A foundation of trust for the future of healthcare: An overview of the BitMED Health Protocol (BXP)

Bo Vargas and Rishi Madhok, MD
BitMED Incorporated, BitMED.io
March 2018

Abstract

BitMED introduces the BitMED Health Protocol (BXP), a consortium blockchain protocol and token ecosystem designed to form a secure foundation for the future of health data transaction and management. The BXP leverages from existing blockchain protocols, including Ethereum, InterPlanetary File System (IPFS), and Hyperledger, and adds functionalities for the needs of a global healthcare market. BXP has been developed upon an open-source distributed consensus ledger, Internet protocol, and native token currency called BXM. BitMED enables instant, safe, and low-cost healthcare access of any scale. The protocol supports decentralized applications, smart contracts, prevents double-spending, and supports health outcome nano-payments.

Note: BitMED is a work in progress. New white papers on updates to the system will be posted on our repo. For comments and questions, reach us at https://www.bitmed.io/contact-us/.

Table of Contents

1. Introduction **4**

2. Why healthcare needs its own blockchain protocol **5**

2.1 A short overview of relevant problems in healthcare **5**

Healthcare is zero trust 5

Legal and regulatory barriers are preventing innovation 6

Health data is fragmented, inaccessible, and incomplete 6

2.2 Existing blockchains don't work for healthcare **7**

Legal and regulatory requirements 7

The problem of scale 8

3. Introducing the BitMED Health Protocol (BXP) **11**

3.1 How it works **11**

1. go-Ethereum 11

2. The BXM Protocol 11

3. The BXM token 11

4. BXM token mining 12

5. Decentralized applications, or dApps 13

Example token use 13

3.2 Borrowing what works, building what's missing **14**

Hyperledger/Quorum Fork 15

The Red Belly Blockchain (RBBC) algorithm 15

3.3 Benefits **16**

Increases access to care 16

Increases access to accurate health information 16

Enforces compliance while reducing its cost 16

Lowers transaction costs and reduces fraud 16

Securely stores healthcare data and protects personally identifiable information (PII) 17

Scales to the needs of healthcare 17

Incentivizes data sharing 17

4. Conclusion **19**

References **20**

1. Introduction

BitMED has developed a digital health platform to create global access to healthcare that is user-friendly, personalized, and affordable. Our blockchain implementation and utility token, BXM, creates an infrastructure to incentivize the healthcare eco-system with the following key features:

- Care: Members can access board certified medical providers in a range of specialties via the BXM token from anywhere in the world.
- Community: Members are incentivized to connect and communicate about their health, whether with AI system(s), a neighbor down the street, or people with shared experiences.
- Content: Members are incentivized to create, validate, share, and consume accurate health information.
- Data: BXP utilizes smart contracts to maintain confidentiality, integrity, and availability.
- Providers: Provider identity and practice profile verification are incentivized to maximize the medical professional supply.
- Therapeutics: Allows patients access to drugs, devices, and treatments regardless of time and location while securing use and intellectual property.
- Insurance: Smart contracts create price, coverage, and service transparency on demand for all parties.

BitMED is redistributing relationships and roles to reflect necessary changes in healthcare. Decentralization and the individual's increasing participation in their health data provide an opportunity to realign healthcare to its original, ideal goals.

Problems in healthcare are complicated and numerous, and technical solutions that do not account for regulatory, legal, and cultural challenges and requirements are no solutions at all. As a technical solution, the BXP is one part of BitMED's roadmap to a new foundation in healthcare and health data management. If you'd like to help build the future, please join us. The crypto-community is essential to the journey ahead.

The scope of this white paper is the BXP, what it does, and how it works. It doesn't cover every part of BitMED's mission, but you can find more information at BitMED.io.

Who this white paper is for

The primary intended audience for this white paper is the cryptography and cryptocurrency community. Readers should be somewhat familiar with blockchain technology. A great primer for beginners is Explain Bitcoin Like I'm Five by Nik Custodio for freeCodeCamp's Medium community or Blockchain's Learning Portal.

2. Why healthcare needs its own blockchain protocol

For us every day is a new opportunity to tell people about our mission and plans for achieving it. Nearly everyone in the cryptography, security, and privacy world has responded along the same lines:

> "Why not use Ethereum?"
> "Aren't you describing Hyperledger? Just use that."
> "Why are you building a new blockchain? Why not use what's already out there?"

Indeed, existing blockchain systems are robust enough for many kinds of sensitive data transactions, so why not health data? The short answer: transacting health data with existing blockchain protocols breaks the law.

To more thoroughly answer this question, we'll start with brief explanations of some of the most pressing problems in healthcare. Then we'll briefly describe existing blockchains, and what about them doesn't work for the use case of securely storing, updating, and transacting health data anywhere in the world.

2.1 A short overview of relevant problems in healthcare

Healthcare is burdened with too many problems to cover in this white paper. As medical providers, entrepreneurs and technologists, the BitMED founding team have experienced many of them firsthand. The main and overarching problem for our purposes is that actors within the system can't trust each other.

