BitClaims: Pre-Payment Adjudication for Healthcare Claims Network v1.1

David Alexander,
James C. Henry,
Michael J. Tabacco, JD, Esq.

February 2018

Abstract

This whitepaper describes a blockchain-based (i.e. decentralized, peer-to-peer) smart contract-enabled platform for pre-payment adjudication of healthcare claims. BitClaims uses a consensus protocol between payers, billers, coders and providers while a validation ledger on a blockchain 1) Checks providers for medicare and medicaid authorization 2) ensures compliance with billing claims metrics; and 3) prevent payments for services billed by excluded providers. This network provides value for payers (health insurance companies such as Blue Cross Blue Shield and subsequent affiliates) seeking to prevent reimbursement to a provider for unjustified services and preclude the allocation of resources to cost recoupment actions via various auditing entities. The BitClaims infrastructure is designed with the goals of interoperability, compatibility, and integration into current legacy systems – both decentralized and legacy systems. BitClaims network seeks to both eliminate administrative inefficiencies related to currently-implemented physician compliance programs and increase value savings to health insurers by reducing the need for recoupment actions. BitClaims network has far-reaching potential to promote the development of healthcare compliance as to: **establish a self auditing claim**.

CURRENT STATE OF U.S. HEALTHCARE

HEALTH INSURANCE

The election of Donald J. Trump has ushered in a new era for the U.S. healthcare industry, which has spent years adapting to the Affordable Care Act. A majority of consumers have concerns about the affordability of healthcare products and services. Indeed, consumers place a high priority on the cost of their care, insurance and prescription drugs.

In spite of the potential policy changes in Washington (and the effects thereof throughout the country), the work of shifting to value-based care has become all the more crucial. Various reports regarding the health insurance industry have highlighted the forces expected to have the most impact on the healthcare industry this year, in 2018, and beyond.

Many of the top issues health insurance companies are adapting to face how a shift toward value is occurring, and how traditional health organizations and new entrants are responding to it. Some of the primary tactics health insurance organizations are using to address this shift to value are adapting to emerging technology and building new programs and approaches to their work.

U.S. HEALTH INSURANCE TO EMBRACE EMERGING TECHNOLOGIES

The U.S. health industry lags behind other industries, such as retail and telecommunications, in deploying emerging technologies, including digital records, online portals, cloud based data solutions, and, now, blockchain. The upcoming years will mark the arrival and the eventual adoption of these technologies, and we're beginning to see their impacts on business models, operations, workforce needs and cybersecurity risks.

Emerging technologies are beginning to remake business operations and become integral parts of consumers' lives. As these technologies make their way into the health industry, organizations will need to hire new talent or to partner with enterprises stocked with these skills. The 3 Trillion dollar U.S. healthcare ecosystem is set for disruption at the hands of these emerging technologies.

Compliance is in the interest of physicians and health insurers

It is no secret that the government is becoming increasingly aggressive in its enforcement against health care providers. At the same time, regulations are becoming more complicated. The combination of these two forces means that many unknowing providers are being caught up in costly investigations of their practices. The government is taking a “return on investment” approach to health care fraud and is seeing a good return on every dollar that they put into the

efforts. As a result, we cannot expect fraud enforcement to decrease any time soon.
For this reason, it is important that providers, including medical practices, develop and operate systems to help them comply with governmental regulations and third party payer billing requirements (Medicare, Medicaid, and/or private insurance).

At the same time, health insurers have a significant stake when it comes to the compliance of their physician/provider members. The insurers do not want to overpay for services billed to them by providers, nor do they wish to expend resources on various auditors who conduct expensive recoupment actions due to inadvertent billing mistakes or fraud. The insurance companies have a vested interest in the member providers' compliance. In fact, **a high rate of compliance can prove very helpful in substantiating claims billed to the health insurer**. (see AMA and American Academy of Neurology Re: Preparation for a Health Insurer's Retrospective Audit).

Providers
Claims
Government
Health Plans

The development of a formalized compliance program has become an indispensable part of risk management. Failure to maintain compliance can lead to an increase in reimbursement disputes, increased uncollectible fees, more demands for repayment, civil litigation and in extreme cases, potential criminal prosecution.

Matters to be addressed in compliance programs include not only billing practices but also anti-kickback compliance, state and federal self-referral prohibitions, state fee-splitting laws, licensure and accreditation requirements, labor relations matters, antitrust and price fixing prohibitions, HIPAA and medical records issues and a whole host of other state and federal laws.

