بررسی الگوریتم رمزنگاری در دنیای کریپتو

ارزهای دیجیتال جزو مهمی از دنیای امروز محسوب می‌شوند. برای این که ارزهای دیجیتال به وجود آمده و کار کنند، چند اصل مهم و بزرگ در کنار هم به این هدف کمک می‌کنند. به همین خاطر ارزهای دیجیتال در حال حاضر یکی از مهم‌ترین بازارهای مالی را به خود اختصاص داده‌اند.

یکی از مهم‌ترین دلایلی که افراد به این نوع از ارزها علاقه مند شده‌اند، امنیت بالای آنها است. به این صورت که هیچ فردی نمی‌تواند در دارایی‌های افراد تغییری ایجاد کرده یا آنها را مشاهده نماید. رمزنگاری یکی از اصول اصلی استفاده شده در ارزهای دیجیتال است. به این ترتیب ارزهای دیجیتال توانسته‌اند امنیت زیادی داشته باشند. رمزنگاری که نام رمزارزها نیز از آن گرفته

شده، یکی از مفاهیم مهم در دنیای بلاک چین است که در این مطلب از مجموعه کیف پول من به بررسی آن خواهیم پرداخت.

رمزنگاری چیست؟

رمزنگاری به فرایندی گفته می‌شود که یک پیام یا داده را برای افزایش امنیت با استفاده از الگوریتم‌های مختلف مورد تغییر قرار می‌دهیم تا پیام رمزنگاری شده بار دیگر در مقصد به حالت اصلی خود باز گردد. شاید این کار را خود شما نیز در کودکی به صورت غیرحرفه‌ای و بسیار ساده انجام داده باشید.

رمزنگاری تنها به دوره بلاک چین و عصر حاضر محدود نمی‌شود. چرا که هزاران سال پیش نیز مردم از رمزنگاری برای ارسال و دریافت پیام استفاده می‌کردند. در فرایند رمزنگاری، پیام‌ها را به اشکال مختلفی تبدیل می‌کنند که غیرقابل فهم باشند. به این صورت هیچ فردی نمی‌تواند از پیام‌های ارسال شده استفاده کند، مگر این که کلید رمزگشایی آن را در اختیار داشته باشند. رمزنگاری یا کریپتوگرافی به عنوان یکی از اصول اصلی ارزهای دیجیتال محسوب می‌شود.

بدون رمزنگاری رمزارزها نمی‌توانند امنیت چندانی داشته باشند و اطلاعات کاربران برای همه افشا خواهد شد. بدون رمزنگاری دزدی از دارایی‌های افراد در دنیای بلاک چین بسیار ساده خواهد شد. چرا که همه داده‌ها در بلاک چین به صورت شفاف هستند و تنها رمزنگاری است که از اطلاعات کاربران محافظت می‌کند.

رمزنگاری فرایندی است که در آن از پروتکل و الگوریتم‌های مختلف برای رمزگذاری داده‌ها استفاده می‌شود. رمزگذاری یا Encryption اولین مرحله‌ای است که در رمزنگاری انجام می‌شود. در این مرحله داده‌های ساده به شکل غیرقابل فهمی تبدیل می‌شوند. رمزگشایی یا Decryption فرایند عکس رمزگذاری است. در این فرایند داده‌های رمزی دریافت شده با استفاده از الگوریتم در دست به داده‌های ساده اولیه تبدیل می‌شوند.

در طول تاریخ از رمزگذاری برای کارهای مختلفی استفاده شده است. به طور مثال در جنگ‌های جهانی از انواع الگوریتم‌های رمزنگاری برای ارسال و دریافت اطلاعات مهم استفاده می‌شد. در حال حاضر نیز رمزنگاری بخش بزرگی از دنیای ارزهای دیجیتال را به خود اختصاص داده است.

سایفر دیگر بخش مهم رمزنگاری بوده و همان الگوریتمی است که در هنگام رمزنگاری استفاده می‌شود. چرا که بیش از یک راه برای رمزگذاری داده‌ها وجود دارد. افراد، شرکت‌ها و تیم‌های مختلف می‌توانند از روش‌های مختلفی برای رمزگذاری اطلاعات خود استفاده کنند. الگوریتمی که در این فرایند داده ساده را به یک داده غیرقابل فهم تبدیل می‌کند همان سایفر رمزنگاری خواهد بود.

رمزنگاری در دنیای ارز دیجیتال

رمزنگاری در دنیای ارزهای دیجیتال بی شباهت به انواع دیگر رمزنگاری نیست. در این دنیای بزرگ به طور معمول از دو کلید مختلف برای رمزنگاری و رمزگشایی استفاده می‌شود. یکی از اصلی‌ترین تجهیزات مورد نیاز برای فعالیت در دنیای ارزهای دیجیتال، کیف پول دیجیتالی است. کیف پول دیجیتال برای هر فرد دو

کلید تولید می‌کند. شما با ثبت نام در یک کیف پول ارز دیجیتال، کلید خصوصی و کلید عمومی دریافت خواهید کرد. این دو کلید وظیفه حفظ امنیت بلاک چین اطلاعات شما و ارسال یا دریافت پول را بر عهده دارند.