Healthcare is zero trust

Healthcare systems operate such that no party can trust another. Every transaction or agreement in healthcare is bogged down with time-intensive and expensive processes that are necessary for any degree of security and confidence.

- Providers don't trust insurers to reimburse for procedures, and increasingly, even to cover them in the first place. Due to changing regulations and healthcare markets in the U.S., many clinics and hospitals have changed the insurance they accept year by year.
- Insurance companies don't trust providers, regularly contesting claims and adding to providers' administrative burdens. The American Medical Association (AMA) has estimated that inefficient claims processing costs 10-14% of practice revenue [1].
- Patient trust in doctors and other healthcare professionals varies along many indicators: geography, socioeconomic status, culture, age group, etc. Patient trust in health insurance is more clear-cut; yearly results of the Harris Poll since 2003 have consistently shown it's one of the least trusted industries, faring barely better than oil and tobacco [2, 3].

To consider just one example, credentialing, let's say a doctor wants to work at a hospital in another state where doctors are more needed, so she applies and gets accepted. Could she start working there next month? No, because credentialing the doctor according to regulations in the new state takes an average of six months. These regulations are put in place to protect patients—you wouldn't want your doctor to

be practicing medicine without board certification. However, for doctors, this makes career moves more difficult than most professionals', and it contributes to the global shortage of doctors. The Association of American Medical Colleges reports that by 2025, the United States alone will be short 90,400 doctors [4].

Added to this, patients must first navigate prior authorizations—who, what, and when care is covered through their insurance policies—often restricting or delaying access to available providers. The AMA has found that "90 percent of surveyed physicians reported that prior authorization sometimes, often, or always delays access to care" [5]. Yet the care we do access is expensive, and costs are rising. In 2017 the CMS reported the U.S. is projected to spend a whopping 20 percent of GDP on healthcare by 2025 [6].

Patients foot the bill for the patchwork of credentialing and regulatory processes covering every aspect of the services they receive. Nestled somewhere within opaque language in their medical bills, they're paying for the time and expense involved in credentialing, certifying, and regulating every step of their care.

Legal and regulatory barriers are preventing innovation and access to healthcare

To varying degrees in healthcare systems around the world, legal and regulatory barriers initially intended to protect patients are now preventing badly needed innovation in care delivery.

Fragmented approaches to healthcare management has been an expensive and growing problem for decades. In 2010, the World Health Organization published a global study of health systems financing which found that, "Conservatively speaking, about 20–40% of resources spent on health are wasted, resources that could be redirected towards achieving universal coverage" [7]. They find the main culprit to be medicines—expensive brands over generics, antibiotic and injection overuse, poor storage, and wide variations in price—but this waste also includes inefficient hospital processes, medical errors, underutilized or inefficiently used technologies, and the way service providers are paid. Fee-for-service payment structures tend to over-serve those who can pay and under-serve those who cannot. In addition, local laws and regulations put walls around health data generated or recorded in each location. This is explained in more detail in Section 2.2.

Health data is fragmented, inaccessible, and incomplete

Data is the foundation for insights and development of healthcare innovation. Yet when compared to other industries, healthcare has been slow to benefit due to the entrenched problem of incomplete and inaccessible data across organizations.

Health records have been stored entirely on paper until relatively recently, but are increasingly stored electronically. These electronic health records (EHRs) are housed within healthcare systems with hospitals, not patients, in control of the data. However, healthcare consumers are mobile. They may visit multiple doctors in various institutions by choice or by forced circumstance. Unfortunately, their data does not travel with them. In fact, regulation around data privacy, intended to protect patients, has led to

both significant healthcare waste and patient harm in the form of treatment delays and errors, as well as over-testing and inappropriate testing.

It is important to note that the structure and focus of EHRs is not on accurate and effective recording of data for the patient and their wellbeing, but on medical billing. It is indisputable that EHRs have improved medical communication and data recording of health events for patients as compared to paper-based systems, but this process remains far from ideal.

When there is no incentive for parties in healthcare to share data, patients who need their data exchanged quickly between providers pay the price by waiting between each step of their care. Exchanging data between providers can take weeks with outdated administrative processes.

Furthermore, EHRs are woefully incomplete. Healthcare consumers don't live inside of hospitals; their lives go on once they leave they physician's office. Increasingly abundant health data collected via digital health products and services in between physician visits is rarely incorporated into a person's treatment plan. Most existing EHRs would have to be overhauled to allow for this.

2.2 Existing blockchains don’t work for healthcare

There are two main reasons why existing blockchains don't meet the needs of healthcare: 1) the legal and regulatory framework in which all healthcare services must operate, and 2) the transactions-per-second limitation of existing blockchain protocols when compared to the scale healthcare markets require.

Legal and regulatory requirements

In many nations around the world, including the U.S. [8], Germany [9], and Canada [10], the law mandates that personal health data cannot leave the country. Among the types of data one might consider transacting via blockchain, health data tends to be subject to further restrictions. For this reason alone, existing blockchains won't work for healthcare: it simply violates the law.

