## **مقدمه :**

به دلیل پیچیدگی های تبادل در زندگی بشری دو چیز به وجود آمد : ۱.پول ۲.اعتبار

بزرگترین مشکل پول دیجیتال double spending میباشد به این صورت که ممکن است که از یک پول بشود یک نسخه ی دیگر به وجود آورد و همزمان از هر دو نسخه استفاده کرد

مشکل بعدی bootstrap میباشد به این صورت که حتی اگر یک پول دیجیتال هم ساخته میشد آدم‌ها ( فروشنده و خریدار ) حاضر به استفاده از آن نمیشد (bootstrap به این معنا میباشد که در حالت اولیه به ثباتی برسد که بتواند حرکت کند )

در پول‌های دیجیتال دو مفهوم خیلی جدی شده است : ۱. اعتبار در این پول‌ها به سمت حل پازل یا مساله رفته است ۲. Ledge یا دفتر سیاهه کل معماملاتی که در آن درحال پیشروی هستیم

خالق bitcoin شخصی به نام satoshi nakamoto میباشد که حوالی سال 2007 تا 2009 bitcoin را ساخته و white paperش را در forum ها منتشر کرده است

=====================================================================================

**هش ها و امضاها :**

بلاکچین یک شکلی از data structure میباشد که bitcoin روی آن طراحی شده است

چند فیچیری که بیتکویین دارد و آن را برای ما جذاب کرده به عبارت زیر هست :  
 ۱. decentralized : مرکزیتی ندارد   
 ۲. برای اینکه شما بتوانید ارزش تولید کنید نیازمند این هستید که یک چیز کمیاب داشته باشید

ما برای ساختن پول دیجیتال به چندتا چیز نیاز داریم :  
 security (در پول‌های مرسوم دولت ها امنیت و موارد اینچنینی را تأمین میکند )  
 اینکه اون پولی که کسی به صورت رمز ارز به من میدهد ببینیم چقدر اصل و اوریجینال میباشد  
 آیا تاریخچه ی تبادلات بر روی سنگ نوشته شده است و غیر قابل تغییر میباشد   
 هیچ کسی نباید بتواند double spend کند

برای پاسخ به مشکلات بالا رمزنگاران با دو ایده ی اصلی (هش کردن و امضای دیجیتال) به کمک ما آمدند

هش ( hash ) :  
 یک تابعی میباشد که به ازای هر ورودی خاص یک خروجی خاص داشته باشد . هش های در دنیای عمومی ما باید ۳ ویژگی زیر را داشته باشند :  
 ۱. طول مقدار ورودی هر چقدر که میخواهد باشد   
 ۲. طول مقدار خروجی باید ثابت باشد   
 ۳. خیلی هم سخت نباشد محاسبه کردنش ( یک کامپیوتر معمولی بتواند در زمان معقولی آن را محاسبه کند )

اما هش در دنیای cryptographic باید ۳ ویژگی دیگر نیز داشته باشد:  
 ۱. به دلیل اینکه طول خروجی ثابت میباشد در نهایت ورودی های وجود دارند که مقدار هش آن‌ها یکسان میباشد و مشکلی وجود ندارد به این مورد collision گفته می‌شود اما کسی نباید بتواند collision بوجود آورد ( ورودی پیدا کند که خروجی خاصی را دارد )

۲. شما از خروجی هم نباید بتوانید به ورودی برسید ( one way )  
 ۳. حساب کردن هش هم نباید خیلی سریع باشد ( تا از مشکل brute force جلوگیری شود )

hash pointer :هنگامیکه dataیی وجود دارد و pointerی که به آن اشاره میکند در داخل pointer مقدار هش آن دیتا نیز وجود دارد به این مجموعه در‌واقع hash pointer گفته می‌شود

امضای دیجیتال ( signatures ) : به طور عمومی مفهوم رمزنگاری به وسیله ی کلید عمومی و کلید خصوصی (جفت کلید) میباشد

به طور کلی ما میتوانیم یک فانکشن به عنوان مثال GenKey داشته باشیم که که سایز مورد نظر خود را به آن بدهیم و دو کلید به نام های key secret و key public را برای ما تولید کند :