Formalized compliance programs first began appearing in the late 1990s as a way to minimize risk in primarily large institutions. Compliance programs are a child of the Federal Sentencing Guidelines which factors in the adoption of 7 pillars of an effective compliance program when a healthcare organization is facing potential institutional criminal penalties for legal violations.

Formal compliance programs were more deeply woven into the fabric of many organizations as the Medicare Office of Inspector General began releasing compliance guidance directed toward specific segments of the healthcare industry in the late 1990s and continuing through the mid 2000s.

FORMAL COMPLIANCE HAS BECOME INDUSTRY "BEST PRACTICES" AND WITH THE PASSAGE OF THE PATIENT PROTECTION AND AFFORDABLE CARE ACT OF 2010, PHYSICIANS WHO TREAT MEDICARE AND MEDICAID BENEFICIARIES WILL BE REQUIRED TO ESTABLISH A COMPLIANCE PROGRAM

Even though compliance programs were not traditionally been mandatory, they now are. Indeed, they have become "industry standard" as a way to minimize risks associated with healthcare regulations such as the Health Insurance Portability and Accountability Act of 1996, the Medicare and Medicaid Fraud and Abuse Laws, Anti-kickback Statute, Civil Monetary Laws, False Claims Act, the Clinical Laboratory Improvement Act and all other state and federal statutes, regulations and directives that apply to the operation of a physician's practice.

Section 6401 of the Patient Protection and Affordable Care Act of 2010, as amended by the Health Care Education Reconciliation Act of 2010 (the "Affordable Care Act") requires HHS and the Office of Inspector General to promulgate regulations that require most healthcare providers and suppliers to establish compliance programs. The compliance programs are intended to be "effective in preventing and detecting criminal, civil, and administrative violations" under the Medicare and Medicaid laws and other laws that govern operations.

Under the Affordable Care Act, physicians and group practices, along with other relatively small providers, are required to establish compliance programs as a condition of enrollment in the Medicare program. Early versions of the Affordable Care Act included an exception for physicians which was deleted from the version of the Act that was signed into law. We know that the mandatory compliance program requirement will apply to physician practices absent further legislative action.

BASIC ELEMENTS OF AN EFFECTIVE COMPLIANCE PROGRAM

Developing a compliance program that will be effective to reduce internal and external risk is a "practice specific activity." There is no "one size fits all" compliance program and there is no good "off the shelf" form solution. There are certainly vendors, consultants and lawyers out there who would like you to believe that you can take a form, make a few changes and fill in a few blanks, and create an effective compliance program for your organization. This approach really misses the point of what is required in order to develop and effective program.

There are generally seven basic core elements that are required of an effective compliance program including:

1. Adoption of written guidelines and policies to promote the organization’s commitment to compliance;

2. Identification and appointment of a high ranking individual within the organization to serve as compliance officer;

3. Establishment of anonymous reporting systems, preferably through multiple pathways, to encourage individuals to make complaints regarding compliance items without fear of retaliation;

4. Effective education and training programs for all levels of employees and others with close relationships to the organization;

5. Ongoing auditing systems to assess the effectiveness of the compliance program and to provide input into areas that require additional emphasis;

6. Mechanisms to enforce the requirements of the compliance program and to discipline employees for violations of the organization’s commitment to compliance; and

7. An ongoing system of program modification based upon audit, feedback and experience that can further adapt the compliance policies to the specific issues faced by the organization.

A compliance program should be developed with consideration for the actual risks that are present in the specific practice.

SOME PHYSICIANS, HOWEVER, HAVE REPORTED DIFFICULTY IN EFFECTIVELY IMPLEMENTING AND/OR ADHERING TO VARIOUS ASPECTS OF THEIR COMPLIANCE PROGRAMS. Likewise, Insurance companies catching such compliance failures after the fact, has resulted in payment of claims which should not have been paid and/or initiation of expensive recoupment actions via auditors.

Traditionally implemented compliance programs have been reported to ‘miss’ or fail in some or all of the following respects:

> Validating bills for services and ensuring proper clinical coding;
>
> Adhering to encryption requirements to ensure compliance with security measures and breach notification when there is a wrongful disclosure of PHI (Protected Health Information);

Payments made for services ordered or referred by excluded physicians, physicians without valid NPI, DEA number, appropriate state licensure, and/or billing privileges;

Difficulty quickly validating and verifying that the situs (place of service) from which the service(s) was billed is accurately reflected within the bill for services;

Failure of employees to report violations (even anonymously by hotline or other traditional anonymous means) due to fears of retaliation;

Upper management detecting and responding promptly to offenses and undertaking corrective actions;

Routine training of employees and ensuring consistent attendance; and

Ensuring required forms are up to date with the most recent regulations, guidance, LCDs and NCDs.

