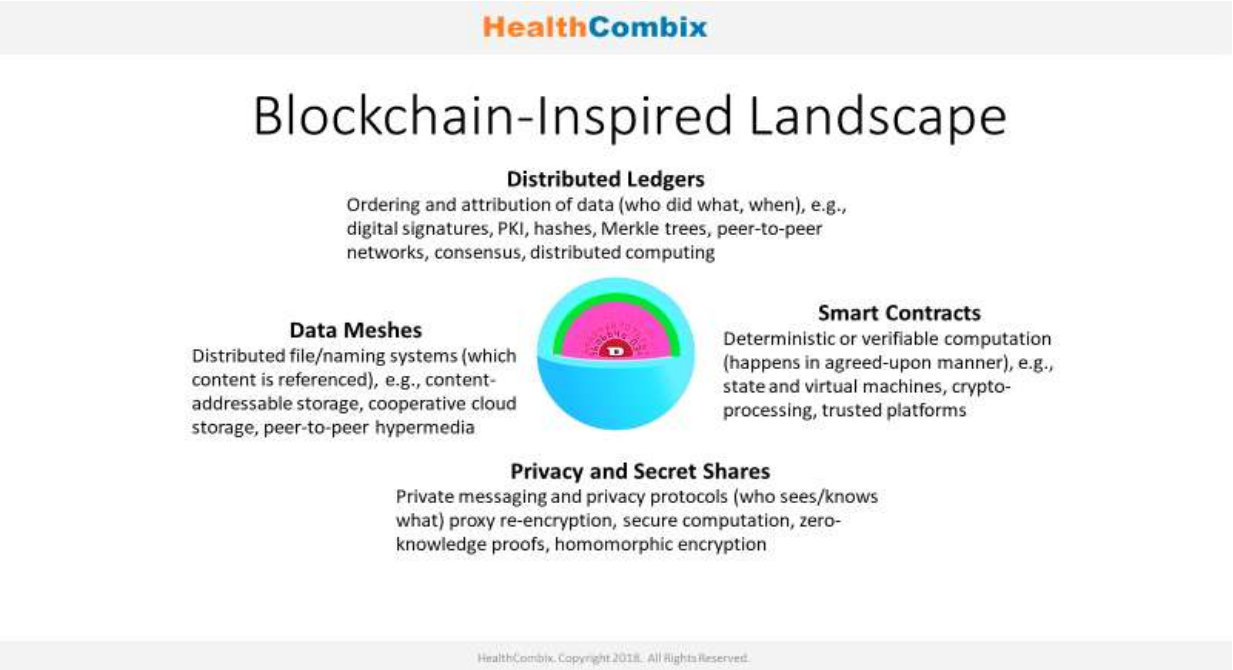
Replacing the existing market structure with decentralized blockchain networks, shared secrets, and tokenization would translate into the displacement of *unnecessary and opaque businesses and processes* while creating a vastly more secure environment for all stakeholders.

The HCX conditional payment infrastructure will redefine the flow of healthcare data with payments as a mechanism to assure the fluidity, accuracy, sharing, rightful monetization, performance centric compensation, and maximum security and privacy.

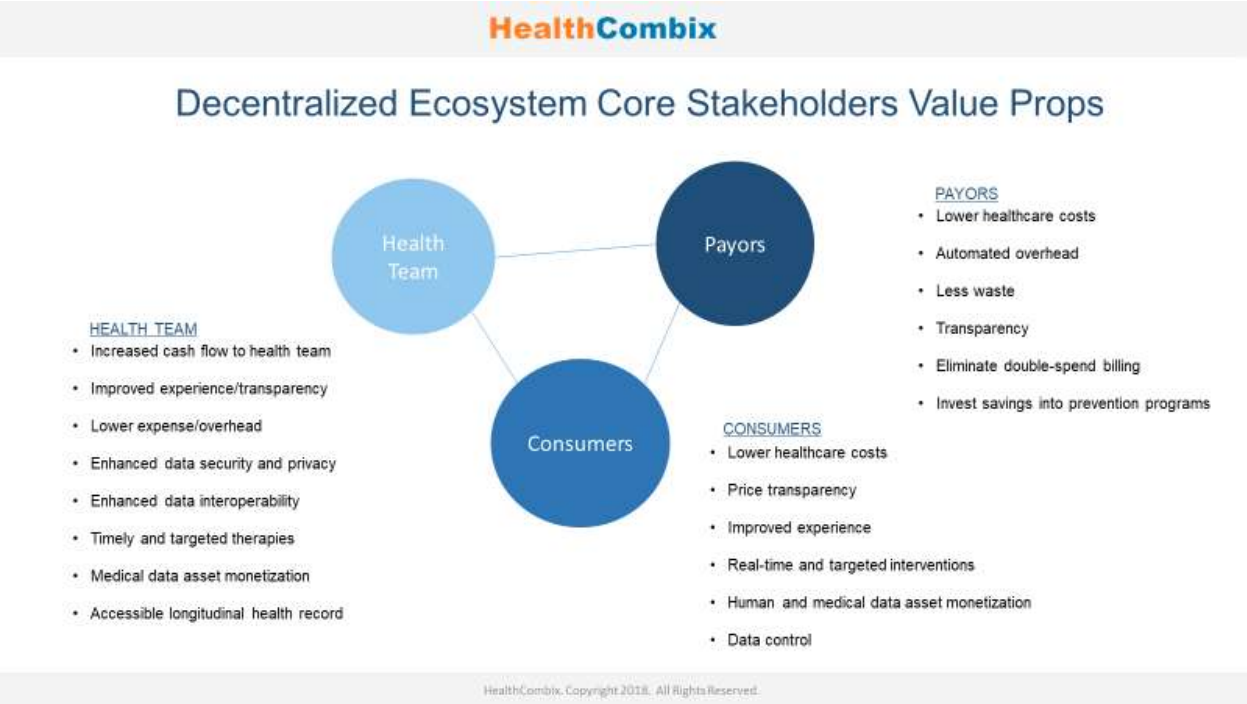
Blockchain-inspired technology will transform the macro healthcare industry and distribution of capital and influence.