( keyS , keyP ) = GenKey(size)

توجه شود که GenKey یک تابع منحصربه فرد نمیباشد بلکه توابع و فانکشن های گوناگونی وجود دارند که میتوانند برای ما جفت کلید تولید کنند

حال اگر یک msg را به وسیله keyS رمز نگاری کنیم خروجی حاصل یک signature یا به اصطلاح sign میباشد

(msg , keyS) => sign

حال اگر این خروجی ( همان sign ) را داخل اینترنت قرار دهیم و همراه با دو مقدار دیگر که keyP و msg را درکنار هم قرار دهیم و به فانکشنی آن‌ها را بدهیم و خروجی فانکشن قابل قبول بود نشان داده می‌شود که msg به وسیله ی keyS رمز گذاری شده است و به sign تبدیل شده است

IsValid = (keyP, msg, sign)

در‌واقع در bitcoin میخواهیم ثابت کنیم که msg از طرف کسی که مدعی شده است آمده است

در بیت کویین keyP در‌واقع identity شما میباشد   
 در دنیای بیت کویین در‌واقع ما نیمه ناشناس هستیم یعنی اسم واقعی شما را کسی نمیداند اما با همین keyP یک identity خواهید داشت

آدرس کیف پول شما hashی هست که از keyP به دست می‌آید

address = hash(keyP)

=====================================================================================

# **گوفی و اسکروچ اولین پولشون رو می سازن :**

مفهوم بلاک چین به این صورت است که یکسری block وجود دارد که قرار است یکسری اطلاعات در آن‌ها ذخیره شود هنگامیکه در مورد BTC صحبت می‌شود قرار است در داخل بلاک ها چندین transaction یا به اختصار TRX همراه با timestamp که هر TRX چه زمانی صورت گرفته است همراه با هش آن‌ها ذخیره شود

برای اینکه بهتر بتوانیم با این مفاهیم ارتباط برقرار کنیم بهتر است از مثال‌هایی استفاده شود برای اولین مثال از goofy coin استفاده میکنیم

goofy coin :  
در مثال‌های زیر مفهوم امضا همان keyS میباشد   
 در goofy coin به اجماع میرسیم که goofy میتواند سکه تولید کند روش ساخت سکه هم به این صورت است که بر روی فایلی کدی unique مینویسد و همراه آن امضای خود را نیز قرار داد حال میتوانیم به آن یک سکه بگوییم

حال میخواهد این سکه را به شخصی به نام Z بدهد . بر روی همان فایل مینویسد که این سکه تحویل Z داده شد و این جمله ی تحویل Z بشود را goofy امضا میکند

حال شخص Z قصد دارد این پول را به شخص دیگری به نام y بدهد دوباره همانند روند بالا در ادامه فایل مینویسد که این سکه تحویل y داده شد و شخص Z به وسیله keyS خود آن را امضا میکند

تا الان میتوان گفت که درواقع پایه ی یک پول دیجیتال ساخته شده است چرا که بوسیله keyPها میتواند روند بالا را به سمت عقب طی کرد و به goofy رسید تا مطمئن شد امضا ها و حرف‌ها یا TRXها درست است یا نه

مشکلی که در این طرح وجود دارد double spend میباشد چرا که شخص Z به راحتی میتواند دو نسخه از این پول به وجود آورد به این صورت که همزمان جمله ی این پول تحویل y داده شد را همراه با امضای خود روی یک نسخه بنویسید و آن را به y بدهد و هم میتواند همزمان روی نسخه ی دیگر بنویسد که این پول تحویل x داده شد و امضای خود را به آن نیز اضافه کندو آن را به x بدهد . هر دوی این نسخه ها قابل قبول میباشد چرا که با استفاده از keyPها میتوانید به goofy برسید

scrooge coin :  
 در مثال goofy به مشکل double spending برخورد کردیم . در این مثال قصد داریم این مشکل را برطرف کنیم

تمامی روندهای انتقال پول مانند goofy میباشد اما با این تفاوت که scrooge که در این مثال مسئول ساخت سکه میباشد یک لیستی دارد که حاوی اطلاعاتی میباشد . این لیست در هر خانه ی آن حاوی هر trx همراه با hash آن trx که scrooge آن را امضا کرده است وجود دارد