Above are just a few examples. Some of the difficulties with these examples arise from: non-existent or poor verification processes; lack of appropriately prompt response times; lack of self-validating measures; and use of traditional or legacy systems, which do not have efficiently organized ledger and consensus capabilities.

A BLOCKCHAIN TECHNOLOGY TO ADDRESS FREQUENTLY ENCOUNTERED COMPLIANCE ISSUES. Use case for health insurers and physicians.

1.Validating Provider Bills for Services

Overbilling insurance, specifically double billing for medical services, is a problem which costs Medicare and private insurance vast sums in recoupment actions every year. Even with compliance plans in place, providers have continued to experience issues with overbilling and double billing.

Double billing occurs when the physician bills for the same item or service more than once or when another party bills the Federal health care program for an item or service also billed by the physician or when two providers attempt to get paid for the same procedure rendered to the same patient on the same date. Although duplicate billing can occur due to simple error, the knowing submission of duplicate claims--which is sometimes evidenced by systematic or repeated double billing--can create liability under criminal, civil, and/or administrative law.

One of the key problems blockchain consensus, validation and ledger technology solves is the problem of double spending. If a chunk of value is sent one place, there needs to be an internal check that prevents that value from being sent again. Something about the first payment must preclude the second from initiating.

BitClaims seeks to create a ledger that ensures when a bill for services is submitted, a second bill does not get resubmitted for a second payment and result in double payment for the same procedure rendered to the same patient on the same date.

2. Prevention of Payments for Services Billed by Excluded Provider

Remitting payments to providers who do not have valid billing privileges is an issue faced by many health insurance companies. Insurance is forced to expend vast sums in recoupment costs to recover improper payments to providers after the fact.

Federal programs and certain private payers are prohibited from paying for any items or services furnished, ordered, or prescribed by an excluded provider. Additionally, managed care plans and their network providers may not employ or contract with an excluded individual to provide items or services paid for.by Medicaid. Nationally, approximately 70 percent of Medicaid beneficiaries receive some or all of their Medicaid services through managed care. Furthermore, it is a violation of law when providers submit bills for services provided if they do not have valid insurance billing privileges, good standing state licensure, an expired DEA number, and/or lack of an NPI (National Practitioner Identification) number. Insurance payers have a vested interest in preemptively preventing reimbursement to such providers.

BitClaims platform seeks to create a ledger which runs checks with various databases and verify that provider's' billing privileges and requisite identifications are in good standing before remitting reimbursement payments.

Enter BitClaims - A Blockchain Platform Leveraging Time Series and Open Source Utilities

A transportable blockchain across GP’s and Insurance company eco-systems. The BitClaims blockchain, containing contextually based smart contract and ancillary child tree chains are purpose built for the GP - Insurer primary use cases.

BitClaim: The Proof of Process Healthcare Platform

A healthcare communications platform that enables the verification of the processes associated with compliance and billing in the healthcare industry. Through validated best practices in IT and the use of Smart Contracts and Blockchain technology, BitClaims seeks to streamline compliance verification by a permissioned public/private blockchain thus expediting billing remittance payments associated with claims:

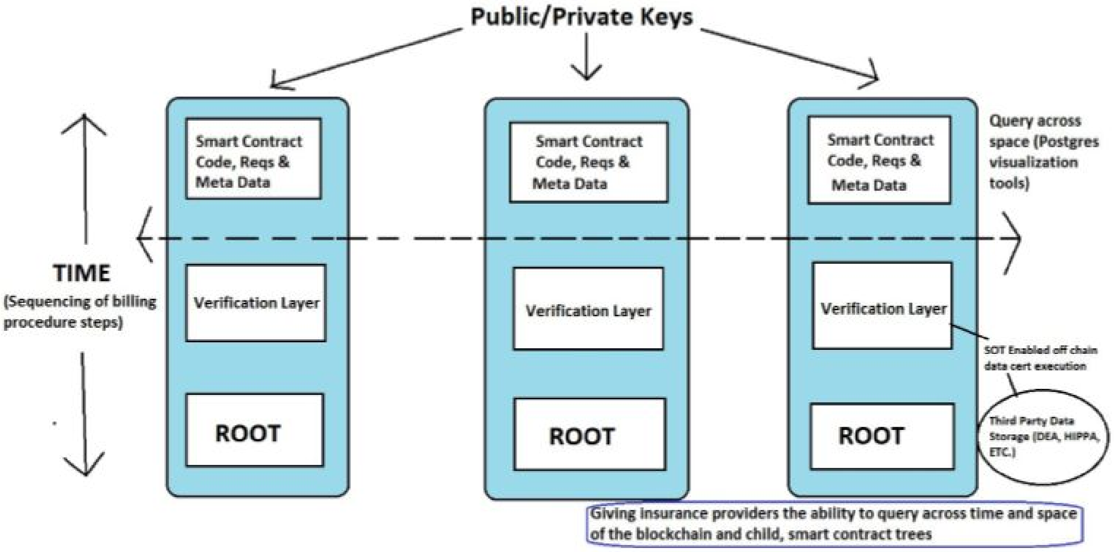
- Establishing Smart Contract layers on the BitClaims blockchain platform, sequencing steps
- View only cryptographically hashed block header metatags
- Validated network participants facilitating and verifying party transactions on sub smart contract chains via root chain
- Contextual, procedure only smart contracts mapped to Medicare and best practice claims billing procedure standards
- Auto populate metadata tags via BitClaims AI

Our mission is to simplify billing and compliance in the healthcare industry.

The intent of the BitClaims Ecosystem is to automate the the signal of transfer (SOT) of certain procedural based billing transactions between subsets of primary healthcare providers and insurance companies. This is strictly a communications layer and does not actually hold nor store any patient data. This PHASE ONE approach ensures that the integrity of patient data is kept to the highest regulatory standards and automates the archaic, oftentimes cumbersome task of communication between GP's and insurance companies.

This is accomplished through anchoring nodes to GP's and insurance companies computers that run a specialized VM to which billing procedure claims information can run through securely and efficiently.

TIMES SERIES APPROACH TO BLOCKCHAIN VIRTUAL MACHINE PROTOCOLS


Public/Private Keys
Smart Contract Code, Reqs & Meta Data
Smart Contract Code, Reqs & Meta Data
Smart Contract Code, Reqs & Meta Data
Query across space (Postgres visualization tools)
TIME
(Sequencing of billing procedure steps)
Verification Layer
Verification Layer
Verification Layer
SOT Enabled off chain data cert execution
ROOT
ROOT
ROOT
Third Party Data Storage (DEA, HIPPA, ETC.)
Giving insurance providers the ability to query across time and space of the blockchain and child, smart contract trees

Time Series Principle Utility

Time Series workflows offer a new angle of approach to blockchain architecture. For starters, time series data is largely immutable, correlating directly to the core tenants of an unalterable ledger (blockchain). New data writes occur independently and not as updates to existing rows. As new data arrives, it is correlated to existing time periods that data has been written to. Writes therefore are made primarily to recent time intervals. In a Time Series environment, data points that are written to the database are done so to the latest time activity and the data sources (smart contract metadata tags, smart contract protocols, SOT requests from cloud data stores). With this in mind, data queries are not constrained to one metric, and can instead select multiple metrics at the same time, or functions that call upon multiple metrics.

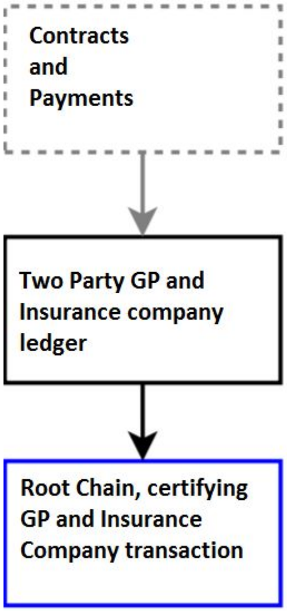
This methodology maps directly with the practices and processes involved around the sequencing of billing from the standpoint of insurance companies and GP's, in addition to several other use cases which BitClaims is aggregating for PHASE TWO implementations. Additionally, it allows maximum scalability and robust query support for the highest level of integrity demanded by resource heavy users.

The primary care provider (GP), who must be regulatory compliant, runs a node which has the protocols of our VM. This takes the form of a core blockchain being the unalterable ledger. The consensus model between partner machines and insurance companies authorizing the transaction fundamentally occurs here. The VM is a series of protocols that run on the primary care providers machine which translates into the nodes of any distributed, decentralized computing network.