Blockchains and distributed networks are infrastructures to be adopted by a critical mass of healthcare counterparties or implemented across an existing ecosystem. These networks will replace existing centralized infrastructure and help redefine the terms "firm" and "company" over time to the network.

The emergence, convergence, and scalability of blockchain-inspired technology (distributed ledgers, privacy and secret share technology, digital contracts, and data meshes), trusted witnesses or oracles, cryptographic currency, and machine learning, are all necessary conditions to create the efficiencies promised by blockchain and decentralization.



These efficiencies can reduce the cost of capital pooling, virtualize underwriting, automate overhead, eliminate double-spend billing, optimize human resource allocation, improve pricing transparency, reduce bad acts, and enhance operational and performance predictive analytics. Eliminating or reducing medical fraud is a significant benefit to society as this is a $500 Billion annual global problem. The resulting efficiency savings can be realized and allocated to the *right participants* including the patients, providers, clinics, suppliers, and risk management advisors. The chart below illustrates the decentralized ecosystem value proposition for health team, payers, and consumer, the right participants.



In addition to administrative savings, decentralization and self-sovereign privacy-preserving technology will enable new and innovative ways to enhance patient data privacy, security, and control, stimulate patient engagement behavior, streamline data-asset monetization, and ultimately improve outcomes as data availability, recency, integrity, and verification are optimized enabling timely and targeted therapies and tokenized rewards.

In combination with smart contract and tokenizing capabilities, the HCX PAY privacy-based payment network will enable conditional payouts, payment and behavior confidentiality, business transaction privacy, reduced payment friction, reduced payment cycle times, and reduced transaction fees. The HCX PAY network will be comprised of both open source and proprietary technology to be expressed via widgets, APIs, and solutions for participants to build new and lean innovative processes, marketplaces, and on-demand delivery to improve operational efficiency, transparency, and facilitate the creation of new and highly performant healthcare delivery models.

Network Opportunities

The HCX PAY network will initially focus on payment related use cases where trust is an issue, transaction costs are high, and where conditional payments can improve the overall patient experience and transparency, and anonymous witnesses validate out-of-clinic events.

As the blockchain-inspired technology stack matures, HealthCombix will develop or partner with ecosystem companies building advanced capabilities that will enable the delivery of healthcare ecosystem solutions that are highly-efficient, scalable, and secure with high data integrity.

HCX PAY is designed as a core privacy payment infrastructure capability to integrate with future components including non-fungible tokens, smart contract systems, proxy re-encryption, distributed data meshes, trusted oracles, identity, and other layers that can scale with the growth of the envisioned HealthCombix ecosystem.

HCXP mining node operator network management and toolbox

After a brief market test, HealthCombix discovered that over 75% of respondents who reserved a mining node are interested in mining but don't have the technical or financial ability or staff to manage their own mining nodes.

The market test included a short Google AdWords campaign and a mailing to our stakeholders as well. There were over 100 reservations made for Docker-based and virtual miners.

The market test results broke down as 75% for a virtual miner, 16% for Docker download, and 9 percent for enterprise support. More conclusive market tests will be conducted.

Approximate Miner Reservation Locales

Consequently, we will launch just after Mainnet a revenue generating Virtual Mining eCommerce platform to support this large group of interested parties and to accelerate network growth.

HCXP Virtual Node Management and Product Development Proforma

Profit & Loss	2018	2019	2020	2021
Revenue	3,238	362,868	1,299,997	2,008,504
Operating Expenses	208,895	1,365,203	1,897,520	1,885,820
NOI	**(205,657)**	**(1,002,334)**	**(597,523)**	**122,684**

Our HCXP node goal is to grow the network to over 2,500 virtual nodes over the first two years of operations. The operating expenses in the above proforma includes both node management operational and product development costs. The proforma includes projected virtual node management subscription revenue and does not reflect revenue generated

from other opportunities identified below. The virtual node operator revenue will be used to offset development costs in the early stages of the project's development.