مشاهده می‌شود که scrooge میتواند مشکل double spending را حل کند چرا که سرعت در این موضوع خیلی مهم می‌شود اگر سرعت ذخیره سازی scrooge به اندازه کافی بالا نباشد هنوز این مشکل وجود خواهد داشت

مشکل های بزرگی که در این روش وجود دارد این است که :  
 1. ما باید به scrooge اعتماد کامل داشته باشیم   
 ۲. مرکزیت scrooge ( در عمل ما همان کار بانکی را انجام میدهیم )

نکته ی جذابی که در کل این ماجرا دنبالش هستیم decentralize میباشد که میخواهیم مرکزیتی وجود نداشته باشد و لیست دست یک نفر نباشد

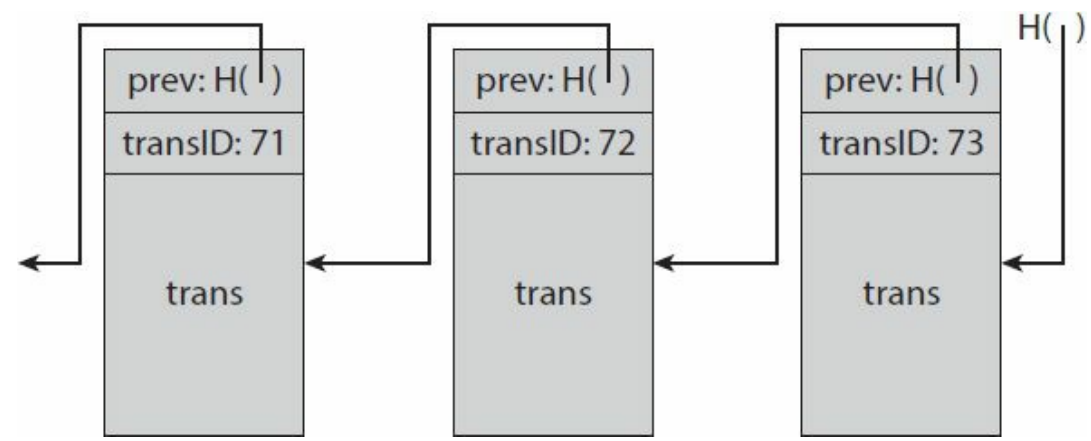
بیت کویین کار بزرگی که انجام داد decentralize بودن را پیاده‌سازی کرد

=====================================================================================

**عدم تمرکز و بحث اجماع :**

مفهوم بلاک به این صورت بود که در یک بلاک مجموعه‌ای از اطلاعات وجود دارد که hash آن اطلاعات نیز در بلاک وجود دارد

مفهوم بلاک چین به این صورت است که در هر بلاک هش بلاک قبل وجود دارد ماننده تصویر زیر :



به دلیل اینکه از hash pointer استفاده شده است شما نمیتوانید اطلاعات یک بلاک را به تنهایی عوض کنید

برای مفهوم decentralize پنج پرسش اساسی خواهیم داشت (در‌واقع این سه پرسش اول و جواب آن‌ها کاملاً فنی میباشد)

۱. ledger ها یا دفتر صورت حساب هارا چه کسانی نگهداری میکنند

۲. چه کسی authority یا قدرت دارد که بگوید کدام TRX معتبر یا valid میباشد

۳. چه کسی میتواند coin جدید درست کند

دو پرسش و مفهوم دیگر نیز وجود دارد که :

۱. چه کسانی حق دارند که تصمیم بگیرند که این قوانین از کجا بیایند  
 ۲.چه کسانی تصمیم میگیرند که امروز ارزش این coin چقدر باشد

مفهوم بسیار مهمه دیگر به نام consensus یا اجماع نیز وجود دارد که کدام ledger درست تر و کاملتر میباشد ( در‌واقع مشکل و مفهومی که وجود دارد در شبکه‌های غیر متمرکز یا decentralize میباشد چرا که در شبکه‌های متمرکز مشکلی وجود ندارد )