On top of the blockchain runs a series of child chains, formulated to store only pertinent data between parties of transaction on that chain. This includes the smart contract layer, via the protocols already established in the VM. These smart contracts, through a series of proprietary enablers only known to BitClaims running on the VM, allow for the smart contracts between the GP and insurance companies. Utilizing this methodology, BitClaims does not touch or hold any patient data whatsoever. It merely is a secure healthcare communications platform for smart contracts that enable the transfer of transaction compliance metrics to occur. Furthermore, since the VM nodes are only executed on partner machines, there is an added layer of trusted consensus since only authenticated, validated and vetted providers are part of the trusted node network.

When a GP and an insurance company begin the process of enabling a smart contract transfer, with pre-set criteria being met, the insurance company authorizes the use of the BitClaims token to then enable the transaction between the two, with the compliance validation being paid by the caller funds for procedure billing from the insurance company. This token exchange occurs via the two, who may or may not both be needing to run trusted nodes on the network.

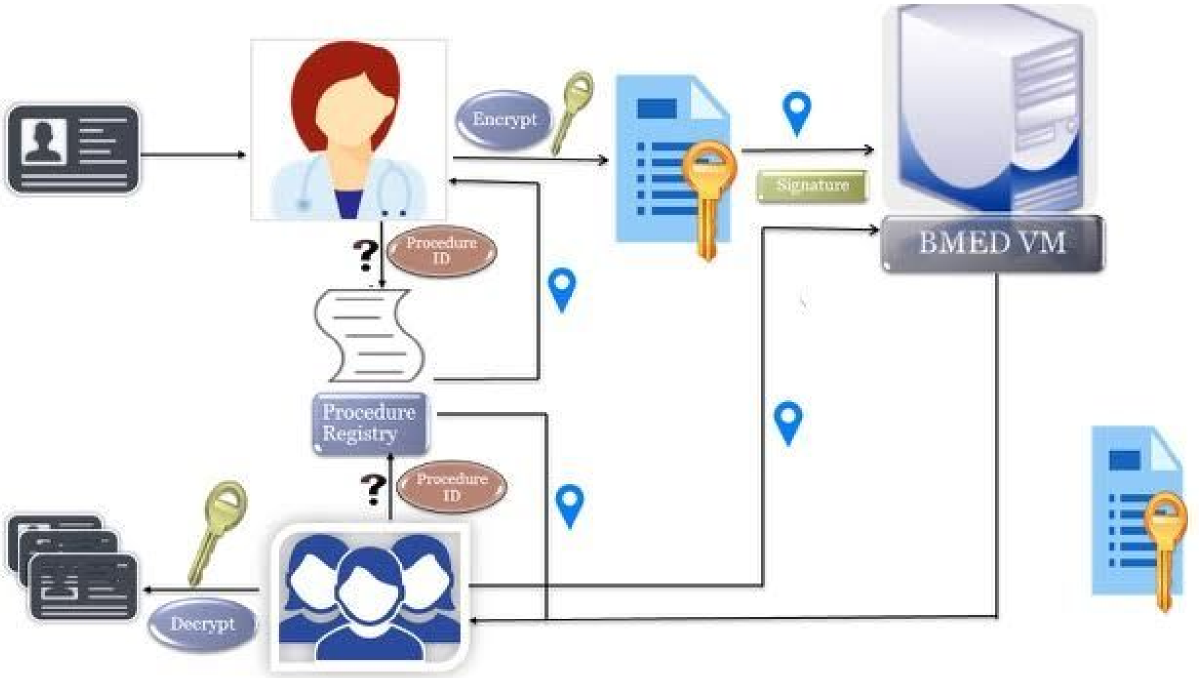
In order for the funds of a procedure to be released to the General Practitioner (GP), the GP and the insurance provider enter into a smart contract agreement.


Contracts and Payments
Two Party GP and Insurance company ledger
Root Chain, certifying GP and Insurance Company transaction

Process

Primary care providers who are running the BitClaims Node (BCVM) can interact with each other to pay for signal of transfer requests. Inherently each node is run on a separate ‘machine’, at the primary care providers facility, that interacts with an API. Think of the BCVM as a docker like container, with a compiler esque blockchain enabled by meeting the criteria of smart contract conditions. The outcome that BitClaims platform is continuously driving towards is a self policing, self auditing healthcare claims rail that is easily queried to meet the needs of GP’s and insurers.

