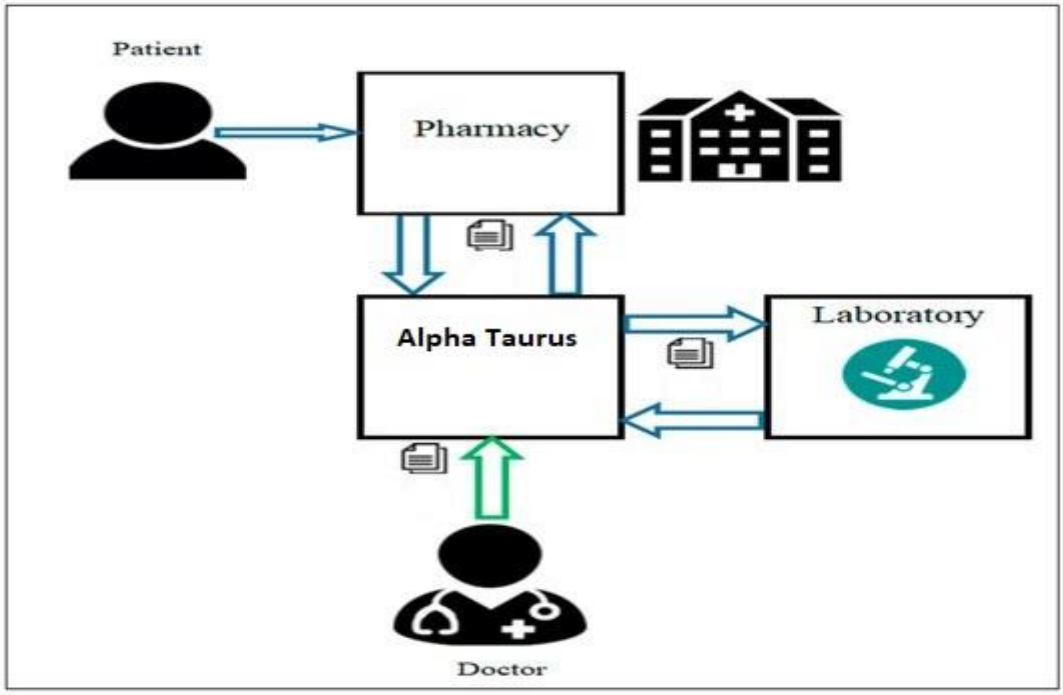
WHITE PAPER

ALPHA TAURUS

V.1.1

Providing a secure environment for data recording and transmission, Alpha Taurus are network providers that support Alpha Taurus applications in managing industry-generated data by clinics, hospitals, pharmacies and insurance companies by creating a technology foundation that connects stakeholders. Blockchain technology is basically how patients and healthcare providers share claim information, how provider data is updated and recorded over a network, how a patient's medical records are shared and updated over the course of treatment (from a primary care provider to a specialist to a pharmacist), population health It will change how prescription drugs are collected and analyzed, and how prescription drugs are tracked and tracked throughout the supply chain.



You can buy it from the worldwide supply package. However, the subject is health, this care and attention reaches the highest level. Blockchain technologies offer more solutions in the supply chain in general. Because being watched late can bask in chaos. Alpha Taurus technology plays a key role for the healthcare industry to benefit from a production to production in a very safe way

We show how the Alpha taurus blockchain technology supports a distributed payment network and improves methods for receiving and sharing health data. How identity components fit into blockchains, how validated data can form the basis for a single medical identity, how cryptography can support a physician's secure approval of healthcare data among patients related to their profession, how Alpha taurus technology can automate and eliminate many internal quality controls and how patient claims they are. We will show you how you can change your processes. Strengthening a shared infrastructure can bring new efficiencies to patients and healthcare providers, and we will have an impact on labor costs, reconciliation efforts, automated decision-making rates and the overall member experience.

Healthcare data is the cornerstone of the health information system. Physician demographics, such as office addresses, doctor's appointment times, phone numbers, specialties, and certifications are used to populate doctor's directories, which are used by members to find relevant and in-network doctors in their area. Healthcare data is also crucial to insurance payments. The patient must verify that the request for reimbursement comes from a certified network physician and that the care provided is

