

ذخیره‌سازی و نگهداری رمزپول‌ها با کیف‌های دیجیتال

محمد بابک^{۱*}

امیر مسعود سعادت‌مند^۲

محمد رضا مرادی^۳

تاریخ پذیرش: ۱۳۹۹/۱۲/۲۶

تاریخ ارسال: ۱۳۹۹/۰۳/۰۲

چکیده

رمزپول‌ها به‌عنوان یکی از محصولات فناوری بلاک چین دارای چالش‌های راهبردی زیادی همچون نگهداری و ذخیره‌سازی هستند که به دغدغه‌ای برای فعالان این عرصه تبدیل شده که می‌تواند دارای کاربران و امنیت سرمایه‌گذاران را تهدید کند. ذخیره‌سازی این رمزپول‌ها غالباً از طریق ابزارهایی با نام کیف پول دیجیتال صورت می‌گیرد که انواع و اقسام مختلفی دارد؛ لذا هدف این تحقیق شناخت ویژگی‌های انواع کیف پول دیجیتال با توجه به نوع نیاز کاربران جهت مدیریت بهتر رمزپول‌ها است.

روش تحقیق از نوع توصیفی-پیمایشی بوده و داده‌های پژوهش با ابزار پرسشنامه جمع‌آوری شده و پاسخ‌ها طبقه‌بندی شده در طیف لیکرت از یک تا پنج می‌باشد. جامعه آماری، خبرگانی هستند که در زمینه بلاک چین و رمزپول‌ها در دانشگاه‌ها، بانک‌ها و پژوهشکده‌ها فعالیت داشته‌اند این افراد با توجه به تازگی موضوع رمزپول‌ها به‌خصوص بخش کیف پول دیجیتال، بسیار محدود بوده و محقق موفق به شناسایی ۲۰ نفر شد؛ بدین ترتیب حجم نمونه همان ۲۰ نفر در نظر گرفته شد. جهت روایی پرسشنامه از تأیید نخبگان امر استفاده شده و پایایی آن توسط ضریب آلفای کرونباخ با استفاده از نرم‌افزار SPSS.26 محاسبه گردید.

یافته‌های تحقیق حاکی از آن است که از بین ۵ نوع کیف پول (سخت‌افزاری، تحت وب، موبایلی، دسکتاپ و کاغذی) جهت انتخاب یک کیف پول دیجیتال، داشتن امنیت کیف پول، دسترس‌پذیر بودن، آفلاین یا آنلاین بودن، پشتیبانی از انواع رمزپول‌ها، قیمت کیف پول و هزینه تراکنش‌ها، رابط کاربری و پشتیبان‌گیری از کلیدهای خصوصی از اولویت‌های بالاتری برخوردارند و در پایان نیز روند نمایی برای انتخاب کیف پول مناسب هر فرد ارائه شده است.

واژگان کلیدی: رمزپول، کیف پول دیجیتال، ذخیره‌سازی.

^۱ دانشجوی دکتری مدیریت راهبردی سایبر، دانشکده مدیریت راهبردی، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران. نویسنده مسئول. (m.babak@sndu.ac.ir)

^۲ دانشجوی دکتری مدیریت راهبردی سایبر، دانشکده مدیریت راهبردی، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران. (a.saadatmand@sndu.ac.ir)

^۳ دانشجوی دکتری مدیریت راهبردی سایبر، دانشکده مدیریت راهبردی، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران. (mrmoradi20009@gmail.com)

۱. مقدمه

در حال حاضر در کشور ما به دلیل کم توجهی به خط مشی گذاری، قانون گذاری و برنامه ریزی در فضای مجازی، از فرصت های پیش روی ظرفیت های این فضا به خوبی استفاده نشده و آسیب های ناشی از آن رو به گسترش است. (جمشیدی بروجردی، علیرضا، ۱۳۹۷). رمز پول ها^۱ نیز به عنوان یکی از محصولات فناوری بلاک چین^۲ از این آسیب ها استثنا نبوده و نگهداری و ذخیره سازی آن ها به دغدغه ای برای فعالان این عرصه تبدیل شده است.

فناوری نوظهور بلاک چین و به طور خاص ارزهای دیجیتال یکی از مهم ترین موضوعات در اقتصاد فضای سایبر می باشد. (رجبی، ۱۳۹۷) امروزه بسیاری از کشورهای دنیا برای مسئله ارزهای دیجیتال برنامه ها و طرح های ملی را در دستور کار قرار داده اند. این نوع ارزها از فناوری های رمزنگاری برای انتقال امن در بستر شبکه اینترنت استفاده کرده و لذا امنیت این اطلاعات در حد مطلوبی بوده و دسترسی به آن برای افراد غیرمجاز به سادگی میسر نیست.