Once running, the BCVM integrates with the API of the GP and insurance companies portal. The BCVM by design cannot store, nor read the patient data in que to be transferred. To alleviate this issue, BitClaims uses several cryptographic hashing layers and a blend of public private keys, generated on a per account, per transaction and per procedure to claim basis. While seemingly complex on the surface, following these protocols and procedures insures the highest integrity for GP’s and subsequent billing insurers business.

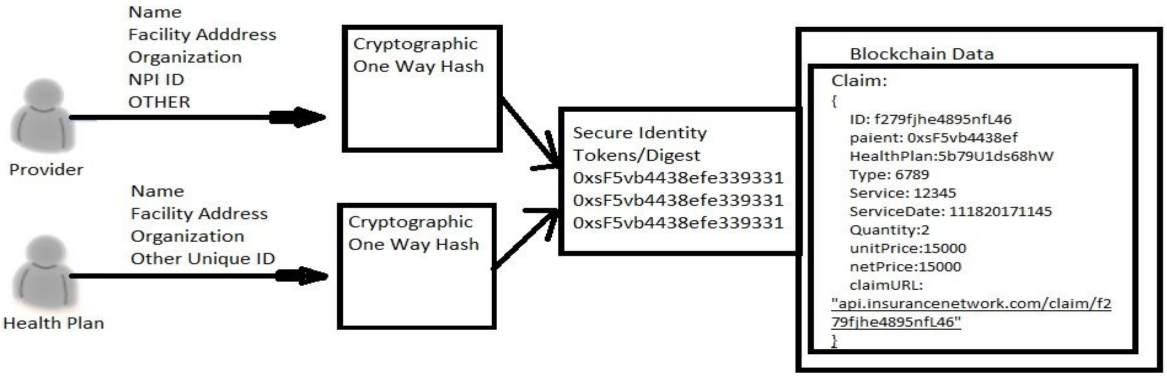


BitClaims Primary care providers can request the already validated cryptographic hash headers of a validated transaction on the blockchain. This occurs off chain and using public/private keys. The decentralized consensus via the blockchain protocols enables the request to happen being accepted or denied based on the network consensus. Upon consensus by the nodes on the blockchain, the transaction hits the root chain ledger.

The BitClaims Process consists of three main elements:

(1) A grouping of contextually based smart contracts via specific procedure numbers tied to claims established by Medicare, industry or otherwise.
(2) The R.A.N.S. mechanism that rakes a percentage of daily revenue into a BCH custodial wallet which then sweeps to receipt holders.
(3) A front end portal that allows the eco-system to interact with the GP's and insurance companies directly