In Ethereum, data placed into a smart contract is shared with everyone, everywhere on the Ethereum Blockchain. The sharing of this data across borders violates the privacy laws of many countries. Hyperledger addresses performance scalability and privacy issues by permissioned mode of operation, specifically by using a Proof of Elapsed Time (PoET) and Proof of Work (PoW) consensus models and fine-grained access control. However, adjustment must still be made to account for healthcare’s legal and regulatory requirements.

We can see how this plays out in practice through one example regulation in the United States: HIPAA. The passing of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) led the U.S. Department of Health and Human Services (HHS) to establish the HIPAA Privacy Rule and the HIPAA Security Rule [11]. This was the first set of generally accepted standards for protecting health information in the healthcare industry.

HIPAA regulations apply to all U.S. healthcare providers, health plans and healthcare clearinghouses.

Protected health information includes the following [12]:

- Names
- Birth dates, death dates, treatment dates, admission dates and discharge dates
- Telephone numbers and other contact information
- Addresses
- Social Security numbers
- Medical record numbers
- Photographs
- Finger and voice prints
- Any other identifying numbers

Under the HIPAA privacy rule, patients have a number of rights, including:

- The right to receive notice of privacy practices of any healthcare provider, plan or clearing house.
- The right to see their protected health information and receive a copy.
- The right to request changes to their records to correct errors or add information.
- The right to have a list of those their protected healthcare information has been disclosed to.
- The right to request confidential communication.
- The right to complain.

These regulations offer significant protections for patients' health data, but its application does not extend to every party that comes into contact with personal health information. Entities required to follow HIPAA rules include obvious parties such as health plans or health insurance companies, most healthcare providers, and "business associates" of covered entities, including medical billing and medical records companies [11]. However, entities that are not required to comply with HIPAA include [11]:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

So, even regulations created with good intentions aren't protecting patients as well as they could. Our protocol, BitMED seeks to programmatically ensure privacy protections for all healthcare consumers everywhere, through the implementation of smart contracts and dApps.

The problem of scale

According to the CDC, in 2014 in the U.S. alone there were 884.7 million visits to a physician's office, or about 28 visits per second [13]. A blockchain built for global healthcare would have to support something on the order of 100,000 transactions per second. As of this writing, existing blockchains are not able to support applications with millions of users around the world [14].

Take the example of Hyperledger Fabric, an open source implementation of Hyperledger initially

contributed by Digital Asset and IBM with the goal of improving enterprise-level security [15]. Fabric is permissioned, with users and validators taking on specific roles in the system [16]. Nodes are differentiated based on whether they are clients, peers, or orderers [17]. A client acts on behalf of an end user and creates and thereby invokes transactions. They communicate with both peers and orderers. Peers maintain the ledger and receive ordered update messages from orderers for committing new transactions to the ledger. Endorsers are a special type of peer, as their task is to endorse a transaction by checking whether they fulfill necessary and sufficient conditions, such as the provision of required signatures. Orderers provide a communication channel to clients and peers over which messages containing transactions can be broadcasted. With respect to consensus in particular, the channels ensure that all connected peers are delivered exactly the same messages with exactly the same logical order.