رمز پول ها به عنوان بخشی از ارزهای دیجیتال، بر روی زیرساخت های پایگاه داده توزیع شده در محیطی به نام بلاک چین ذخیره و اجرا می شوند. شیوه ذخیره سازی این پول ها در محیط های آفلاین و آنلاین از مسائل مهم و حساس برای توسعه دهندگان آن می باشد. از جمله فرصت های ایجاد شده توسط رمز پول ها می توان به تسهیل مبادلات بی واسطه و کاهش زمان و هزینه انجام تراکنش ها علی الخصوص تراکنش های برون مرزی اشاره کرد. (الوانی و همکاران ۱۳۹۳). استفاده از روش های ذخیره سازی رمز پول ها دارای نقاط قوت و ضعفی بوده و می تواند فرصت ها و تهدیدهایی برای کاربران را به وجود آورد؛ بنابراین شیوه مواجهه و مدیریت ذخیره سازی آن ها از مسائل مهمی است که در باید در دستور کار دولت ها قرار گیرد.

با توجه به حجم بازار مبادلات رمز پول ها در هر کشور و وضعیت اقتصادی آن، ممکن است مخاطراتی برای یک کشور وجود داشته باشد که در کشور دیگر موضوع تهدید آمیزی محسوب نشود؛ بنابراین هر کشور با توجه به شرایط ویژه خود، بایستی تهدیدها را بررسی کرده و میزان خطر آفرینی آن ها را برای سیستم مالی و اقتصادی خود برآورد کند. (محمدی، ۱۳۹۷)

ذخیره سازی این رمز پول ها غالباً از طریق ابزارهایی بانام کیف پول دیجیتال صورت می گیرد البته روش های دیگری چون استفاده از صرافی ها و یا استفاده از قفل زمانی به کمک قراردادهای هوشمند نیز برای ذخیره رمز پول ها استفاده می شود.

^۱ رمز پول، ترجمه صحیح crypto currency بوده که در یک اشتباه رایج به رمزارز ترجمه می شود بنابراین در این تحقیق هر جا واژه رمزارز استفاده شده منظور همان رمز پول است.

^۲ Block chain Technology

کیف پول‌های دیجیتال، طبقه‌بندی‌های مختلفی از جمله سخت‌افزاری- نرم‌افزاری و یا آفلاین- آنلاین دارند که هر نوع این کیف پول‌ها با توجه به روش ذخیره‌سازی آن مزایا و معایبی را در پی خواهند داشت به طوری که شرکت‌های مختلف با توجه به نیاز مشتریان خود طیف وسیعی از این کیف‌ها را تولید و ارائه کرده‌اند علاوه بر آن که شرکت‌های بزرگ همچون سامسونگ، ایچ تی سی و آی بی ام^۱ هم در جدیدترین گوشی‌های هوشمند خود امکان ذخیره‌سازی کلید خصوصی رمزپول‌ها را به محصولات خود اضافه کرده‌اند و یا شرکت سوئیسی فوراند فیلس اقدام به ساخت ساعت‌های مچی مجهز به کیف پول رمزنگاری شده کرده است که از سرویس امنیتی اختصاصی مبتنی بر بلاک چین بهره می‌برد.

امروزه امنیت این کیف پول‌ها و انتخاب بهترین نوع آن، یکی دغدغه دارندگان رمزپول‌ها شده و مسائلی همچون هزینه خرید و نگهداری آن، قابلیت دسترسی سریع و آسان، پشتیبانی کیف از انواع ارزهای دیجیتال، پنهان کردن آدرس آی پی^۲ و قابلیت استفاده در سیستم‌عامل‌های موردنیاز ما در اولویت‌های بعدی قرار گرفته است.

از دیگر مسائلی که در امنیت این کیف‌ها مهم است نوع احراز هویت آن می‌باشد. اکنون ترکیبی از احراز هویت‌های بیومتریک همچون تشخیص امضای حرارتی، سنجش ضربان قلب و اثرانگشت، مورد استفاده قرار می‌گیرد با این حال، تنوع زیاد کیف‌های پول دیجیتال، باعث شده است دارندگان رمزپول‌ها در یک سردرگمی نسبی برای انتخاب کیف پول مناسب خود قرار گیرند چراکه بیم آن می‌رود که رمزپول‌ها، به علت عدم آگاهی صحیح و یا دلایل دیگر از بین رفته و صاحبان آن متضرر شوند ضمن اینکه تاریخ رمزپول‌ها هم پر از نمونه‌های فراوان هک صرافی‌ها و سرقت سرمایه کاربران بوده است همین امر در یک سطح گسترده، می‌تواند زمینه‌ساز نارضایتی مردم، بحران اقتصادی و یا حتی بحران امنیتی شود. بنابراین، نمی‌توان از استقبال عموم مردم و مقبولیت رمزپول‌ها و به خصوص بیت‌کوین در کشور چشم‌پوشی کرد و بایستی هرچه سریع‌تر دستگاه‌های حوزه رگلاتور^۳ پولی کشور، نظر قاطع خود را در این حوزه بیان دارند هرچند که پیش‌نویس ضعیفی در اواخر سال ۱۳۹۷ با عنوان الزامات و ضوابط رمزپول‌ها توسط بانک مرکزی برای بررسی منتقدین منتشر شده است اما این سند پیشنهادی، نواقص زیادی داشته و در آن ویژگی‌های کیف پول مناسب که حافظ منافع ذینفعان باشد به درستی مشخص نیست.