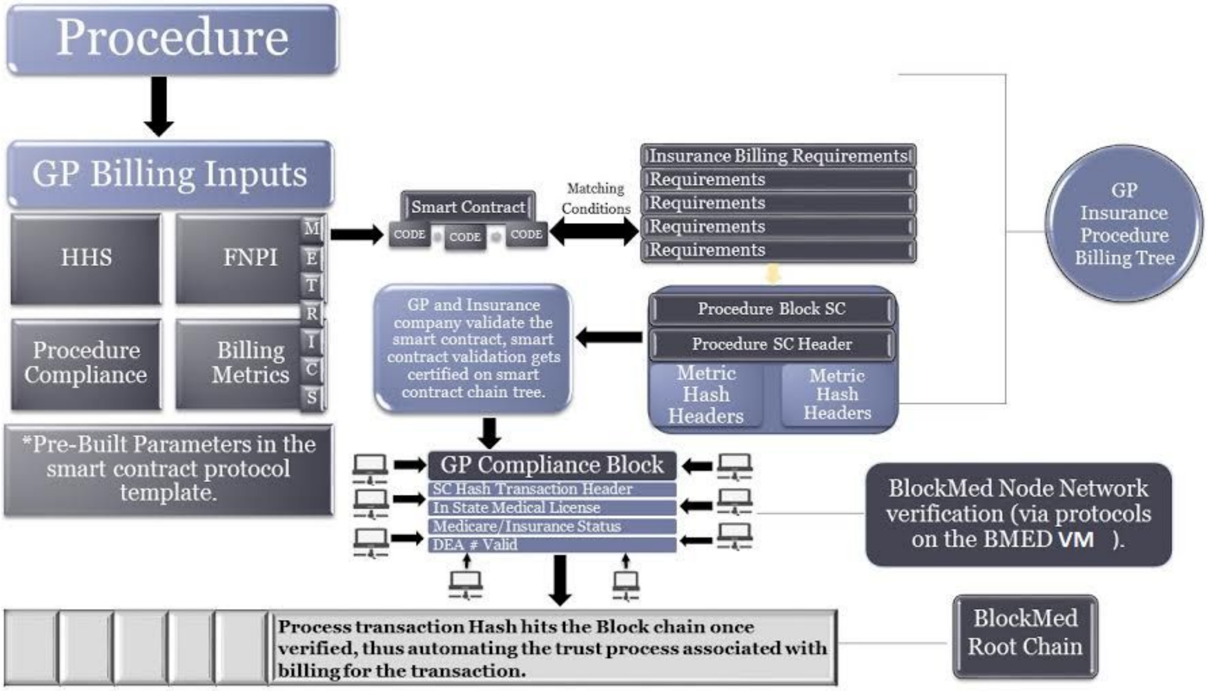
BitClaims eco-system will be validated through GP's and insurance companies who are compliant with healthcare regulations. BitClaims validates the compliance of said care providers through existing regulatory channels. Validated providers then only interact with other compliant nodes in the BitClaims network. This way, when a provider records a SOT on the BitClaims chain, certification of the SOT's occurs in that block. The certification is a hash of the SOT, and certain pieces of metadata related to the specific SOT. This way the GP who in turn needs to certify that the billing requests are in fact legitimate, can attest to that legitimacy through the work already done by the network on the blockchain, via the smart contract child trees.



```
Claim:
{
   ID: f279fjhe4895nfL46
   paient: 0xsF5vb4438ef
   HealthPlan:5b79U1ds68hW
   Type: 6789
   Service: 12345
   ServiceDate: 111820171145
   Quantity:2
   unitPrice:15000
   netPrice:15000
   claimURL:
"api.insurancenetwork.com/claim/f2
79fjhe4895nfL46"
}
```

Through the use of contextual smart contract trees and the BitClaims blockchain, Bitclaims healthcare communications platform will be built on a proprietary blockchain and smart contract layer similar to the security of the bitcoin network (for the secure validation of transactions on an unalterable ledger, in this case SOT's), while still providing agility to maneuver through a complex regulatory and technical environment.

Due to the complex technical and regulatory nature of the healthcare industry, BitClaims seeks to reward GP's and insurance companies that adhere to already established regulatory compliant standards, and are in compliance with the BitClaims platform by enabling the certification of a block to come with a BitClaims coin reward. On a network of GP's and insurance companies who act as miners, that are all in good standing with these factors, the incentive to both stay in good standing and only certify compliant SOT's becomes clear.


Procedure
GP Billing Inputs
HHS
FNPI
Procedure Compliance
Billing Metrics
M
E
T
R
I
C
S
*Pre-Built Parameters in the smart contract protocol template.
Smart Contract
CODE
CODE
CODE
Matching Conditions
Insurance Billing Requirements
Requirements
Requirements
Requirements
Requirements
GP Insurance Procedure Billing Tree
GP and Insurance company validate the smart contract, smart contract validation gets certified on smart contract chain tree.
Procedure Block SC
Procedure SC Header
Metric Hash Headers
Metric Hash Headers
GP Compliance Block
SC Hash Transaction Header
In State Medical License
Medicare/Insurance Status
DEA # Valid
BlockMed Node Network verification (via protocols on the BMED VM).
Process transaction Hash hits the Block chain once verified, thus automating the trust process associated with billing for the transaction.
BlockMed Root Chain

The BitClaims App and Provider Interface

The front end of the BitClaims platform will allow GP's and insurance companies to ping each other for a SOT, while keeping the nature, location and cause of said SOT ping anonymous. The BitClaims app, of which GP's and insurance companies will interact with each other to validate the completion of an SOT, will be an intranet portal able to interact with smart contracts directly. Allowing the GP and insurance company to 'spin up' child trains directly,with pre-set rules understood by both parties and unalterable via the smart contracts, at will and on a per claim basis. When the admin at a GP initiates the billing for a procedure, they are guided via the web portal to fill out the necessary metrics associated with the procedure they are requesting the insurance company release funds for.