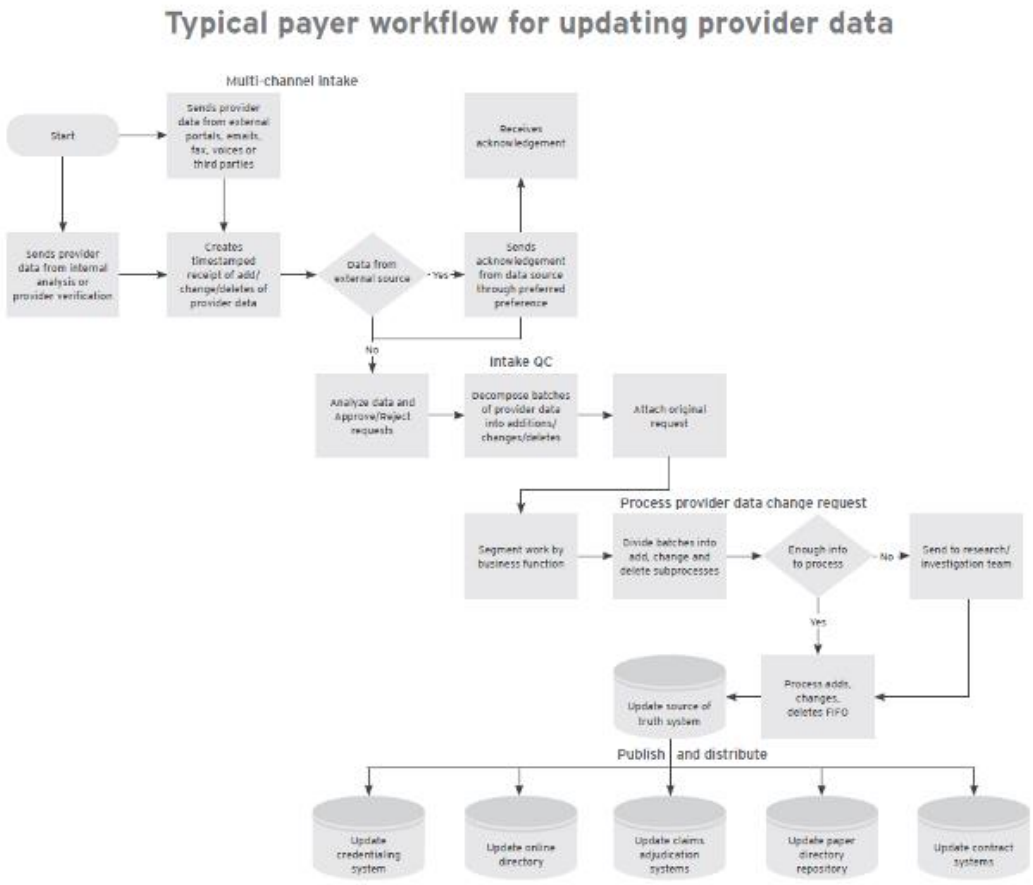
payable under the policy. Maintaining and disseminating precise and up-to-date service data is very important for the healthcare industry.

Unfortunately, the quality of healthcare data is not always directly proportional to the value it adds to the industry. Recent research shows that the doctor's records in the hands of the patient or the institution contain up to 40% of errors or incomplete information. This is a direct result of doctors constantly entering and exiting networks, changing places and hours. There are already existing processes for monitoring and updating physician information, but they are manual and extremely dysfunctional due to the numerous systems that need to be fully and accurately updated.

The image below shows a typical workflow used to update provider data in a payer's "source of truth" system and associated databases.

For a physician joining multiple networks, updating demographics is not as simple as updating their field of study. Each patient applies to health care institutions every six months or once a year in order to request confirmation of the demographic information in their files. If the information has changed, the organization will provide the patient with up-to-date data. Unfortunately, there is no reliable mechanism for healthcare organizations to share demographic information with multiple payers. Verification and updating of data is done by each healthcare provider several times a year. In addition to this obviously inefficient method, it also introduces a high risk of error. During data acquisition, a health institution or a person who will receive health care services, on web portals, By transferring each transaction in electronic medical record databases and insurance payment systems to be updated, the probability of making mistakes is also increased. Another important problem is the uniqueness of the data. Regardless of errors, the same doctor information may be formatted differently between patients. In an industry focused on interoperability,

having standard and uniform healthcare data formats will improve quality and sharing.