We believe the development of both our Docker-based and virtual miners will enable us in the future to become a distribution mechanism for future ecosystem partners seeking distribution and access to our healthcare node mining participants.

Additionally, our roadmap includes the development of an ecosystem ToolBox for employers and healthcare participants to integrate with our network and components. The HCX PAY ToolBox will support revenue management, EHR, HSA, POS, Apple, FHIR, and ecosystem partner integration. We believe the ToolBox will help end-users to quickly develop, test, and implement our network and ecosystem components with minimal disruption to their internal operations.

Cross-border healthcare markets

People from all over the globe every year travel to different countries for healthcare services for a variety of reasons including lower costs, specialist availability, and higher quality facilities.

The current size of the cross-border healthcare market is $54 billion and is projected to grow by 25% per year through 2025, according to studies conducted by Deloitte and Visa International.

Trust, transaction costs, and verification are key payment related pain points in cross-border healthcare. Additionally, pain points exist around data sharing and portability, translation, outcome-based (conditional) payments, and reimbursement.

The healthcare cross-border market is highly fragmented with fractured offerings by regional handlers, consultants, travel agencies, and other non-medical providers. The market is opaque as provider and facility reputations are difficult to assess and maintain. Middlemen inflate costs

and obfuscate quality indexes. Lastly, post-trip remote patient status verification is a challenge for providers to determine outcomes.

Cross-border healthcare transaction costs are high with many correspondent banks and intermediaries assessing significant gatekeeper fees. Cross-border payments are typically large sum in the $10,000-$100,000 range (or even higher) depending on the services rendered. Cancer and heart disease treatment are the two most commonly sought-after cross-border care. The HCX PAY network combined with a future bundled token travel wallet and payment-like card capability will foster adoption, reduce costs, engender trust, and facilitate the transfer of funds and data.

Employer channel partnering

Amazon, JP Morgan, and Berkshire Hathaway teamed up recently to disrupt healthcare. Berkshire Hathaway Chief Executive Warren Buffett who described increasing health care costs as "a hungry tapeworm on the American economy" in a press release statement, adding that the three companies do "not come to this problem with answers. But we also do not accept it as inevitable. Rather, we share the belief that putting our collective resources behind the country's best talent can, in time, check the rise in health costs while concurrently enhancing patient satisfaction and outcomes."[i]

The use of open public networks such as HCX PAY and complimentary ecosystem components such as reputation systems, provider identity ledgers, tokenized delivery contracts, and distributed data-driven machine-learning can enable employers to build their own transparent and cost-effective ecosystems. An employer-based ecosystem would integrate risk management, healthcare delivery, and payments by reducing the need for third-party administrators, managed care companies, siloed EMR companies, and insurers underwriting risks.

HCX PAY ecosystem infrastructure will enable employers to onboard health team members, employees, and risk management experts to create a

lean peer-to-peer healthcare system to deliver healthcare directly to their employees in the timeliest, most cost efficient, and data driven way possible while maintaining optimal data security.

Virtual care and on-demand delivery

Virtual care or telemedicine and blockchain technology can both enable consumer and provider empowerment while reducing the cost of healthcare delivery and improving the overall experience for clinician and patient. How much healthcare can happen over the Internet? In the home or by the patient remotely being assisted? Bringing healthcare to the consumer and creating an ecosystem of video and on-demand healthcare providers will help drive down the cost of healthcare around the globe and maximize data fluidity and security.

The inherent security characteristic of the cryptographic distributed ledger will enable the inversion of the existing healthcare system. This will eliminate centralized processors that add little value including pharmacy benefits managers, credentialing, staffing, managed care organizations, and insurance companies. Virtualizing and decentralizing healthcare workforces will ultimately improve data collection, personalization, and automate value-based care programs to drive intermediary costs out resulting in savings for both providers and consumers.

Uberizing medical claims and patient adherence with anonymous witnessing

You see a doctor at their office. Tests are ordered. The doctor examines you. The doctor diagnoses you. A treatment is prescribed. The doctor schedules a follow up appointment. Insurances companies reimburse after the fact for the doctor's exam, tests, and drugs and supplies. In a decentralized provider ecosystem (physicians' network) with a virtual underwriter or medical smart cost sharing network, witnesses will be needed to verify claims and to approve payouts. To prevent fraud and assure quality, anonymous and qualified witnesses, e.g., nurse practitioners, are needed to validate real world events to trigger payments

for services rendered. These anonymous witnesses can be randomly assigned to validate claims and physicians' work as well as confirm that the patient has adhered to treatment plans outside of the clinic. Token rewards and reputation can be used as the carrot and stick for both patient and provider.