برای درک مشکل اجماع مسأله ای وجود دارد به نام ژنرال های بیزانسی یا byzantine generals به این صورت که جایی وجود دارد که قرار است چندین ژنرال در یک زمان به آن حمله کنند اگر اکثریت ژنرال ها در یک زمان باهم حمله نکنند شکست خواهند خورد حال فرض کنید که فاصله ی این ژنرال ها زیاد است و شب است و نمیتوانند به هم علامت دهند   
مشکلات زیادی وجود دارد از جمله سوارکار ژنرال اول که قرار است به بقیه ی ژنرال ها خبر دهد در راه دستگیر نشده است   
یا یکی از ژنرال ها آدم بدی است و وظیفه‌اش در خبر رسانی را درست انجام نداده است و ….

در حالت کلی گفته می‌شود که اگر مطمئن نباشید که همه آدم خوبی هستند و درست کار میکند خیلی سخت است که به اجماع برسیم ( اگر بیش از یک سوم گروه آدمی بدی باشد غیر ممکن است که به اجماع برسیم )

در جامعه بیت کویین افراد خوب بسیار زیادی وجود دارد که نشان داده است که در عمل خیلی بهتر از تئوری عمل کرده است به ۲ دلیل این اتفاق افتاده است :  
 ۱. به آدم‌های خوب مشوق داده می‌شود (هر کسی یک بلاک را sign کند هر 10 دقیقه یکبار به صورت رندم 10.5 بیتکویین دریافت میکن . هر 10 دقیقه یکبار یک نفر میتواند یک بلاک را sign کند )  
 ۲. جایزه به صورت رندم داده می‌شود

در قسمت دوم که جایزه به صورت رندم داده می‌شود حمله ی معروفی وجود دارد به نام sybil attack به این صورت که یک شخص از خود چندین کپی درست میکند و احتمال بردن جایزه و مشوق بیشتری به دست می‌آورد ( مثال دیگر: اگر قرار است کاغذی بچرخد و هر کسی موافق است یک خط به کاغذ اضافه کند شما میتوانید چندین خط اضافه کنید )

=====================================================================================

**به اجماع ضمنی رسیدن :**

به طور کلی میتوان گفت که مسأله پاداش دادن به آدم‌های خوب که در بیت کویین هم وجود دارد یک چیز کلی است چرا که مثلاً ایرانی هایی که قصد مهاجرت دارند هنگامی که از کشور خارج می‌شوند تمام تلاش خود را انجام میدهند که حتی یک خطای کوچک حتی در رانندگی انجام ندهند تا بتوانند در آینده بدون هیچ مشکلی پاسپورت خود را بگیرند و یا مثال دیگر در چند دهه قبل آدم‌هایی بودند که برای کارهای عملگی به ژاپن میرفتند و درآمد خوبی از این راه به دست می آوردند

implicit consensus ( اجماع ضمنی ) :  
برای رسیدن به اجماع ضمنی در بیت کویین ۵ قدم وجود دارد   
 - تمام nodeها همه ی تراکنش هایی که در آن‌ها اتفاق می‌افتد( تراکنش های جدید ) را به هم دیگه میگن   
 (new transactions are broadcast to all nodes )

-هر node تمام تراکنش های جدید را داخل یک بلاک (‌ اصطلاح فنی mempool‌ ) ذخیره میکند   
 (each node collects new transactions into a block)

- به صورت رندم هر دقیقه یک بار یک node بلاکی که خودش دارد را به همه اطلاع میدهد   
 (in each round, arandom node gets to broadcast its block )

- بقیه ی nodeها بررسی میکنند که این بلاک قابل قبول میباشد یا نه اگر قابل قبول بود آن را قبول میکنند ( بررسی میکنند که پول قبلاً ارسال نشده باشد یا امضای درست برای ارسال پول استفاده شده باشد )  
 (othe nodes accept the block only if all transactions in it are valid(unsend ,valid signatures))

- اگر بلاک قابل قبول بود آن را در ادامه بلاک هایی که خود دارند قرار میدهند و هش بلاک قبلی را به آن اضافه میکنند  
 ( node express their acceptance of the block by including its hash in the next block they create )