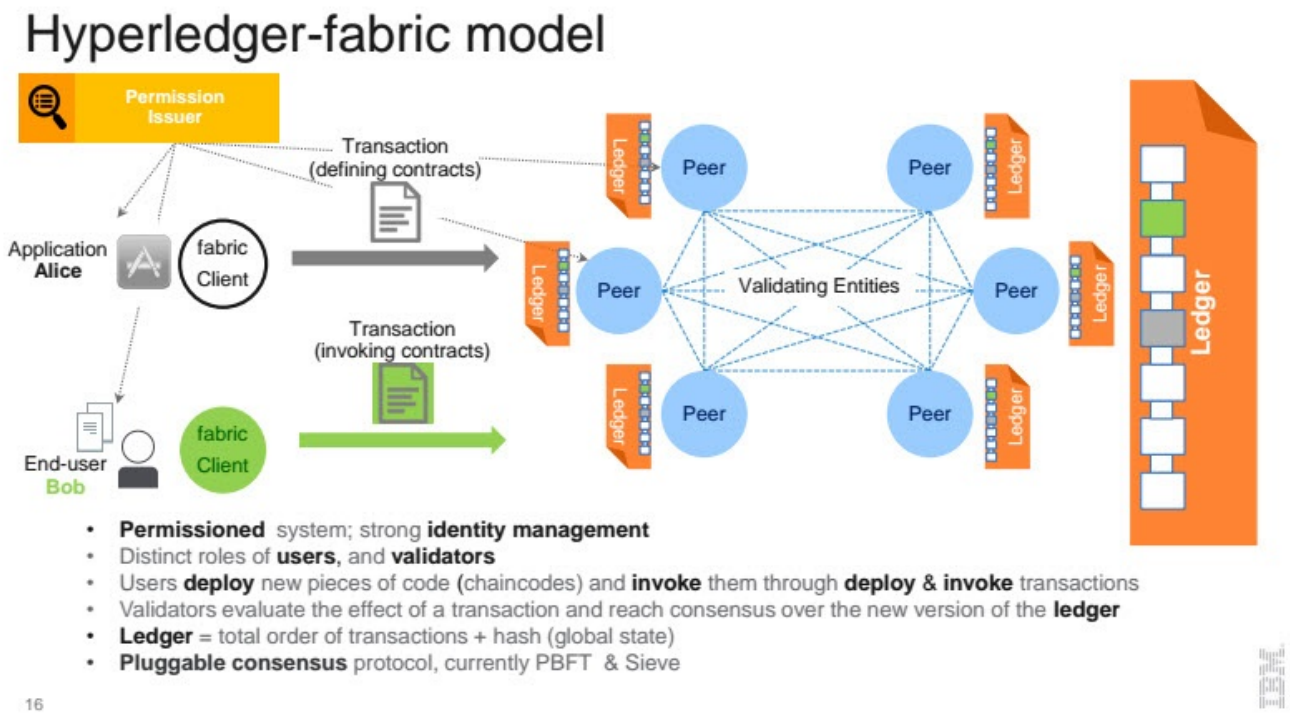

Figure 1. Hyperledger Fabric model.

At this point, when many mutually untrusting orderers are employed, the problem of message delivery errors arises. In order to reach consensus despite any faults that may arise (e.g. inconsistent ordering of messages), a consensus algorithm must be used to make the replication of the distributed ledger fault-tolerant. Fabric's algorithm is "pluggable," meaning that depending on application-specific requirements, various algorithms can be used to enable consensus and membership services [15]. For example, in order to deal with random or malicious replication faults, a variant of the Byzantine fault-tolerant algorithms could be used. Furthermore, channels partition message flows, meaning that clients only see the messages and associated transactions of the channels they are connected to and are unaware of other channels. This way, access to transactions is restricted to involved parties only, with the consequence that consensus has only to be reached at transaction level and not at ledger level as with Ethereum.

This implementation is optimal for many business cases. However, throughput currently maxes out at around 1,000 transactions per second [18].

3. Introducing the BitMED Health Protocol (BXP)

3.1 How it works

The BitMED Health Protocol is an open-source, distributed consensus ledger with a native currency, the BXM token. It supports smart contracts and dApps, or decentralized applications, and protects health data and personally identifiable information (PII). It is designed to prevent double-spending in the healthcare system and incentivizes health participation among patients. The system features the following components.

1. go-Ethereum

A base layer that uses the Go implementation of the Ethereum protocol (go-Ethereum) [19].

2. The BXM Protocol

- Transaction Manager—Allows access to encrypted transaction data for private transactions, manages local data store and communication with other Transaction Managers.
- Crypto Enclave—Responsible for private key management and encryption and decryption of private transaction data.
- Network Manager—Controls access to the network, enabling a permissioned network to be created.
- BXM Chain—Voting-based, Red Belly Blockchain (RBBC) consensus that utilizes core Ethereum features to verify and propagate votes through the network.
- Privacy Manager—Enforces governance, compliance, modeling, and risk to PII.
- Clinical Manager—Manages clinical workflows, observations, treatment, care provision, and medications.
- Specialized Manager—Supports clinical decisions, artificial intelligence, and reporting agents.
- Financial Manager—Access and authorization for claims, benefits, and payments.

3. The BXM token

The products and services on the BitMED platform are powered by the BXM token.

Membership
Members whose profile settings allow data contribution can earn tokens based on market demand. At any time, members can change their permission settings between data contribution and disallowing data contribution. Members can also earn tokens by contributing content and participating in communities.

Incentivizing member participation
A chicken-and-egg problem quickly emerges: a network needs people in order to be valuable, and people have no reason to join an empty, un-valuable network (i.e., Metcalfe's law). Over the last two years, through various partnerships, BitMED has gathered 22.5 million members awaiting onboarding and a

pipeline of 100M more. To accelerate onboarding and utilization and grow the ecosystem, we've designed our first round of incentivization token distribution to be the highest. For every year after our first year, it will decrease by half. By design, it will be more valuable for partner institutions to bring in members earlier rather than later. This is determined logarithmically.

Network and transaction fees
The BitMED network will follow Metcalfe's law, which states the value of the network is "proportional to the square of the number of its nodes, or end users," as the Bitcoin, Ethereum, and Dash networks have been found to follow [20, 21].

Energy required to process transactions must come from the community of users who gain from the ecosystem in which they participate. To cover the cost to run the ecosystem, a small floating base point fee (i.e. gas) is charged on every transaction across the ecosystem. Our objective is to incentivize validators to introduce more resources to the network as demand increases while providing the users of the network greater service.