Virtual underwriting (smart syndicates), medical cost sharing, and health trust networks

HealthCombix believes peer-to-peer insurance, medical cost sharing networks, and smart health trusts will emerge as value is pushed out to the edges of the network and away from centralized trusted parties enabled by blockchain-inspired technology. Transparency, auditability and provenance of pooled funds are assured by being recorded in the blockchain. A fully peer-to-peer model would not be possible without the blockchain. Parametric insurance is a binary yes-or-no triggered claim and signoffs will release a lump sum payment to cover the predetermined cost of care. This deterministic nature of parametric insurance makes it a natural fit for early HealthCombix blockchain/smart contracts. Plus, the provenance of premiums paid, proof of funds and solvency, and peer-to-peer network stake of memberships is public, verifiable transactional data recorded on the blockchain. The HealthCombix ecosystem will be built to effectively handle the traditional insurance, trust, or medical cost sharing operation including actuarial work, underwriting marketplace, claims, and payments. As trusted oracles evolve, such as Town Crier, combined with witnesses, non-parametric insurance will evolve as well and further diminish the need for large insurance companies.

Data fiduciaries and curators

The self-sovereign vision of healthcare data or any personal data being in the control of patients is a noble one. We believe that ultimately for the sake of security, patient safety, and improved health outcomes, patients in control and cognizant of their data is critical. Although the patient rightfully owns its data, the reality today is that self-sovereignty and

decentralized thinking require behavior change which is a big blocker for the adoption of self-controlled data.

As a gateway to self-sovereignty we believe new roles will emerge for trusted healthcare professionals to assist consumers with the creation and management of their healthcare records. Studies have demonstrated that even when patients are provided with portals to download their personal health records that few take advantage of this. We believe this will persist without the proper incentive or reward structure and assistance with managing the curation of data.

Lastly, we believe that human data monetization will emerge over time but will require third-party fiduciaries to help curate and market your self-sovereign data to buyers for clinical trials, precision medicine, and other uses. These fiduciaries would act as advocates for consumers and perhaps share in the successful monetization of the patient's data.

HCX PAY Platform Capabilities

HCXP peer-to-peer private payment wallet

The HCXP network will initially launch with a Linux based command line simple wallet for sending and receiving HCXP for miners and stakeholders for general use and testing. This wallet will be released with the daemon and other components via our Docker image on the Docker Hub public repository. The wallet can also be used by miners with the HCXP daemon to store mined tokens. In conjunction with a web based virtual mining node system, HealthCombix will release a platform for non-technical miners to store their earned tokens and send and receive tokens 24/7 from any device via the web.

The HCXP product roadmap includes the development of wallets for a variety of platforms including Windows, MacOS, iOS, and Android.

HCXP mining, decentralization, and virtual nodes

To achieve wide, decentralized distribution of the HCXP node, HealthCombix is building a Docker based node distribution system to simplify the installation and operation of the HCXP node for miners and future enterprise users. In addition, a virtual node mining and web wallet system is under development for non-technical users interested in supporting the growth of the HCXP network and mining for HCXP.

The virtual mining node system utilizes a proprietary multi-signature wallet system integrated with a web-based wallet and platform for selling hosted (virtual) mining plans. The system dynamically provisions mining accounts and wallets across multiple cloud partner systems in geographies around the globe with redundant backup key management.

Tokenization and healthcare

As blockchain tokenization standards emerge, the HCX PAY platform will create token generators to codify alternative payments such as bundling

and wrap-arounds, disease management programs, device management, and provider and patient reward strategies.

When discussing tokenization and blockchain, the most common types of tokens today are so-called utility tokens in the form of the Ethereum (ERC-20) standard token. While many of these tokens do not actually provide any value or utility, there will be some decentralized applications and protocols that will, and henceforth challenge and transform traditional industries including healthcare.

An asset backed token is a blockchain token that is connected to a tangible or intangible object that has economic value. There are fungible (often referred to as utility tokens) and non-fungible (ERC-1265) asset backed tokens that can represent various real-world (contract) assets. Non-fungible means that one unit is not equal to another similar unit; two emeralds of equal dimensions are still not interchangeable.

An asset backed token essentially digitizes an asset and records its associated information on a blockchain. For example, a medical device could have a digital record, instead of a paper one. A token that represents a specific medical device could be created which would store information about the device, such as ownership/history/maintenance, and anything else desired. The token could be easily transferred to another owner when the device is sold.

The potential of tokenization of both tangible and intangible assets will create new opportunities for the development of new markets to improve the management of assets, transferability of ownership, and transparency and price discovery. Redefining healthcare with definable tokens will help drive down the costs of asset management (people, services, and procedures), reduce the friction of contracting, and provide conditional payouts for a variety of scenarios in payments, delivery, and data monetization.

Data privacy, proxy re-encryption, and payment

HealthCombix believes giving the patient ownership and control over their own medical data in a decentralized system is imperative for the long-term security, safety, and wellbeing of the patient. Although replacing highly vulnerable and centralized medical record keepers, like Epic, is not likely to happen anytime soon, we believe starting with decentralized personal health record ownership is a good evolutionary use case for distributed networks.

A decentralized record keeping service is only feasible if the data always remains properly encrypted but still shareable with multiple parties, including medical providers, applications, insurance companies, medical researchers, or even other patients.