برا اساس ۵ مورد بالا سؤالاتی به وجود می‌آید که به آن‌ها نیز پاسخ داده می‌شود :  
 - از کجا متوجه شویم nodeی بلاک مورد نظر را قبول کرده یا نه ؟ بلاک چین بیتکویین میگوید برای اینکه node نشان دهد که بلاک را قبول کرده هش node قبلی را حساب میکند و داخل بلاک جدید قرار میدهد

- آیا کسی میتواند بیت کویین سرقت کنند ؟ نخیر جون پول‌ها sign شده هستند ( وقتی شما private key کسی را ندارید نمیتوانید transactionی را داخل mempool قرار دهید که پولی از حساب کسی که مد نظرتون هست کم شود

- آیا میتواند dos attack انجام داد ؟ dos یا denial of service به این معنی میباشد که تصور کنید کسی با سجاد بد است به همین خاطر تمام تراکنش هایی که پول به حساب سجاد می‌آید رو در نظر نمیگیرد . به دلیل اینکه ساخت block از mempool به صورت رندم اتفاق می‌افتد شاید در مرحله ای همچین اتفاقی بیافتد اما در مرحله بعد احتمال اینکه دوباره همان node بتواند block جدید تولید کند کم میباشد به خاطر همین transactionهایی که در block وجود ندارد اما در mempool نود جدید وجود دارد blockی ساخته می‌شود که transactionهای سجاد در آن وجود دارد

=====================================================================================

**اثبات کار ( proof of work ) :**

برای جلوگیری از حمله sybil attack راه حلی که در بیتکویین وجود دارد به این صورت میباشد , برای اینکه هر node بتواند mempool خود را به بلاک تبدیل کند باید یک کار خیلی خیلی سختی انجام دهد اگر این کار سخت را انجام داد در این صورت میتواند mempool خود را به بلاک تبدیل کند

این کار سخت به این صورت میباشد , هنگامیکه قرار است هش mempool حساب شود باید هش به گونه‌ای حساب شود که وقتی هش به عدد تبدیل می‌شود باید این عدد از عدد خاصی کمتر باشد

در حالت کلی ما میدانیم که امکان ندارد هش mempool به صورتی باشد که همچین ویژگی را داشته باشد برای این موضوع جایی را در mempool به node میدهیم که اجازه دارد مقادیر دلخواهی را در آن قرار دهد و hash را همراه این مقادیر خاص حساب کند

مقدار خاص دیگری هم در mempool وجود دارد که مثلاً 12.5 بیتکویین ( این مقدار هر چهار سال یا به طور دقیقتر هر 210000 بلاک نصف می‌شود ) را به کلید عمومی خود منتقل میکند

پس در حالت کلی مقادیری که در mempool وجود دارد به این صورت میباشد :  
 ۱. تمام تراکنش هایی که به node اعلام شده هست و قرار است انجام شود   
 ۲. مقدار پولی که node به کلید عمومی خود منتقل میکند ( در‌واقع همان جایزه ای که راجبش صحبت کردیم )  
 ۳. Nonce که همان مقدار دلخواهی است که node به وسیله ی آن hash را حساب میکند

حالت‌های مختلفی وجود دارد که ما به مشکل میخوریم به دلیل اینکه در شبکه decentralize قرار داریم ممکن است که گروهی از node ها متوجه ساخت بلاک جدید نشوند و آن‌ها نیز سعی در ساخت بلاک داشته باشند . راه حل این مشکل خیلی ساده میباشد به این صورت که بزرگترین blockchain را قبول میکنند به دلیل اینکه کار بیشتری روی این بلاک انجام شده است

مسأله ای که وجود دارد 51% attack میباشد به این صورت که ۵۱% از node های شبکه دست به یکی کنند که کار خاصی رو انجام دهند که بر اصول شبکه بیتکویین نمیباشد مثلاً trxی رو پاک کنند جواب به این سؤال به این صورت میباشد که شاید نتوانند در کوتاه مدت همچین کارهایی رو انجام دهند اما به دلیل اینکه نصف بیشتر انرژی شبکه دست یک گروه خاصی میباشد در دراز مدت توانایی همچین حمله هایی رو خواهند داشت

=====================================================================================