



GLOBAL CONNECT PROJECT

<STORAGE>
<PERSISTENCE LAYERS>

WWW.PARADIGMA.CL
INFO@PARADIGMA.CL

18 DE AGOSTO DE 2018

TABLA DE CONTENIDOS

DESCRIPCIÓN DEL ECOSISTEMA
CAPAS DE PERSISTENCIA

DESCRIPCIÓN DEL ECOSISTEMA

El ecosistema de aplicaciones distribuidas de Paradigma permite y promueve la evolución y mejoramiento de los negocios mediante la tecnología Blockchain.

Las aplicaciones del ecosistema de paradigma son “sin servidor” (Serverless Application) y son totalmente descentralizadas. No hay intermediarios ni servidores.

Son aplicaciones SPA (de una sola página) en Javascript y Haskell. Contienen una librería llamada "blockstack.js".

El ecosistema de aplicaciones de paradigma facilita el intercambio de transacciones entre una organización y sus usuarios finales, y permiten la persistencia de los datos en la nube, en formato JSON, para que sean importados a los sistemas de gestión propias de la organización.

Las aplicaciones de paradigma facilitan, mediante “Blockstack”, manejar y autenticar al usuario, para que tenga el acceso a sus recursos, realizar las transacciones y permitir el almacenamiento de datos en la nube. El almacenamiento de datos es simple y fiable y utiliza la infraestructura existente en la nube. Los usuarios se conectan con su Dropbox, Google Drive, One Drive, entre otros, y los datos se sincronizan desde su dispositivo local a la nube.

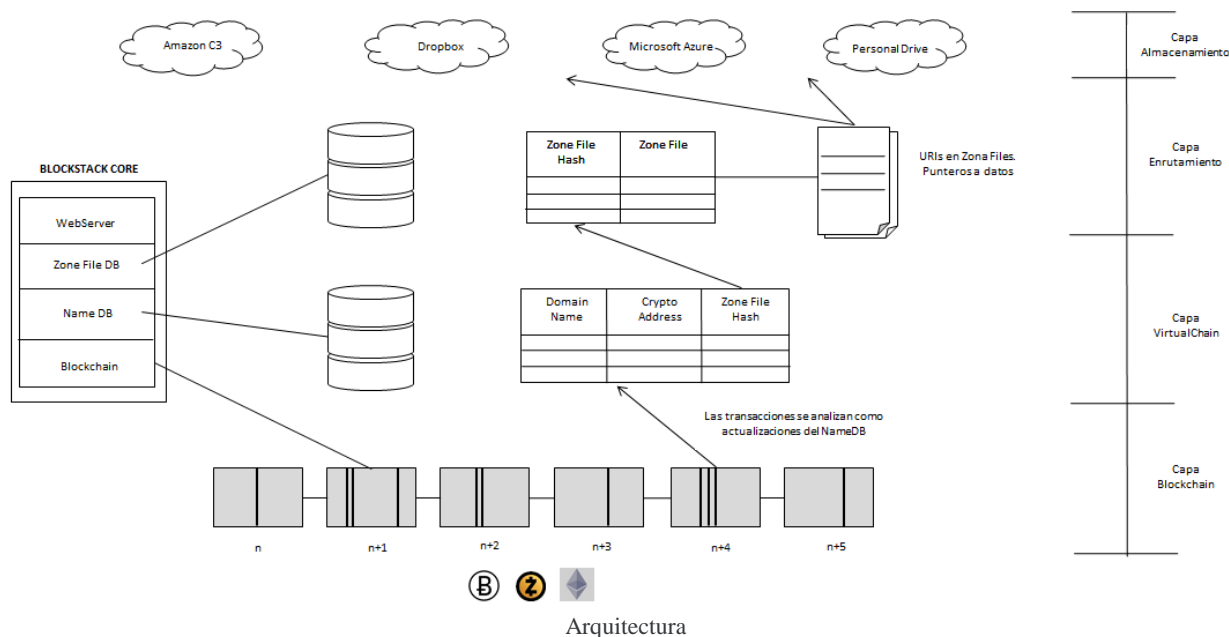
La identidad es controlada por el usuario y utiliza el “Blockchain” para la gestión segura de las claves, dispositivos y nombres de usuario.

La conexión de los usuarios con las aplicaciones, son anónimas por defecto y utilizan una clave de aplicación específica, pero su plena identidad puede ser revelada en cualquier momento. Las claves son para firmar y cifrar y se pueden cambiar.

Mediante “Blockstack” se proporciona un sistema descentralizado de nombres de dominio (DNS), que permite crear un ambiente distribuido pero cerrado bajo un dominio para una organización financiera, es decir, donde participen todos los actores que se encuentren bajo el dominio.

Permite además un sistema de distribución de claves públicas descentralizada, un registro de las aplicaciones y permite también el control de las identidades de los usuarios.