4. BXM token mining

Blockchains such as Bitcoin and Ethereum operate on proof of work: solve a problem, compute the next block, get a reward. This method is open, participatory, and zero-trust. It is also computationally intensive, and at 3 to 20 transactions per second on average, does not currently scale to the needs of healthcare [22].

BitMED has instead opted for the proof of stake method. To increase throughput to the order of 100,000 transactions per second (that healthcare applications require), we introduce highly vetted validators or miners, designed to have a real stake in the game.

While the ledger is open source and public, only BitMED's vetted miners can validate the ledger. This works somewhat like a newswire that everyone in the system can see, but only certain parties are allowed to update. The validators are public and private institutions that must comply with healthcare requirements regarding confidentiality, integrity, and availability.

Certain costs are associated with becoming a validator, and so to incentivize good validators we plan to grant them a certain number of tokens at the outset. However, they haven't earned them, yet. Validators, by mining BXM tokens, can earn tokens per transaction. They can also work toward a much bigger bounty or pot for which several validators may be competing. However, if a validator is caught violating any requirement, they stand to lose not only the transaction but access to the larger bounty. Egregious actions constitute a loss of all earnings. Most importantly, validators take on the additional risk of violating laws in their country. For example, a validator in the U.S. who leaks a single health record would be at risk for civil penalties (i.e., $10,000 fine) and criminal penalties (i.e., up to 10 years in prison).

However, if validators complete the transaction according to requirements, they win the wager. Each successful wager adds up winnings and moves the validator closer to earning the pot. This method incentivizes miners to shepherd and validate the data correctly, with real stakes.

5. Decentralized applications, or dApps

At the outset, the BitMED ecosystem will include four main dApps: care, curated content, communities, and data.

Care
BitMED provides members real-time messaging with board certified medical providers. Members can chat through our messaging platform and can also make appointments for live video consultations. Members choose how they would like to access our health services: by contributing their data or tokens. There are no copays or fees when using BitMED's telehealth services.

Curated Content
Researchers at the Pew Research Center reported in 2013 that 72% of internet users had looked online for health information in the past year [23]. Unfortunately, Dr. Google did not go to medical school. BitMED matches medically verified content to our members' concerns and interests. Content is delivered directly to each member's personal profile for them to review, save, and share with their communities or doctor.

Communities
In BitMED communities, members can discuss common interests, share experiences, provide emotional support, and continuously learn how to cope with day-to-day health situations. Communities can be created with the transaction of an BXM token. Active participation in communities, including leading and moderating, will be rewarded with BXM tokens.

Data
The BitMED ecosystem incentivizes the transaction of data between all stakeholders. Data is aggregated, de-identified, and accessed based on conditions set by the contributor. Data can be used for patient care, health outcome reporting, research, clinical trials, algorithm development, actuarial analysis, and better understanding of consumer behaviors. When data is accessed, stakeholders use BXM tokens to access data for a defined period of time as defined in smart contracts.

Example token use

To illustrate an example use of tokens, let's assume some fictional institutions and actors:

- Acme, Inc. is a health system that has 25 million patient health records in paper form dating between 1990 and 2010. It costs $200,000 a year to maintain these records in storage.
- Star, Inc. is a health system that has 5 million patient records in mixed form between 2000 and 2017. It costs $50,000 a year to maintain paper and electronic records.
- A Johns Hopkins startup, Quanttus, Inc. needs 200,000 health records for patients who suffer an atrial fibrillation (AFib) or myocardial infarction (MI) and have an EKG in their charts at least 2 weeks prior. Quanttus has a breakthrough early warning Afib detection algorithm that is estimated to save 200,000 lives yearly once it clears the Food and Drug Administration.
- Safe, Inc. is a medical record storage company that is looking for new revenue stream as companies move to EHR.

Process
Safe offers to digitize all paper health records for 50 mBXM per sheet to all companies in the U.S., discount 40 mBXM for granting access to anonymized fields for 3 years, and pay 20 mBXM to each patient if they allow syncing to their current record. An example smart contract might be the following:

```
type contract = {
        uint public value;
        address public to;
        address public from;
        enum State { Created, Locked, Inactive }
        State public state;
        modifier condition(...){ /* rules of contract */ }
        function validatePatientContent(Address add){...}
        function computePayment(...) { /* payments to parties */}
        function storage(...) { /* data storage access, location, and conditions */)
    }
```

Figure 2. Sample smart contract for the BXP.

Star and Acme agree to have all paper based records digitized by Safe. Furthermore, Star informs all of its patients that they now have universal access to their own electronic health records via the BitMED ecosystem. Members maintain full control of their own health records and can be compensated for granting access to them if they so choose.

Quanttus places a new contract seeking 200,000 charts with AFib or MI on the BitMED ecosystem. Quanttus is offering to pay 2 BXM per record that matches their conditions. Without the BitMED ecosystem, it would have taken Quanttus as long as 2 years to accumulate the necessary records, with total costs exceeding $10 million, not to mention the lives lost while this data is gathered.