With NuCypher's proxy re-encryption blockchain network, a HealthCombix security ecosystem partner, future patients using the HCX PAY data wallet incorporating the NuCypher proxy-re-encryption network, could encrypt and store each medical record with their own encryption keys and then upload their encrypted records to a data mesh of their choice such as IPFS or AWS.

A patient who wants to grant access to a healthcare provider can create a new re-encryption key using the healthcare provider's public key and issue it to the NuCypher Network. The network will use the re-encryption key to transform the encryption on the medical record, so that the healthcare provider can decrypt them using their own private key. The patient can revoke access to that healthcare provider at any time by issuing a revocation request to the NuCypher network. At that point, the service provider would no longer be able to decrypt the encrypted records.

HCX PAY is currently researching the integration of the NuCypher network with the HCX PAY protocol in the form of a validated and conditional payload to improve both the patient's and provider's overall experience.

Blockchain and CryptoNote Algorithm Technology [ii, iii, iiii]

CryptoNote algorithm

This section of our white paper highlights key foundational capabilities introduced by the original creator(s) of the algorithm. [iii, ii] The CryptoNote (Night) algorithm and derivative modifications are released under an open source license and have been adopted and incorporated into HCX PAY. This forms the basis for a well-tested cryptocurrency core. The CryptoNote white paper was released in 2013 with subsequent derivative improvements from a variety of projects such as Monero, Bytecoin, Graft, etc.

Untraceable payments and ring signatures

The conventional digital signature verification process requires the public key of the signer. This is a necessary condition, because the signature proves that the creator possesses the corresponding secret key. But this is not always an adequate condition such as with public networks where creators desire privacy and confidentiality from third-parties surveilling business or sensitive medical or healthcare transactions. For example.

Ring signature is an advanced signature verification scheme which requires several different public keys for verification. The ring represents a group of creators or individuals/entities that possess their own private and public key pair. The ring verification scheme proves that the signer of a

given message, i.e., a transaction, is a member of the ring, but the verifier will not be able to establish the exact identity (public key) of the signed.

Ring signature is used to make HCX PAY transactions untraceable by using the public keys of other members in the ring signature applied to transactions. This application of ring signatures proves that the creator of the HCX PAY transaction is eligible to spend the amount in the transaction.

This approach proves that the creator of the transaction is eligible to spend the amount specified in the transaction, but his identity will be indistinguishable from the users whose public keys he used in his ring signatures.

Although your public key may appear in another's ring signature, its use is only for obfuscation purposes. Additionally, if two parties create ring signatures with the same set of public keys, the signatures will be different as the private keys of each are unique.

Unlinkable transactions

Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature. To avoid linking, you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address. (2)[iv]

CryptoNote solves this dilemma by an automatic creation of multiple unique one-time keys, derived from the single public key, for each p2p payment. The solution lies in a clever modification of the Diffie-Hellman

exchange protocol. Originally it allows two parties to produce a common secret key derived from their public keys. In our version the sender uses the receiver's public address and his own random data to compute a one-time key for the payment.

The sender can produce only the public part of the key, whereas only the receiver can compute the private part; hence the receiver is the only one who can release the funds after the transaction is committed. He only needs to perform a single-formula check on each transaction to establish if it belongs to him. This process involves his private key; therefore, no third party can perform this check and discover the link between the one-time key generated by the sender and the receiver's unique public address.

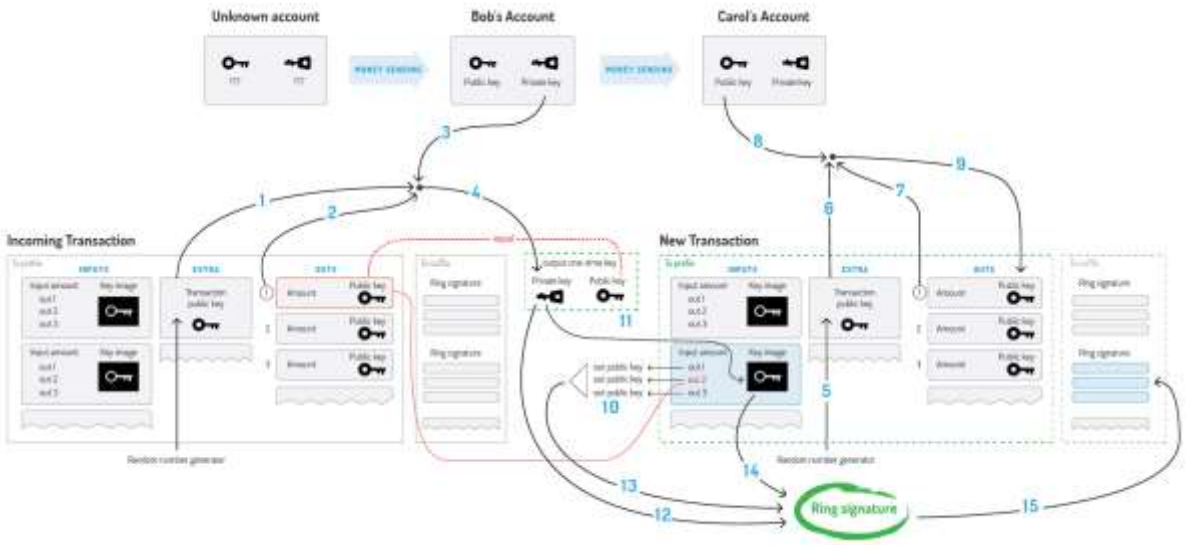
An important part of our protocol is usage of random data by the sender. It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions. This is why the key is called "one-time". Moreover, even if they are both the same person, all one-time keys will also be unique.

