خلاصه مباحث پروژه تحقیق پیرامون
سیستم پول دیجیتال

درس: مبانی رمزنگاری، خانم دکتر زیبا اسلامی

سجاد رنجبر یزدی

نیم‌سال اول 1403-1404

بشر موجودی اجتماعی است و برای بسیاری از امور زندگی و خود نیازمند تعامل با سایر انسان‌ها می‌باشد. یکی از اصلی‌ترین لازمه‌های زندگی اجتماعی، داد و ستد است. این امر موجب شده است تا انسان‌ها از همان ابتدای شکل‌گیری تمدن‌های نخستین، به دنبال راهکارهای متفاوتی به منظور داد و ستد با یکدیگر باشند. علم به عنوان زبان مشترک بین تمامی انسان‌های هوشمند، سراسر زندگی ما را از روز نخست تا کنون دچار تحول کرده است. فرآیندهای داد و ستد نیز از این قاعده جا نمانده و شاهد تحولات بسیار زیادی بوده‌اند. این پیشرفت‌ها و تحولات سرعت بسیار زیادی در عصر کنونی یافته‌اند. برای درک این موضوع کافی است نگاهی به رود این پیشرفت‌ها بیاندازیم. سکه‌های گران‌بها برای هزاران سال ابزار اصلی داد و ستد ما بوده‌اند. پس از چندین هزاره ما توانستیم با پیشرفت‌های صورت گرفته در صنعت چاپ، نخستین اسکناس‌ها را چاپ کنیم. پس از این اسکناس‌ها کمتر از یک صده طول کشید تا کارت‌های اعتباری تبدیل به اساس معاملات روزانه ما شوند. در نهایت ظرف مدت زمانی در حدود یک دهه، ما وارد دنیای پول‌های دیجیتال و رمز ارزها شدیم. این امر نشان میدهد که سرعت پیشرفت‌های این حوزه تا چه اندازه بالاست و ممکن است تا پنج سال آینده تفاوت‌های شگرفی با زندگی کنونی ما داشته باشد. لذا می‌توان برای مطالعه این حوزه اهمیت بسیار زیادی قائل شد. در ادامه با کانسپت Digital cash به عنوان لبه کنونی علم در فرآیندهای داد و ستد آشنا خواهیم شد.

سیستم پول دیجیتال

نیاکان ما برای هزاران سال از سیستم‌های پولی فیزیکی(مانند فلزات ارزشمند، انواع سکه‌ها و اسکناس) استفاده کرده‌اند. کمی کمتر از دو دهه است که به لطف پیشرفت‌های وسیع علم، ما توانسته‌ایم به سیستمی نوین تحت عنوان سیستم پول دیجیتال دست پیدا کنیم.

همانطور که میدانیم، برای ضرب هر سکه یا چاپ هر اسکناس، نیازمند صرف منابع مالی و زمانی متعددی هستیم. اما سیستم پول دیجیتال به ما این امکان را داده است تا با هزینه‌ای بسیار کمتر قادر به ساخت پول باشیم. اما از طرفی بر خلاف اسکناس‌های فیزیکی، جعل پول دیجیتال می‌تواند از پیچیدگی و دشواری کمتری روی کاغذ برخوردار باشد.(از نظر دسترسی به تکنولوژی لازم) در نتیجه در نظر داشتن ملاحظات امنیتی دارای اهمیت بسیار زیادی می‌باشد.

اگر فرآیندهای معامله در این سیستم را به صورت چندین سناریو در نظر بگیریم، بازیگران این سناریو سه عنصر بانک، خرج‌کننده بازرگان خواهند بود. در برخی موارد ممکن است با حضور مهاجم نیز مواجه باشیم که در قسمت‌های اولیه از توصیف آن صرف نظر کرده و در قسمت کنترل خطا و سنجش تقلب به آن می‌پردازیم. در ابتدا لازم است تا عناصر این سناریو را مورد بررسی قرار دهیم. پیش از آن تنظیمات اولیه سیستم را بررسی می‌کنیم.

مقداردهی اولیه یا initialization:

این فرآیند تنها یک مرتبه توسط ارگان‌های شاخص انجام شده و پس از آن برای کلیه فرآیندها استفاده می‌شود. در این مرحله ابتدا یک عدد اول بزرگ مانده p به صورتی که q=(p-1)/2 نیز اول باشد انتخاب می‌شود. مرحله بعد یافتن عدد g به صورتی که مربع یک ریشه اولیه در مد p باشد است. حال می‌توا گفت:

$$g^{k_1} \equiv g^{k_2} (mod\ p) \Leftrightarrow k_1 \equiv k_2\ (mod\ q)$$

به کمک این دو مقدار می‌توان g را به دو متغیر دیگر با نام‌های g_1 و g_2 بسط داد. در نهایت تنها لازم است تا دو تابع هش تعریف کنیم. این توابع با فرمت زیر همل می‌کنند.

H(5 tuple) -> int in mod q

H0(4 tuple) -> int in mod q

کلیه توابع و اعداد تعریف شده در این قسمت به صورت عمومی در اختیار عناصر سیستم قرار دارند. با استفاده از این تنظیمات اولیه، سایر ارکان قابل تعریف هستند.