Star can fulfill requests for 150,000 records, but knows that Dawn, Inc., a health system company, has 10 million records in which it estimates the remaining 50,000 records can be found. However, Dawn has everything in paper form and legacy systems to address. Star sends a proposal to Dawn to digitize all their records at no upfront cost, but requires access to anonymized fields from these records for 5 years. Dawn agrees to these terms, under the condition that Star helps with modernization and moves all members to the BitMED ecosystem for all future records. With these additional records, Dawn now has the 200,000 records that fulfill Quanttus' contract.

3.2 Borrowing what works, building what's missing

BitMED does not aim to reinvent the wheel. The BXP incorporates components from existing

technologies, and connects and adds components as needed to meet the unique legal and regulatory challenges of a global healthcare market.

Hyperledger/Quorum Fork

The BitMED blockchain is based on Hyperledger, Quorum, and IPFS technology, which addresses the challenges of a permissionless ledger, scale, and storage, while supporting both transaction-level privacy and network-wide transparency, as well as allowing for customization to business requirements.

- All public and private smart contracts and overall system state are derived from a single, shared, complete blockchain of transactions validated by every node in the global network.
- The private smart contract state is known to and validated by only parties to the contract and approved third parties, like regulators.
- Smart contracts written for an existing Ethereum implementation remain network-transparent on BXM out of the box.
- Enhancing many existing smart contract designs to meet different sets of privacy requirements is simple and straightforward.

By implementing a permissioned distributed ledger of up to 200 trusted nodes, we lower the transaction cost, maintain thousands of transactions per second, comply with PII standards governing confidentiality, integrity, and availability, and provide a path forward for existing health standards and protocols.

While Hyperledger does offer enterprise-level security, HIPAA and other location-specific health data laws require extra measures. The key divergence from Hyperledger in the BXP is that HIPAA-covered data fields are not replicated on the entire block. Instead, we leverage IPFS' IPLD mechanism that states where the information is found. Records are anonymized in real-time, and only the node for the country where the patient resides will host the HIPAA fields. In essence, this is vertical partitioning specific to the HIPAA fields, with shard key.

The Red Belly Blockchain (RBBC) algorithm

The BXP leverages the work of Crain, Gramoli, Larrea, and Raynal on the Red Belly Blockchain (RBBC) and binary Byzantine consensus (BBC) algorithm [24]. Their algorithm is designed to comply with an extended definition of the consensus validity property, and is structured with two components:

1. A reduction of multivalued consensus to binary consensus. The reduction is fully asynchronous and "uses neither randomization, nor an eventual leader, nor signatures" [19]. It "always decides a non-predetermined value in $O(1)$ sequence of binary consensus. The reduction only waits for the earliest terminating of the concurrent reliable broadcast instances before spawning binary consensus instances. As it assumes $t < n/3$, where n is the number of processes and t is an upper bound on the number of faulty processes, this reduction is resilience optimal" [24].
2. A binary Byzantine consensus (BBC) algorithm. It also requires neither randomization, nor an eventual leader, nor signatures [24]. Computationally, it always terminates except in cases where transfer delays are always increasing. The BBC "always terminates in time $O(1)$ if all non-faulty

processes propose the same value, otherwise it may still terminate in constant time but is guaranteed to terminate in $O(t)$ time, which is optimal" [24].

The result is not only resilience optimal ($t < n/3$) but time optimal as well, as it terminates in $O(t)$ [19].

3.3 Benefits

The BXP is designed for two main goals: 1) to meet the current needs of healthcare and 2) to create the foundation for a secure, open ecosystem upon which future opportunities for cost savings and innovations in care delivery can be built.

Increases access to care

Existing companies no longer need to build their own healthcare practices. Vetted healthcare companies can leverage the Care dApp and BitMED medical providers, or build their own dApp and services, to accomplish such goals as lowering readmissions rates or interpreting medical data or results.

Increases access to accurate health information

BitMED provides a central location for personally relevant, medically validated health information or content, accessible to everyone. Content creators and supporting staff, such as editors and translators, can be compensated for their work.

Enforces compliance while reducing its cost

The BXP leverages compliance protocols, dApps from other vetted health entities within the ecosystem, without having to address the typical time and expense of audit, compliance, and onboarding. The protocol will enforce compliance and prevent usage that would expose anyone to regulation violations.

The cost of HIPAA compliance varies depending on the size and requirements of a given institution or practice, but can be anywhere from a few thousand dollars to $50,000 or more [25]. The cost of a violation is much more expensive than compliance, but it is a cost nonetheless, not only in dollars but in impeded health research [26]. Everyone can share in the cost savings when compliance is enforced in the protocol itself.

Lowers transaction costs and reduces fraud

The ecosystem reduces costs by eliminating time-consuming manual processes (e.g. reconciliation between multiple isolated ledgers, administrative processes, etc.). It also reduces fraud by time-stamping entries and sharing a common, immutable ledger across the network. This prevents the common problem of double-spending in healthcare systems.

