فیش ۱

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش: ۱-۴	نوع نوشته: مستقیم	شماره فیش:۱	منبع: G۵

تکنولوژی 5g قابلیت اتصال دستگاه ها را به همراه افزایش مکرر ظرفیت شبکه دارد. همچنین این تکنولوژی کاربرد های بسیاری در حوزه امنیت، کانون زدایی و به اشتراک گذاری داده ها دارد.

فیش ۲

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش: ۲	نوع نوشته: مستقیم	شماره فیش:۲	منبع: G۵

تکنولوژی بلاکچین در مواردی مانند پرداخت های آنلاین ،سیستم سلامت، قرارداد های هوشمند و ... به کار میرود
در شبکه هر انتقال اطلاعاتی بدون ناظر خاصی ثبت و انجام میشود.بلاکچین مجموعه ای بلاک ها است که به کمک یک زنجیر متصل هستند . یک بلاک بعد از تایید توسط تمامی بلاک ها به این زنجیره اضافه میشود.
بعد از اضافه شدن بلاک ،بلاکچین به سه بخش تقسیم میشود :

۱. بخش private
۲. بخش public
۳. بخش permissioned

از فواید بلاکچین میتوان به حافظه بیشتر،امنیت، غیر قابل نفوذ بودن،سرعت در پردازش و سیستم غیر کانونی اشاره کرد.
هسته بلاکچین گره ها، انتقالات، بلاک، و زنجیر هست.

فیش ۳

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش: ۲	نوع نوشته: غیر مستقیم	شماره فیش:۳	منبع: G۵

الگوریتم تخته توزیع شده (distributed ledger):
در این الگوریتم هر دیتابیس در شبکه نظیر به نظیر به اشتراک گذاشته میشوند
در بلاکچین دیتابیس برای تمامی مخاطبین شبکه به اشتراک گذاشته میشود .هیچ بیگانه ی خارج از شبکه ای برای به انجام در آمدن تراکنش ها نیاز نیست . هر نقل و انتقالی بدون کمک شی بیگانه ای میتواند بین دو یا چند مخاطب بیتکوین به اشتراک گذاشته شود.
هر رکورد دارای یک نشانه امنیتی خاص به همراه خط زمانی مشخصی که زمان دسترسی ها را نشان میدهد ، است. به همین دلیل تخته غیر قابل تغییر و قابل بررسی میشود.

الگوریتم توافق عام (Consensus algorithms):
فرایند یک بلاک تنها در میان چند گره ای که به آنها تعلق ندارد اشاره میکند . بلاک های بلاکچین از این نوع الگوریتم بهره میگیرند

قرارداد هوشمند (smart contract):
برنامه برنامه نویسی شده ای که که بر روی بلاکچین اجرا میشود.

بهبود امنیت :
به دلیل رفع اجازه دسترسی اجباری از سوی قدرت مرکزی ، هیچ فردی به راحتی نمیتواند مشخصات سیستم را برای نفع خود عوض کند.

فیش۴

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش: ۲	نوع نوشته: غیر مستقیم	شماره فیش:۴	منبع: G۵

الگوریتم توافق عام (Consensus algorithms):
فرایند یک بلاک تنها در میان چند گره ای که به آنها تعلق ندارد اشاره میکند . بلاک های بلاکچین از این نوع الگوریتم بهره میگیرند

قرارداد هوشمند (smart contract):
برنامه برنامه نویسی شده ای که که بر روی بلاکچین اجرا میشود.

بهبود امنیت :
به دلیل رفع اجازه دسترسی اجباری از سوی قدرت مرکزی ، هیچ فردی به راحتی نمیتواند مشخصات سیستم را برای نفع خود عوض کند.

فیش ۵

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش:۲-۳	نوع نوشته: غیر مستقیم	شماره فیش:۵	منبع: G۵

با استفاده درست از بلاکچین، میتوان میزان بهره وری را در سیستم سلامت بالا برد. چرا که امنیت، محافظت را بالا برده و هزینه را کاهش میدهد. framework مورد نظر میتوان کار ها را با نظم مشخصی به کمک NFV ها که پاسخ دهی اینترنت اشیا را ارتقا میدهد ، انجام دهد.
وظیفه بلاکچین در اطمینان حاصل کردن از درستی اشتراک اطلاعات و برقراری امنیت خلاصه میشود . به طور مثال ارتقای امنیت و قدرت میان سازمان بیمه و بیماران و یا انتقال امن اطلاعات میان دستگاه ها و یا قرارداد ها.