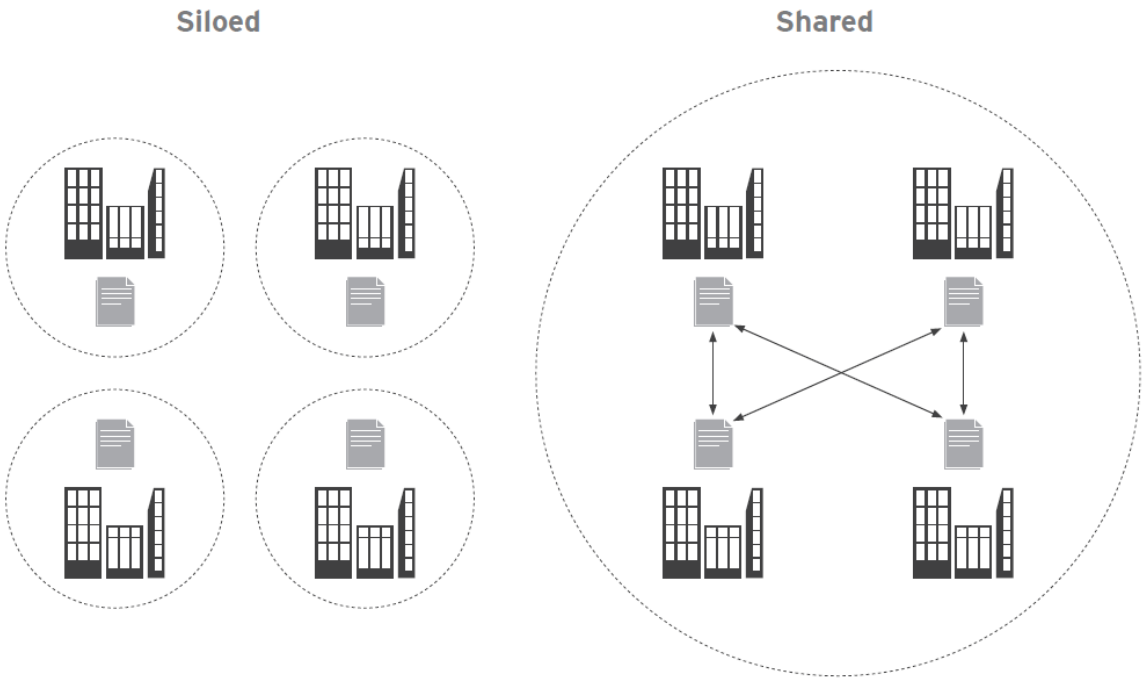


Database technology is not a new technology, distributed databases have been around for about ten years but relational databases have been around for a longer time. Blockchains are another form of database and while they share many elements with more traditional forms, what makes it innovative is their difference from other database forms. By design, blockchains are intended to be shared by individuals, organizations, and even devices. In a digital world, where databases are the underlying infrastructure, blockchains are common infrastructures—shared as an “application” through which many types of data can be stored, referenced, and transferred—and a mechanism by which this activity can be recorded in an unalterable manner.

Blockchains contain a built-in identity mechanism—a cryptographically secure individual—public key pair that is used to associate activity on the network with a

specific participant (e.g. person, entity, device). By itself, the key pair anonymizes the participant rather than revealing his true identity. However, information such as name, contact information or professional credentials can be associated with a key pair that combines on-chain and off-chain identities. In the context of the healthcare industry, the unique identity mechanism of blockchains can provide the basis for a single, reliable patient identity between patients and physicians.

Using the identity system as a basis, permissions can be assigned to participants in a network. Permissions refer to certain capabilities on the blockchain, such as the ability to read or write data. Permissions can be attributed to individuals at the most granular level; For example, an individual can be given permission to read and write Document A, but only to read Document B. Because these permissions are also stored on the blockchain, a network participant can be sure that the data they upload can be accessed only by the party that has access, i.e. only the authorized party, even though it is hosted in a decentralized location.



One of the most valuable features of a blockchain-based network is audit trail or transaction recording. Transactions on the network or in a non-financial context are grouped into blocks for batch processing. These transactions can involve any type or amount of data and can range from a simple token transfer to the execution of a smart contract with complex privileges and features. Over time, blocks of motion form a chronological chain, with each new block necessarily referencing information contained in the previous block, as each link in a chain fence necessarily overlaps adjacent link segments. Because of this "reference overlap", any attempt to change the information in the previous block will necessarily change the information in all subsequent blocks.

This chronological chain of activities is shared with everyone and anyone joining the network can keep a full history of activity. From a financial standpoint, this means that multiple parties can collectively maintain a common copy of a transaction ledger.

In blockchains, one type of chain is not suitable for everyone or every organization. A blockchain-based system can be open and public or private and permissioned. Public blockchains are accessible to everyone. No permissions are required to join and be on the network. They are also naturally transparent; all actions in the network must be verified and visible to all participants in the network. If any transaction is not visible to all participants, the transaction cannot be properly verified.

Private, permissioned blockchains work just the opposite. Before a participant can join and be in the network, the participant must be given permission. As noted earlier, participants can only be granted one or both read and write permissions. Some participants may have read and write permissions, while others may only have read or write permissions. The ability to grant various permissions to network participants makes it particularly suitable for use in more commercial settings, such as healthcare, where actions and information are not intended to be public. In this way, participants

will be able to maintain the advantage of a common infrastructure while maintaining the level of security and privacy. Our aim is to develop blockchain technology in the health sector and to create a digital ledger in the health sector.

Alpha Taurus Team