بانک

بانک را می‌وان به عنوان موسسه‌ای دارای مجوز از بانک مرکزی پول‌های الکترونیک(Central Bank of Digital Cash) جهت دریافت سپرده‌ها معرفی کرد. اگرچه چرخ اقتصادی اغلب بانک‌ها از طریق وام‌ها میگردد، در این پژوهش به مقوله وام نمی‌پردازیم. به صورت کلی این بانک‌های در سیستم پول دیجیتال دارای چهار نقش می‌باشند.

1. **صدور پول:** پول نقد دیجیتال را با ارزهای دیجیتال بانک مرکزی (CBDC) یا به عنوان پول دیجیتال خصوصی(برای اشخاص خرج‌کننده) مانند استیبل کوین صادر می کند.
2. **تأیید تراکنش‌ها:** صحت تراکنش های دیجیتال را برای جلوگیری از تقلب و جعل تأیید می کند.
3. **امنیت تراکنش‌ها:** از اقدامات رمزنگاری برای ایمن کردن تراکنش‌ها و جلوگیری از دسترسی غیرمجاز یا مسائل مربوط به هزینه مضاعف استفاده می‌کند.
4. **مقررات جهانی:** به عنوان یک تنظیم کننده عمل کرده و انطباق با هنجارهای ضد پولشویی (AML) و احراز هویت(KYC) را بررسی می‌کند.

خرج کننده و بازرگان

خرج کننده و بازرگان دو بازیگر اساسی در این سیستم می‌باشند. خرج کننده به کمک بانک پول لازم جهت شارژ صندوق سپرده پول دیجیتال خود را ایجاد می‌کند. از طرفی او می‌تواند در ازای دریافت خدمات یا کالا از بازرگان، این پول‌ها به او بدهد. بازرگان نیز از اعتبار پول دریافتی اطمینان حاصل کرده و آن را به حساب بانکی خود واریز می‌کند.

پیش از هر چیز لازم است تا این عناصر در سیستم ثبت و شناخته شوند. هر سه عنصر دارای دو کد معرف که به کمک اعداد اول بزرگ ساخته می‌شوند شناخته می‌شوند. یکی از این کدها عمومی بوده و دیگری به صورت کاملا خصوصی برا صرفا به منظور تایید صحت تراکنش‌ها ساخته می‌شود.

بانک یک شناسه هویتی رندوم مانند x را انتخاب کرده و مقدار زیر را محاسبه می‌کند:

$$h \equiv g^{x} \ (mod\ p)$$

در اینجا شماره h عمومی شده و بانک را مشخص می کند. خرج کننده نیز یک شماره هویت مخفی u را انتخاب کرده و شماره حساب را به صورت زیر محاسبه می کند:

$$I \equiv g_1^{u} \ (mod\ p)$$

خرج کننده می‌تواند با ارسال این شناسه عمومی در بانک حساب افتتاح کند. از این مقدار جهت کلیه تراکنش‌ها استفاده خواهد کرد. بازرگان نیز در این سیستم تنها از شناسه عمومی M استفاده می‌کند. بازم به ذکر است که افراد می‌توانند با هر دو نقش مذکور در این سیستم فعالیت کنند.

ساخت پول دیجیتال

فرآیند ساخت پول دیجیتال سناریویی است که میان بانک و خرج‌کننده صورت می‌گیرد. این سناریو نهایتا منجر به تولید دنباله شش تایی به صورت (A, B, z, a, b, r) شده که بیانگر یک کوین می‌باشد. یک سکه برای معتبر بودن باید باید توسط بانک و خرج‌کننده معتبر تولید شده باشد. در غیر این صورت قابل استفاده در سیستم نبوده و توسط روش‌های کنترل تقلب از ورود آن به سیستم جلوگیری می‌شود. فرآیند ساخت سکه شامل محاسبات زیادی است که برای مشاهده آنها می‌توانید به اسلایدها مراجعه کنید.

خرج کردن پول دیجیتال

همانطور که گفته شد، فرد خرج‌کننده در ازای دریافت خدمات یا کالا می‌تواند صورت حساب را به کمک پول‌های دیجیتال خود به بازرگان پرداخت کند. در این تراکنش بازرگان می‌تواند اعتبار سکه را بررسی کرده و در صورت صحت آن را قبول کند. در این تراکنش ممکن است تقلب‌های متنوعی صورت پذیرد که در قسمت کنترل تقلب راهکارهای مقابله با آنها را بررسی خواهیم کرد.

واریز پول دیجیتال به بانک

همانطور که گفته شد پول دیجیتال به کمک تاپل شش تایی (A, B, z, a, b, r) ساخته می‌شود. لذا بازرگان پس از دریافت پول از خرج‌کننده می‌بایست (A, B, z, a, b, r) را به بانک ارائه دهد. اما برای واریز علاوه بر این شش تایی، یک تاپل سه تایی (r_1, r_2, t) را نیز به بانک ارسال می‌کند. این متغیرها در زمان دریافت پول از خرج‌کننده محاسبه شده‌اند و می‌توانید آنها را در اسلایدها مشاهده کنید.