CAPAS DE PERSISTENCIA

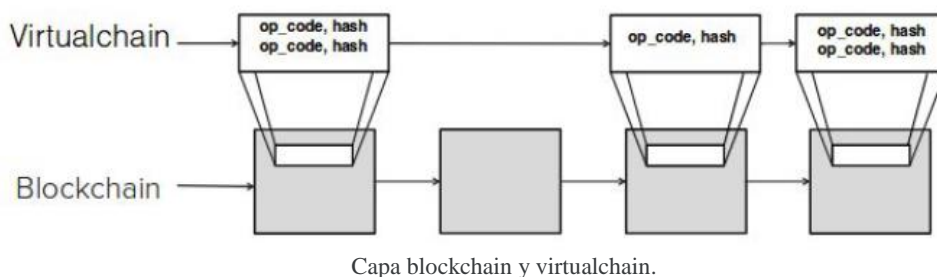


Capa Persistencia Blockchain y Virtualchain

Es la capa más baja y combina la blockchain subyacente y la virtualchain. Tiene dos propósitos: proporcionar el medio de almacenamiento para las operaciones y mantener consenso sobre el orden en el que las operaciones fueron escritas.

Por un lado, la cadena de bloques subyacente se trata como un canal de comunicación que lleva las operaciones totalmente ordenadas, mientras que todos los cálculos operativos y la lógica -incluidas las operaciones de minado y el algoritmo de consenso-, son procesados por la cadena virtual, sin requerir cambios en la cadena de bloques.

La virtualchain o cadena virtual solo procesa transacciones con códigos de operación válidos desde la blockchain. Los códigos de operación (op_code) se anuncian en las transacciones de Bitcoin en el campo designado para datos adicionales, llamado OPRETURN. Las transacciones aceptadas se organizan en bloques virtuales unidos por un hash de consenso que refleja el historial previo de la cadena virtual.

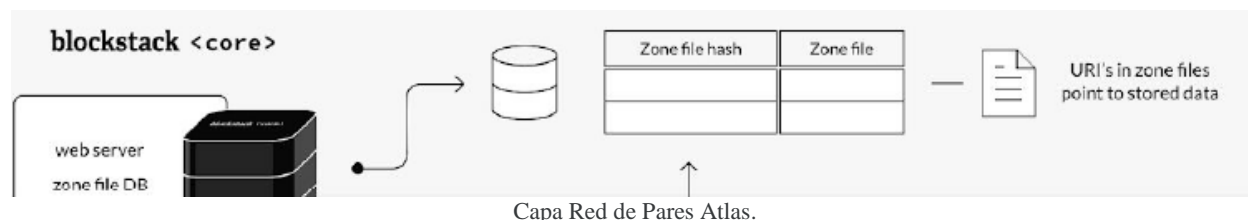


La arquitectura de la plataforma puede funcionar con cualquier número de canales de comunicación subyacentes, y cualquier blockchain subyacente puede alojar varias cadenas virtuales de tipos diferentes. Las principales ventajas de la implementación de la virtualchain son una mejor tolerancia a fallos en el caso de un fallo en la blockchain subyacente y mayor escalabilidad y seguridad al permite migrar de una cadena de bloques subyacente a otra con nuevos protocolos blockchain más seguros.

Capa Red de Pares Atlas (persistencia registros que apuntan zona almacenamiento gaia)

Los nodos forman una red de pared (peer network), llamada Atlas que mantiene un registro de las rutas (“zone files”), que apuntan al almacenamiento de datos principal implementado en la capa superior (almacenamiento Gaia).

La red sólo permite escribir archivos si el hash se anunció previamente en la blockchain. Esto incluye una lista blanca de los datos que se pueden almacenar en la peer network. Los registros de datos que representan rutas se pueden verificar y, por lo tanto, no se pueden alterar. En la implementación actual de la red Atlas, los nodos mantienen una copia completa de todos los archivos, ya que el tamaño es relativamente pequeño (4 KB por archivo).



Capa Cubo de Almacenamiento Gaia

La capa superior almacena los datos. La implementación es similar a otros almacenamientos en la nube, como Google Drive, Dropbox o Drives Personales. Todos los valores almacenados están firmados por una clave definida en el plano de control. Además, Blockstack hace posible el uso de diferentes almacenamientos siempre que los punteros a esos almacenamientos estén almacenados por Blockstack, y los proveedores de almacenamiento guarden únicamente datos cifrados.

Gaia es un “*concentrador de almacenamiento*” descentralizado de alto rendimiento y programable, se implementa por medio de interacciones entre API de desarrollador y el servicio de Gaia y se puede desplegar por medio de Heroku (Heroku es una plataforma en la nube basada en un sistema de contenedor administrado, con servicios de datos integrados y un ecosistema, para implementar y ejecutar aplicaciones)

Gaia funciona alojando datos en uno o más sistemas de almacenamiento existentes a elección. Estos sistemas de almacenamiento suelen estar en la nube. Existen controladores para

S3 y Azure Blob Storage, pero también admite otros soportes de back-end. Se puede elegir dónde se almacenen los datos y permite que las aplicaciones accedan al dato a través de una API.

El enfoque de Gaia hacia la descentralización se centra en el control del usuario sobre los datos y el almacenamiento. Si un usuario puede elegir qué concentrador de Gaia y con qué proveedor de servicios almacenar los datos, entonces esa es toda la descentralización requerida para habilitar las aplicaciones controladas por el usuario.

En Gaia, el control de los datos del usuario radica en la forma en que se accede a los datos del usuario.

El concentrador de almacenamiento de Gaia almacena los datos escritos exactamente como se indique. Pueden estar o no encriptados, pueden ser XML, JSON, TXT, etc...son decisiones de diseño del lado del cliente.

Los controladores de concentrador de Gaia son bastante simples. El mayor requisito es la capacidad de cumplir con el escribir-leer / leer-desde