To simplify the process initially, BitClaims uses the already well established billing sequencing by Medicare and industry for a standardized set of billing requirements for the procedure in play. Once the admin completes this first step, the metrics are populated into the smart contract for that specific claim. The proprietary use of BitClaims smart contracts means that these metrics are hashed, and not all of the smart contract code is publicly available so that the GP and insurance company are the only parties aware of the metadata associated with the procedure metrics going into the smart contracts. In addition, this allows BMED to comply with US regulatory healthcare standards (see coming regulatory paper by BMED for more information regarding our status and relationships). The GP and the Insurance company are the only ones able to unravel the cryptographic hashes associated with the metrics of the smart contract parameters to verify billing specific items. The network nodes however are able to validate the process within the smart contract to ensure that the sequencing of requesting funds for said claim is in fact correct and compliant to industry and regulatory standards.

The only information that hits the BitClaims root chain is the hash header of the GP’s and insurance company's smart contract interaction, and hashes of the sequencing commensurate with the specific procedure. For now, BitClaims serves as the mediator that exclusively interacts with the smart contracts, in the future however, the providers will be able to interact with the smart contract directly. Additionally, the GP’s and insurance companies will be able to provide insight and guidance on the buildout of additional smart contract infrastructure on a procedure based basis. This opens up the opportunity for a merit based ecosystem to evolve, while adhering to regulatory standards, and at the forefront providing superior quality care and service to patients. BitClaims will exclusively develop the the smart contracts being used on the healthcare communication platform and the software thereof, while keeping open the opportunity for third party providers.

Lastly, the GP’s will be the exclusive holders of the patient data. BitClaims will not handle the storage of EHR’s, or any variation thereof, in this context or form. For the BitClaims platform, it suits the providers to to have access to the data they require, with the permission of transfer and SOT coming from another provider on the network. With this approach, BitClaims keeps the benefits of a decentralized and distributed computing structure, while keeping the data integrity and compliance cooperation on the side of the providers and insurance companies.

BitClaims Blockchain Tree Hierarchy

The architecture of the BitClaims platform allows for a network where the nodes assert computation and subsets executing smart contracts and SOT’s between each other are responsible for verifying them.

The architecture as such will be customized for a healthcare communication platform use case. This leverages proven enterprise implementations with Postgres for scalability and interoperability into legacy databases. In our architecture, where the patient data does not actually touch BitClaims, and whereas BitClaims executes a certified SOT for said procedure in play via our platform.

In the third tree depth described above, the GP and insurance company enter into an agreement whereas one node requests the SOT for billing metrics that is in play from another node. The BitClaims API and software interface automates the process of hashing certain procedure billing metrics, metadata that would be in transit between providers, without actually having the task of reading the data, by way of interaction between the BitClaims software and API.

Conclusion

The failure to confront and mitigate compliance risks can be devastating to a physician practice and can mean a slow, but consistent, leak of money from the perspective of the health insurer. For physicians, repayment obligations for false claims are generally three times the amount of the claims plus $11,000 per claim. It is shocking how fast the penalties add up. Extreme cases of fraud can also lead to criminal investigation and prosecution. Recently enacted healthcare reform legislation makes it easier in a number of ways for the government to bring criminal prosecutions in the healthcare area.

Health insurers also have a significant stake when it comes to the compliance of their physician/provider members. The insurers do not want to overpay for services billed to them by providers, nor do they wish to expend resources on various auditors who conduct expensive recoupment actions due to inadvertent billing mistakes or fraud. The insurance companies have a vested interest in the member providers' compliance.

Value based medicine means catching value and savings where they can be obtained. 1) Pinpointing specific difficulties experienced in the implementation and maintenance of physician compliance programs; 2) focusing on the specific difficulties that can be addressed with blockchain technology; and 3) finding blockchain-based solutions for same, results in value obtained from achieving compliance and value obtained from utilizing a lower cost and innovative technology.

Now that compliance programs are mandatory for most providers, it is necessary to ensure they achieve their intended purpose. Making the mistake of taking compliance in a half-hearted manner will result in a loss of the benefits of an effective compliance program and damage an organization when a problem arises.

BitClaims will play an increasingly significant role in healthcare IT and bring beneficial disruption and new efficiencies to every stakeholder in the ecosystem. It is vitally important that healthcare organizations understand the core of blockchain technology to ensure they are ready for the changes the technology entails. The result will be a new generation of powerful, blockchain-based applications that will shape the next era of business in healthcare. For blockchain to full its potential in healthcare, it must be based on standards to ensure the compatibility and interoperability within the siloed health care system landscape.