Securely stores healthcare data and protects personally identifiable information (PII)

The BXP is an open source, permissioned network that enables all patients, providers, and public and private entities to store their healthcare data. Entities can rest assured that the data is safe and secure without taking on the capital and compliance cost to build their own data security solutions. The BXP leverages the following existing health IT and security standards:

- FHIR
- Health Level 7
- ISO 27001
- HITRUST
- FISMA
- Privacy Shield

Although necessary, these standards quickly become outdated, and represent only a snap shot of existing known threats at the time they were created. The BXP protocol enables the best security practices to continue adapting to threats to the ecosystem daily, while also enabling everyone on the network to take advantage of this work.

Scales to the needs of healthcare

As mentioned in Section 3.2, the BXP scales to the needs of healthcare by implementing the Red Belly Blockchain (RBBC), a multivalued Byzantine consensus model proven to achieve "660,000 transactions per second on 300 machines in a single data center" [27]. We are leveraging the work of Crain, Gramoli, Larrea, and Raynal [24] that enables hundreds of thousands of transactions per second. By comparison, Visa's network is capable of processing 56,000 transactions per second [22].

The RBBC algorithm is ideally suited for the BXP and other consortium blockchains, where consensus is neither fully private nor fully public, but performed by vetted validators. It achieves such high throughput because it "decides a non-predefined value in a sequence of $O(1)$ binary consensus instances" [24]. It does this by combining "a reduction from multivalued to binary consensus that applies a bitmask to an array of proposals and a binary consensus to build this bitmask," therefore spawning binary consensus instances in parallel [24].

Incentivizes data sharing

Healthcare systems in the U.S. developed at a time when people knew their doctors and kept the same doctor for a long period of time. Today, providers come and go, and the patient herself is the only constant in a lifetime of interaction with health systems. Now more than ever, it's essential that each person remain in control of their own health data.

The BitMED ecosystem not only enables this degree of control over personal health data, it also enables each person to make money off of their own data. If members want to grant access to family or third-party companies, they can. Third parties might even envision better applications and services for certain populations.

A common saying that has aptly evolved along with media from the 1970s to the present goes, “If you’re not paying for it, you’re not the customer, you’re the product being sold.” Facebook is one example of this—though the company uses your data to make money with advertisers, they’re not paying you any portion of that profit. BitMED envisions a system in which each person whose data is deemed valuable has the option to profit off of it.

An important distinction here is that while services received via the BitMED ecosystem don’t require local currency, every consultation between providers and members require BXM tokens. Members can then message in real time with U.S. board certified medical doctors, chat through the messaging platform, or make appointments for live video consultations.

4. Conclusion

The BitMED protocol and ecosystem enables access to care, content, and community for all members. It also enables incentivized, secure, and reliable collaboration of data between patients, providers, researchers, industry partners, and other stakeholders in the health delivery process. This means a shift from engaging in health only when sick, to health maintenance, to the ultimate goal of health personalization and optimization.

Currently, BitMED is onboarding 22.5 million global members through our existing channel partners. Our goal is to increase the pre-signup reach to 100M by the end of 2018, we will ramp up access to BitMED's platform in mid 2018. In our next phase of development, BitMED intends to rebuild all existing products and services on BitMED ecosystem for scale, as well as build new products and services. We are excited for members of the cryptocurrency community to join us.

We have developed smart contracts for data research and releasing the BitMED blockchain source code and BXM token, which is available by this address: 0x2b7a6374fbf06c080c36ff43fa99f9d6f09019ab. BitMED is a work in progress, and we will keep the community updated with our findings as they occur. [17]

References

[1] M. T.E. Sullivan, "Administrative Simplification in the Physician Practice," [Online]. Available: https://www.ama-assn.org/sites/default/files/media-browser/public/about-ama/councils/Council%20Reports/council-on-medical-service/i11-cms-administrative-simplification-physician-practice.pdf. [Accessed 2017].

[2] The Harris Poll, "Oil, Pharmaceutical, Health Insurance, Tobacco, Banking and Utilities Top The List Of Industries That People Would Like To See More Regulated," 21 December 2012. [Online]. Available: http://www.theharrispoll.com/politics/Oil__Pharmaceutical__Health_Insurance__Tobacco__Banking_and_Utilities_Top_The_List_Of_Industries_That_People_Would_Like_To_See_More_Regulated.html.

[3] R. Xu, "The Health Care Industry's Relationship Problems," 28 October 2015. [Online]. Available: https://www.newyorker.com/business/currency/the-health-care-industrys-relationship-problems.

[4] L. Bernstein, "U.S. Faces 90,000 Doctor Shortage by 2025, Medical School Association Warns," 3 March 2015. [Online]. Available: https://www.washingtonpost.com/news/to-your-health/wp/2015/03/03/u-s-faces-90000-doctor-shortage-by-2025-medical-school-association-warns/.