Standard CryptoNote transaction

A standard HCX PAY CryptoNote transaction is generated by the following sequence covered in the 2013 white paper:

- Bob decides to spend an output, which was sent to the one-time public key. He needs Extra (1), TxOutNumber (2), and his Account private key (3) to recover his one-time private key (4).
- When sending a transaction to Carol, Bob generates its Extra value by random (5). He uses Extra (6), TxOutNumber (7) and Carol's Account public key (8) to get her Output public key (9).
- In the input, Bob hides the link to his Output among the foreign keys (10).
- To prevent double-spending, he also packs the Key image, derived from his one-time private key (11).

- Finally, Bob signs the transaction, using his one-time private key (12), all the public keys (13) and Key Image (14). He appends the resulting Ring Signature to the end of the transaction (15).



Adaptive limits

A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer. Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum). Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state. Therefore, it always changes adaptively and independently, allowing the network to develop on its own.

CryptoNote has the following parameters which adjust automatically for each new block:

1) Difficulty. The general idea of our algorithm is to sum all the work that nodes have performed during the last 720 blocks and divide it by the time they have spent to accomplish it. The measure of the work is the

corresponding difficulty value for each of the blocks. The time is calculated as follows: sort all the 720 timestamps and cut-off 20% of the outliers. The range of the remaining 600 values is the time which was spent for 80% of the corresponding blocks.

2) Max block size. Let MN be the median value of the last N block's sizes. Then the "hard-limit" for the size of accepting blocks is 2*MN. It averts blockchain bloating but still allows the limit to slowly grow with the time if necessary. Transaction size does not need to be limited explicitly. It is bounded by the size of the block.

Smooth emission

The upper bound for the overall amount of all digital coins is also digital:

$$MSupply = 2^{64} - 1 \text{ atomic units}$$

This is a natural restriction based only on the implementation limits, not on intuition like "N coins ought to be enough for everybody". To make the emission process smoother, CryptoNote uses the following formula for block rewards:

$$BaseReward = (MSupply - A) >> 18$$

where A is the amount of previously generated coins. It gives a predictable growth of the money supply without any breakpoints.

Egalitarian proof of work

The proof of work mechanism is a voting system. Users vote for the right order of the transactions, for enabling new features in the protocol and for the honest money supply distribution. Therefore, it is important that during the voting process all participants have equal voting rights. CryptoNote brings the equality with an egalitarian proof-of-work pricing function, which is perfectly suitable for ordinary PCs. It utilizes built-in CPU instructions, which are very hard and too expensive to implement in special purpose devices or fast memory-on-chip devices with low latency.

We propose a new memory-bound algorithm for the proof-of-work pricing function. It relies on random access to a slow memory and emphasizes latency dependence. As opposed to Scrypt, every new block (64 bytes in length) depends on all the previous blocks. As a result, a hypothetical "memory-saver" should increase his calculation speed exponentially.

Our algorithm requires about 2 MB per instance for the following reasons:

1. It fits in the L3 cache (per core) of modern processors, which should become mainstream in a few years;

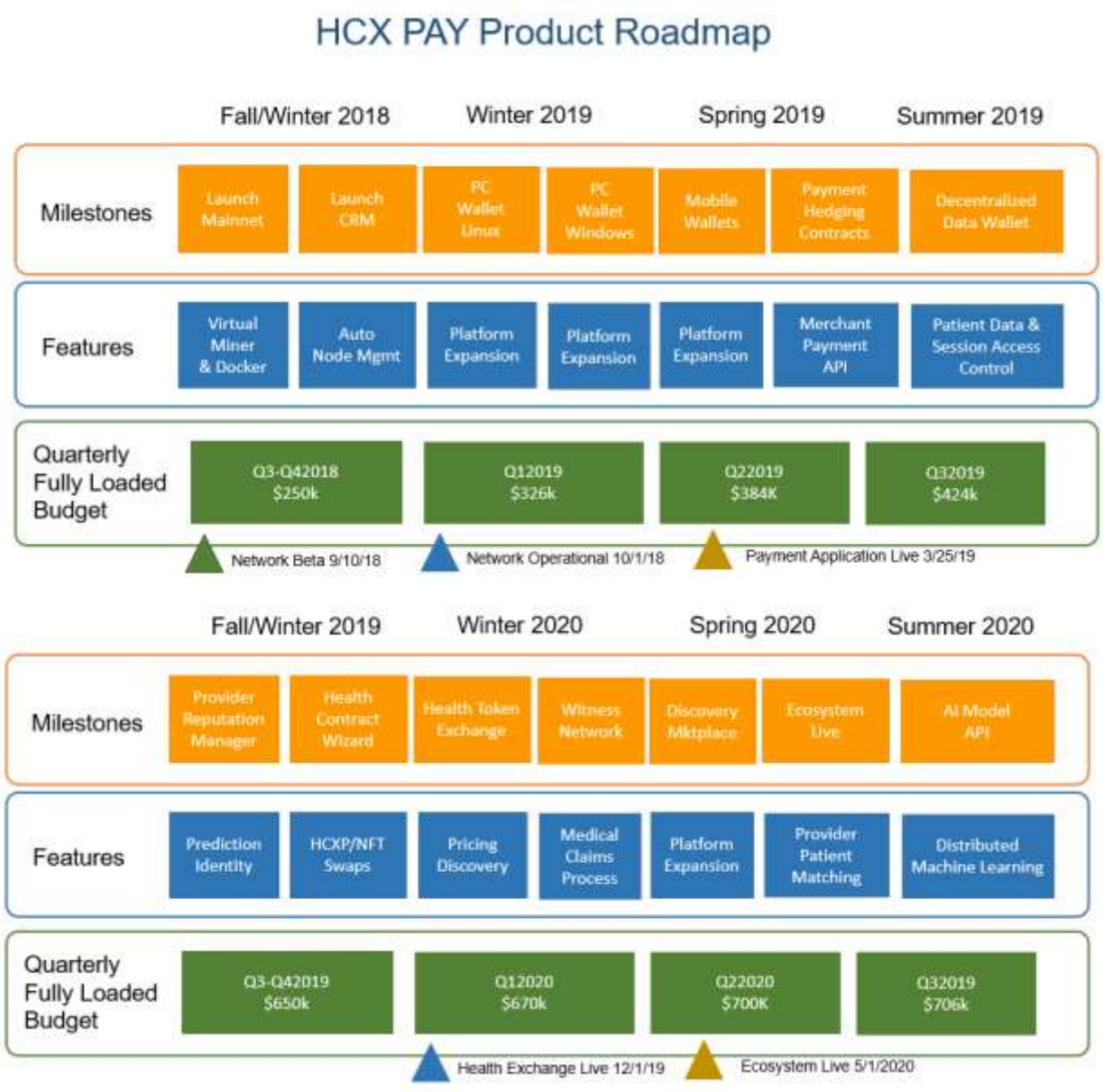
2. A megabyte of internal memory is an almost unacceptable size for a modern ASIC pipeline;

3. GPUs may run hundreds of concurrent instances, but they are limited in other ways: GDDR5 memory is slower than the CPU L3 cache and remarkable for its bandwidth, not random-access speed.

4. Significant expansion of the scratchpad would require an increase in iterations, which in turn implies an overall time increase. "Heavy" calls in a trust-less p2p network may lead to serious vulnerabilities, because nodes are obliged to check every new block's proof-of-work. If a node spends a considerable amount of time on each hash evaluation, it can be easily DDoSed by a flood of fake objects with arbitrary work data (nonce values).

Roadmap

The HCX PAY product development roadmap begins with the development and integration of the foundational technology (ledger, privacy, data mesh, and contracts) in support of the development of ecosystem applications including provider and service discovery, virtual underwriting, data control, virtual delivery, tokenized health contract, and medical cost sharing.



Network Condition and Token Economics

The HCXP token

The token which is used on the HCX PAY blockchain is called HCXP. HCXP is a usage or utility token. The transaction from one HCXP account to another lasts only a few seconds. It is an intrinsic token because, like Bitcoin, it is used to write to the blockchain by paying transaction fees. The transaction fee depends on the number of inputs, outputs, and the Ring size. Due to the "Ring signature technology," the transaction fees are much lower compared to Bitcoin's.

HCX PAY network attributes

- Consensus: Proof-of-work (POW)
- Hash Algorithm: CryptoNight
- Block creation time: 60 seconds
- Circulating Supply: 260 Million HCXP
- Total Supply: 2 Billion HCXP

Supply allocation

The HCX PAY Mainnet will launch with a total supply of 2 billion HCXP. 260 million of which will be allocated towards the development, testing, and maintenance of the core network, incentivizing ecosystem partners, providers, patients, team, liquidity providers, and social purposes.

Core Team

Cyrus Maaghul, the founder of HealthCombix®, is a startup and product development professional based in Nashville, Tennessee. He has over 20 years' experience in launching technology product and services companies and helping develop systems and product strategy for startup and large companies including ***PointNurse®, Digital River***, Deloitte Consulting, ***Fidelity Investments***, and Citibank. Cyrus founded and successfully exited two internet payment companies in 2001 and 2006. He formerly served as the Director of Blockchain Product Development in the Fidelity Investment Blockchain Incubator. Cyrus earned his BA and MS in Applied Mathematics and Psychology from SUNY Stony Brook. Cyrus' thought leadership has been published on Coindesk.com, Nasdaq.com, and Distributed.com. Cyrus enjoys hiking, scratch cooking, and Bikram Yoga.