در فرایند ارسال و دریافت داده‌ها در دنیای بلاک چین و در مورد ارزهای دیجیتال فرایند پیچیده‌ای انجام نمی‌شود. کلید عمومی به عنوان آدرس عمومی شما شناخته می‌شود. می‌توانید به این کلید عمومی به عنوان آدرس خانه خود نگاه کنید. این کلید را می‌توان در اختیار همه قرار داد.

آنها با این کلید نمی‌توانند به اطلاعات شما دسترسی داشته باشند. اما در صورتی که بخواهید افراد دیگر به حساب شما پول انتقال دهند، باید این کلید را در اختیار آنها قرار دهید. در طرف مقابل کلید خصوصی را داریم که به معنای کلید خانه شما محسوب می‌شود. این کلید را نباید به افراد دیگری بدهید. چرا که با داشتن کلید خصوصی افراد می‌توانند به دارایی‌های دیجیتال شما دسترسی داشته باشند.

مطلب پیشنهادی : نحوه دسترسی به ولت دیجیتال پس از گم شدن کلید خصوصی

در هنگام ارسال و دریافت داده در دنیای ارز دیجیتال فرایندی به شکل زیر طی می‌شود. شما کلید عمومی خود را در اختیار دوست‌تان قرار می‌دهید. دوست شما با استفاده از کلید عمومی، اطلاعات ارسال را رمزگذاری می‌کند. سپس این داده‌های رمزنگاری شده در دنیای ارز دیجیتال به شما ارسال می‌شود.

افراد دیگر نیز می‌توانند این داده را مشاهده کنند. اما چیزی از آن متوجه نخواهند شد. چرا که تنها ارقام و حروف تصادفی نشان داده می‌شود. شما پس از دریافت پیام می‌توانید پیام را با استفاده از کلید خصوصی‌تان رمزگشایی کنید. هر کلید عمومی به یک کلید خصوصی مربوط می‌شود و بدون در دست داشتن کلید خصوصی نمی‌توان اطلاعات رمزگذاری شده توسط کلید عمومی را رمزگشایی کرد.

الگوریتم رمزنگاری ارزهای دیجیتال

الگوریتم رمزنگاری یکی از مهم‌ترین مولفه‌های برای هر ارز دیجیتال و بلاک چین است. با استفاده از الگوریتم‌های مختلف، ارزهای دیجیتال رمزگذاری می‌شوند. نحوه فعالیت و رمزگذاری هر الگوریتم با الگوریتم‌های دیگر متفاوت بوده و ممکن است مراحل مختلفی در این فرایند طی شود.

در حال حاضر هزاران ارز دیجیتال مختلف وجود دارد. هر ارز دیجیتال نیز می‌تواند بسته به سلیقه سازنده‌اش از یک الگوریتم خاص استفاده کند. هر چند در دنیای ارزهای دیجیتال برخی الگوریتم‌ها بیشتر از بقیه مورد استفاده قرار می‌گیرند. الگوریتم مورد استفاده در مورد یک ارز دیجیتال می‌تواند تاثیر مستقیمی بر امنیت و سختی شبکه بلاک چین آن داشته باشد.

با استفاده از الگوریتم‌ها، هش‌ها با حجم‌های مختلف تولید می‌شوند. وظیفه ماینرهای ارز دیجیتال یا استخراج کنندگان ارز دیجیتال نیز رمزگشایی این هش‌ها است تا بتوانند بلوک جدیدی در بلاک چین به وجود آورند. به طور مثال بلاک چین بیت کوین به عنوان اولین بلاک چین دنیا که امنیت فوق العاده بالایی دارد، از الگوریتم هشینگ SHA-256 استفاده می‌کند. این الگوریتم می‌تواند یک هش 32 بایتی یا 256 بیتی را تولید نماید. به خاطر استفاده ارزهای دیجیتال مختلف از کد اصلی بیت کوین آنها نیز به اجبار از این الگوریتم رمزنگاری استفاده می‌کنند. این مورد برای ارزهای دیجیتال مختلف می‌تواند متفاوت باشد. به طور مثال ارز دیجیتال دوج کوین از الگوریتم رمزنگاری اسکریپت یا Scrypt استفاده می‌نماید.
الگوریتم محبوب دیگر در دنیای ارز دیجیتال کریپتونایت یا Cryptonight است که در ارزهای دیجیتالی مانند و دش کوین ستفاده می‌شود. در حال حاضر معروف‌ترین الگوریتم‌های استفاده شده در دنیای ارز دیجیتال SHA-256، Skein-SHA2، Scrypt، X11، SHA-256d و NeoScrypt هستند. هر کدام از این الگوریتم‌ها فرایند خاصی را برای تبدیل داده ساده به یک داده رمزنگاری شده طی می‌کنند.