[5] S. Morse, "Prior authorization needs streamlining, new healthcare coalition including AMA, MGMA says," 25 January 2017. [Online]. Available: http://www.healthcarefinancenews.com/news/prior-authorization-needs-streamlining-new-healthcare-coalition-including-ama-mgma-says.

[6] The Advisory Board, "CMS: US health care spending to reach nearly 20% of GDP by 2025," 16 February 2017. [Online]. Available: https://www.advisory.com/daily-briefing/2017/02/16/spending-growth.

[7] World Health Organization, "Health systems financing: the path to universal coverage," 2010. [Online]. Available: http://www.who.int/whr/2010/en/.

[8] Office for Civil Rights, U.S. Department of Health and Human Services, "HIPAA for Individuals," 17 June 2017. [Online]. Available: https://www.hhs.gov/hipaa/for-individuals/index.html.

[9] Team EU-PATIENTEN.DE, "How are my medical data protected in Germany?," 1 September 2017. [Online]. Available: http://www.eu-patienten.de/en/behandlung_deutschland/datenschutz/datenschutz.jsp.

[10] Office of the Privacy Commissioner of Canada, "The Personal Information Protection and Electronic Documents Act (PIPEDA)," 9 September 2016. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[11] U.S. Department of Health and Human Services, "Your Rights Under HIPAA," 1 February 2017. [Online]. Available: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

■

[12] ASC Communications, "50 things to know about healthcare data security & privacy," ASC Communications, 9 June 2015. [Online]. Available: https://www.beckershospitalreview.com/healthcare-information-technology/50-things-to-know-about-healthcare-data-security-privacy.html.

[13] H. E. O. T. Rui P., "National Ambulatory Medical Care Survey: 2014 State and National Summary Tables," 3 May 2017. [Online]. Available: https://www.cdc.gov/nchs/data/ahcd/namcs_summary/2014_namcs_web_tables.pdf.

[14] F. Ehrsam, "Scaling Ethereum to Billions of Users," 27 June 2017. [Online]. Available: https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1.

[15] The Linux Foundation, "Hyperledger Fabric," [Online]. Available: https://hyperledger.org/projects/fabric.

[16] R. Strukhoff, "How Hyperledger Fabric Delivers Security to Enterprise Blockchain," 14 November 2016. [Online]. Available: https://www.altoros.com/blog/how-hyperledger-fabric-delivers-security-to-enterprise-blockchain/.

[17] Hyperledger, "Architecture Explained," 26 July 2017. [Online]. Available: hyperledger-fabric.readthedocs.io/en/latest/arch-deep-dive.html.

[18] C. Gutierrez, "Hyperledger's Sawtooth Lake Aims at a Thousand Transactions per Second," 13 March 2017. [Online]. Available: https://www.altoros.com/blog/hyperledgers-sawtooth-lake-aims-at-a-thousand-transactions-per-second/.

[19] The go-ethereum Authors , "Go Ethereum Homepage," [Online]. Available: https://ethereum.github.io/go-ethereum/. [Accessed 2017].

[20] K. Alabi, "Digital blockchain networks appear to be following Metcalfe's Law," *Electronic Commerce Research and Applications,* vol. 24, pp. 23-29, July-August 2017.

[21] H. R. V. Carl Shapiro, Information Rules, Boston: Harvard Business Press, 1999, p. 184.

[22] J. Vermeulen, "Bitcoin and Ethereum vs Visa and PayPal – Transactions per second," 22 April 2017. [Online]. Available: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html.

[23] M. D. Susannah Fox, "Health Online 2013," 15 January 2013. [Online]. Available: http://www.pewinternet.org/2013/01/15/health-online-2013/.

[24] V. G. M. L. M. R. Tyler Crain, "(Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains," 2017.

[25] T. Ferran, "How Much Does HIPAA Compliance Cost?," 6 April 2015. [Online]. Available: http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html.

[26] The National Academy of Sciences, "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research," 4 February 2009. [Online]. Available: http://nationalacademies.org/hmd/reports/2009/beyond-the-hipaa-privacy-rule-enhancing-privacy-improving-health-through-research.aspx.

[27] J. Peterson-Ward, "University of Sydney's super-fast blockchain gets even faster," 25 October 2017. [Online]. Available: https://sydney.edu.au/news-opinion/news/2017/10/25/university-of-sydneys-super-fast-blockchain-gets-even-faster.html.

[28] R. Guerraoui, "Indulgent Algorithms," in *Proceedings of the nineteenth annual ACM symposium*

■

on Principles of distributed computing, New York, 2000.

[29] C. N. a. V. Gramoli, "The blockchain anomaly," in *Proc. 5th IEEE Int'l Symposium on Network Computing and Applications (NCA'16)*, 2016.

[30] Ethereum, "Solidity," 2016-2017. [Online]. Available: https://solidity.readthedocs.io/en/develop/.

[31] Protocol Labs, "IPLD Homepage," [Online]. Available: https://ipld.io/. [Accessed 2017].

■