Dr. Andreas Freund, based in San Diego, California, has worked in various technology leadership roles in the financial services, management consulting, and technology industries. He is a recognized and published leader in blockchain and distributed technology, currently working as a strategist for the leading global Ethereum consultancy, ***ConsenSys***. He previously led Tata Consultancy's international blockchain technology advisory group. Andreas has hands-on design and development experience with various distributed system projects in areas including consensus, IoT, blockchain scaling, digital identity, and healthcare blockchain applications. Andreas' earned his PhD in Physics from Pennsylvania State University. Andreas is a busy family man when he is not ideating decentralization.

Jason Ma, a blockchain revolutionary, is a lead software engineer who is experienced in blockchain and full-stack web development. Jason is based in Hong Kong. During the last 10 years, he has worked with several startup companies successfully bringing new blockchain and web software systems and platforms to market. Jason is an expert in C++ and C software engineering with full lifecycle development experience including architecture design and systems level coding. He holds a master's degree in computer science and technology from Tsing Hua University earned in 2012. Jason enjoys playing volleyball and watching baseball.

Mathew Conboy is a healthcare professional with a background in strategy, risk assurance, and technology. He began his career as a healthcare and financial services consultant at PricewaterhouseCoopers (PwC), serving clients in healthcare and life and disability insurance. Conboy is currently a director of innovation at CareAllies, a ***Cigna*** company, and leads solution development for CareAllies's home-based chronic care management division, Allegis Care. Prior to joining CareAllies, Conboy worked for Cigna's enterprise strategic operations team, helping business unit leaders translate enterprise-level strategy into operational plans. In addition, **Conboy co-founded Cigna's internal blockchain team**, which assesses blockchain-specific opportunities in alignment with Cigna's strategy. Mathew is a triathlete.

Mitchel Schwindt, MD, is a board-certified emergency medicine physician, author, and clinical consultant. In addition to practicing emergency medicine, he is engaged in a multitude of projects related to medicine and internet entrepreneurial activities. He has hands-on telemedicine experience and has published a book on telemedicine best practices. Dr. Schwindt **completed his residency at Michigan State University and received his MD from the University of North Dakota School of Medicine**. Mitchel is **a triathlete** and marathon runner who enjoys pushing the outer limits. Mitchel is based in Minnesota.

Andrey Zhelnin, based in Poland, has worked for various outsourcing and IT solution companies as a software developer, system administrator, and network analyst. He has played leading roles including cloud system architect, DevOps lead, team manager, and unit manager designing and overseeing large data center networks, operations, and infrastructure. His technical skills include Python, Ethereum, Hyperledger, Zcash, **CryptoNote, Linux, Docker, VMware, Ansible**, and various other network and data center infrastructure platforms. Andrey received his master's degree in electrical engineering from Samara State Technical University. Andrey enjoys being with his family and photography.

Jim Spring, who splits his time between the Bay Area and Sierra Mountains, is a seasoned technologist with broad experience ranging from the design, development, and deployment of large SaaS offerings and distributed systems to building and optimizing applications on constrained and embedded devices. His specialties include security (pki, protocols, network, algorithms), scaling distributed systems, server architectures, file systems, compression, image and video coding, and cobbling esoteric technology solutions together for legacy systems. **Jim has worked for companies including Microsoft and Skype.** Jim received his bachelors and master's degree in computer engineering from the University of California, Santa Cruz.

Annax Thongsami received his B.E. degree in computer science and information technology from the National University of Laos. His career began in operating systems development for embedded network devices. His technical skills developed during this period included Linux systems development, C, C++, and bash. Annax then expanded his skills in applications and database development coding JSP, PHP, and SQL databases developing for companies around the globe. Over the past five years, Annax has focused his attention on mobile applications development, honing his iOS and Android systems and application development skills. Annax is currently researching and developing mobile crypto-wallet and mining systems.

Roni Fox is a licensed Mental Health Family Nurse Practitioner, primary care clinic owner, and consultant based in Phoenix, Arizona. Roni received her MSN/FNP from the University of Arizona and BSN from the University of Phoenix. She was formerly a Linux engineer and technology professional at IBM prior to pursuing her career in healthcare. She is currently Treasurer of the Arizona Nurse Practitioner Council. Roni enjoys reading, gardening, and anything organic or earth-friendly.

Endnotes

---

[i] *Amazon, Berkshire Hathaway and JPMorgan Team Up to Try to Disrupt Health Care*, New York Times, Jan 18, 2018

[ii] *CryptoNote Whitepaper Review by Monero*, Jul 15, 2014

[iii] *CryptoNote v 2.0 White Paper Nicolas van Saberhagen*, October 17, 2013

[iv] *Review of Cryptonote White Paper, Surae Noether*, July 14, 2014