پس از ارسال این دو تاپل به بانک، صحت تراکنش و تکراری نبودن سکه بررسی می‌شود. همچنین تعلق سکه به بازرگان مورد بررسی قرار می‌گیرد. اگر مشکلی در میان نباشد بانک سکه را قبول کرده و اعتبار بازرگان افزایش می‌یابد. بازرگان می‌تواند از این سکه به عنوان یک خرج‌کننده استفاده کرده و آن را به بازرگانی دیگر دهد.

کنترل تقلب

پیشگیری از فعالیت‌های خصمانه و ارائه راهکارهای مقابله با سوء استفاده افراد منفعت‌طلب، از اهمیت بسیار زیادی در سیستم‌های بانکی مالی برخوردار است. به صورت کلی دو نکته اساسی در رابطه با کنترل تقلب در سیستم پول‌های الکترونیکی وجود دارد. نخست، هرگونه فعالیت خصمانه بسیار دشوار یا غیر ممکن بوده و دوم در صورت رخداد قابل رصد و پیگیری باشد.

در این تحقیق به پنج تقلب رایج پرداخته و راهکارهای در نظر گرفته شده را بررسی میکنیم. این پنج تقلب عبارتند از:

1. **پرداخت تکراری:** ممکن است یک پرداخت کننده یک سکه مشخص را به دو بازرگان متفاوت پرداخت کند. در این حالت می‌توان با انجام محاسبات مذکور در ارائه، پرداخت‌کننده خاطی را پیدا کرد.
2. **ثبت سکه تکراری:** ممکن است یک بازرگان سکه دریافتی از پرداخت‌کننده را بیش از یک بار در بانک ثبت نماید. همانطور که دیدیم، سکه‌ها با تاپل‌های شش تایی تعریف شده و اگر بازرگان تاپلی تکراری ثبت نماید به راحتی قابل پیگیری است. تنها را ممکن ارسال سه تایی جدیدی با فرمت (r1, r2, d) است. در این حالت پیدا کردن سه‌تایی که در معادله $g_1^{r'1} g_2^{r'2} \equiv A^{d'}B \pmod p$ صدق کند بسیار دشوار و عملا غیر ممکن است.
3. **ثبت سکه بی‌هویت:** امکان دارد شخصی بخواهد سکه‌ای بدون هویت یا جعلی ثبت نماید. با توجه به معادلات مذکور در قسمت ساخت سکه و مسئله لگاریتم گسسته این عمل بسیار دشوار و عملا غیر ممکن است.
4. **جعل سکه توسط کارمندان بانک:** ممکن است یکی از افراد داخل بانک با توجه به دانش و دسترسی‌هایش بخواهد اقدام به جعل سکه نماید. بنا بر توضیحات ارائه شده این امر تنها در حالتی که متغیر رندوم s برابر 0 باشد ممکن است. لذا در قسمت ساخت سکه شرط نا صفر بودن را برای این مقدار لحاظ کردیم.
5. **سکه دزدیده شود**: اگر شخصی اقدام به دزدیدن سکه نماید با توجه به عدم دسترسی به شناسه u نمی‌تواند آن را خرج کند.

البته اقدامات خصمانه و تقلب‌های بسیار زیاد دیگری نیز وجود دارند که در اینجا مجال کافی برای بیان و بررسی تمام آنها وجود ندارد.

بیت‌کوین و ارزهای دیجیتال

بیت‌کوین یک ارز دیجیتال غیرمتمرکز است که در سال ۲۰۰۸ توسط فرد یا گروهی با نام مستعار ساتوشی ناکاموتو معرفی شد. این ارز از فناوری بلاکچین استفاده می‌کند، که یک دفتر کل توزیع‌شده و شفاف است. در بیت‌کوین، تراکنش‌ها بدون نیاز به واسطه (مثل بانک‌ها) انجام می‌شوند و با استفاده از فناوری‌های رمزنگاری مانند کلید عمومی و خصوصی و امضای دیجیتال ایمن می‌شوند.

ویژگی‌های اصلی بیت‌کوین:

1. **غیرمتمرکز بودن:** تحت کنترل هیچ نهاد مرکزی نیست.
2. **عرضه محدود:** تنها ۲۱ میلیون بیت‌کوین وجود خواهد داشت.
3. **امنیت:** از (Proof-of-Work) و توابع هش برای حفظ امنیت و جلوگیری از تقلب استفاده می‌شود.
4. **تراکنش‌های شفاف:** همه تراکنش‌ها در بلاکچین ثبت می‌شوند و برای همه قابل مشاهده هستند، اما هویت افراد ناشناس باقی می‌ماند.

این سیستم، پایه و اساس بسیاری از ارزهای دیجیتال دیگر و فناوری‌های مرتبط است. در نهایت به مثالی از نحوه انجام یک تراکنش با بیت کوین پرداختیم که جزئیات آن در اسلایدها قابل مشاهده است. نمونه ساده‌ای از فرآیندهای گفته شده در این تحقیق با زبان پایتون پیاده‌سازی شده‌اند که می‌توانید سورس آن را از طریق این لینک بررسی کنید.