فیش ۶

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش:۱-۴	نوع نوشته: غیر مستقیم	شماره فیش:۶	منبع: G۵

با کمک دستگاه های اینترنت اشیا، میتوان علائم حیاتی بیمار مانند ضربان قلب، شرایط خواب، فشار خون، قند خون و ... را اندازه گیری کرد. این اطلاعات توسط دکتر آنالیز شده و در فضای ابری به کمک بلاکچین ذخیره میشود.
همچنین بیمار میتواند اطلاعات خود را با دیگر بیمارستان ها به اشتراک بگذارد. استفاده از قرارداد هوشمند انتقالات در سیستم بلاکچین را میتوان از هرگونه خطر جانبی حفظ کرد.

فیش ۷

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش:۱-۴	نوع نوشته: غیر مستقیم	شماره فیش:۷	منبع: G5

الگوریتم تولید کلید :

به کمک الگوریتم ECC و به کمک مقادیر P & Q امنیت را ایجاد میکنیم

- این دو مقدار دارای کلید های A و B هستند
- P درخواست خود را به Q میفرستد
- Q درخواست را قبول میکند
- مقدار K را حساب میکند.
- $K = \frac{Y_B - Y_A}{Z_B - Z_A}$
- Q مقدار C را از K حساب میکند
- این مقدار را به P میفرستد
- مقدار C از رابطه زیر به دست می آید.

$$Z_C = \kappa^2 - Z_A - Z_B$$

- $$Y_C = (\kappa Z_A - \kappa Z_C) - Y_A$$
- P مقدار C به دست آمده را حساب میکند
- اگر با K برابر بود ، اطلاعات را به Q ارسال میکند.

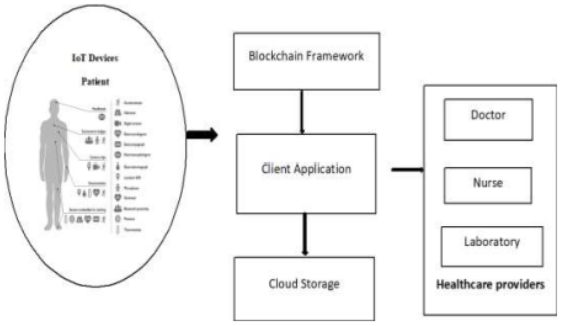
```
function Assignkey ()
{
        if patient confirm data  over blockchain then
        Generate a key K using ECC
        A<- Get values from ECC_Database
        a sends a Req message with A and B values appended to it

         b computes K from A and B

        b sends a reply with C
        Node a checks the C

         If

         {

                C=A+B

                Retum 1

        else
                Do nothing
        }
}
```

فیش ۸

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش:۲-۳	نوع نوشته: غیر مستقیم	شماره فیش:۸	منبع: G5

به هر بیمار یک شماره خاص (patient id) منصوب میگردد. که به سیستم سلامت اجازه دسترسی به اطلاعات بیمار را میدهد.



امنیت این اطلاعت به کمک سیستم کدگذاری میتوان تضمین کرد. این کد توسط بیماران تولید شده و سپس این کد را میتوان با دستگاه های سوم شخص (third pary) به اشتراک گذاشت . زمانی که نمیتوان به بیمار دسترسی داشت به کمک روش key escrow میتوان به اطلاعات دسترسی داشت.

برای قسمت ثبت اطلاعات مقادیر مورد نیاز به صورت

Patient Id, Record, Record Hash, File Id, Date, Doctor Id, Disease Id, Parent)

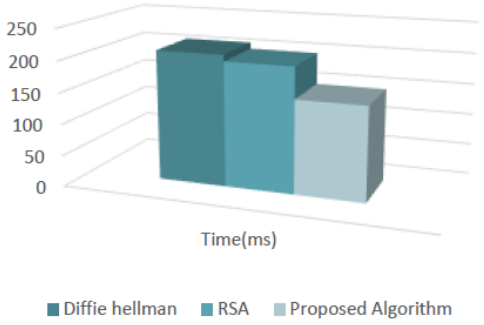
record hash) است

فیش ۹

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش:۱-۴	نوع نوشته: مستقیم	شماره فیش:۹	منبع: G5

هزینه محاسبات برای نود های 5g برای محاسبه توابع مورد نیاز در این پروسه امنیتی به شکل زیر است:



فیش ۱۰

۰۸:۵۲ ب.ظ دوشنبه, ۱۶ اسفند ۱۴۰۰

بخش گزارش:۵	نوع نوشته: مستقیم	شماره فیش:۱۰	منبع: G۵

در این بخش متوجه شدیم که با ترکیب تکنولوژی بلاکچین با اینترنت اشیا میتوان به هدف های مهم تری دست یافت. مهم ترین مسئله اینترنت 5G امنیت است و برای این امنیت از بلاکچین استفاده میکنیم. سیستم پیشنهادی به امنیت داده ها در سیستم سلامت به کمک ترکیب تکنولوژی بلاکچین با اینترنت اشیا به کمک الگوریتم ECC اشاره دارد