در آینده نزدیک، در کشور ما، مردم برای حفظ دارایی‌های خود و یا سود بیشتر، به سمت رمزپول‌ها خواهند رفت و اخذ یک الگوی مناسب برای ذخیره‌سازی آن‌ها در شبکه بانکی کشور باعث کاهش خطرات منافع عامه و نظارت بیشتر حاکمیت می‌شود و همچنین عدم توجه به آن می‌تواند باعث از بین رفتن سرمایه کاربران و نارضایتی‌های عمومی شود مخصوصاً اینکه یافتن کیف پول امن و معتبر جهت رمزپول‌های جدید به چالشی برای کاربران تازه‌کار تبدیل خواهد شد بنابراین اکنون که شرکت‌هایی همچون تلگرام با انتشار رمزپول گرام،

¹ IBM & HTC & Samsung

² IP

³ Regulation

امنیت ما را هدف قرار داده‌اند باید به گونه‌ای عمل کنیم که از این فناوری برای کاهش مشکلات اقتصادی و محدودیت‌های مقابل کشور استفاده کنیم. لذا ارائه شناخت ذخیره‌سازی رمزپول‌ها در سامانه بانکی و آگاهی بخشی به جامعه مخاطب آن از ضروریات امروز اقتصاد دیجیتال می‌باشد تا بتوان با یک انتخاب مفید و درست، بهترین نگهداری از رمزپول‌های مردم کشور در قبال تمام مخاطرات داخلی و بیرونی صورت گرفته و شاهد کمترین آسیب در این حوزه باشیم مخاطراتی چون پول‌شویی، فرار مالیاتی، خریدوفروش قاچاق، تأمین مالی جرائم و گروه‌های تروریستی و بی‌ثباتی سیستم بانکی کشور که هر کدام به‌تنهایی می‌توانند به دغدغه‌ای فراروی امنیت اقتصادی و نهایتاً امنیت ملی ما تبدیل شوند.

بنابراین با توجه به شیوع استفاده از رمزپول‌ها و همچنین عدم آشنایی کامل با کیف‌های پول دیجیتال و خطرات در کمین نشسته آن‌ها، هدف اصلی این تحقیق شناخت ویژگی‌های یک کیف پول دیجیتال ایده‌آل و مناسب برای هر فرد جهت نگهداری و ذخیره سازی رمزپول‌ها تعریف می‌شود که با کمترین آسیب‌پذیری و بیشترین امنیت همراه باشد.

۲. مبانی نظری پژوهش

۲-۱. ارز دیجیتال، ارز مجازی، رمزارز و رمزپول

فناوری بلاک چین فضایی را برای ما فراهم کرده است که ما می‌توانیم در این فضا مبادلات را ساماندهی کنیم و ابزارهای متعددی خلق کنیم که قابلیت مبادله با هر کالای دیگری را دارند بدون اینکه تأیید بانک مرکزی روی آن باشد و یا اصلاً نیازی به تأیید آن باشد. (رنجبر فلاح، محمدرضا، ۱۳۹۷). ارزهای دیجیتال، ارزهایی هستند که به‌صورت الکترونیکی ذخیره و منتقل می‌شوند. هرگونه پولی که بر مبنای صفر و یک باشد در این تعریف می‌گنجد. مثلاً ریال‌های موجود در حساب بانکی بازنمایی کننده ریال‌های واقعی هستند که جایی نگهداری می‌شوند، در تعریف ارز دیجیتالی جای می‌گیرند (مورهایم، ۲۰۱۹). بیتکوین‌ها همچون مبنای صفر و یک دارند ارز دیجیتالی هستند. در نتیجه از نظر حقوقی عبارت «ارز دیجیتالی» یک عبارت موسع است. (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۹۷)

ارزهای مجازی^۲ گونه‌ای از ارزهای دیجیتالی به شمار می‌آیند، اما هرگونه ارز دیجیتالی^۳ ارز مجازی به شمار نمی‌رود (وگنر، ۲۰۱۸). رمزپول‌هایی مانند بیت‌کوین^۴ نیز گونه‌ای از ارزهای مجازی هستند، اما همه ارزهای مجازی، رمزپول^۵ نیستند.

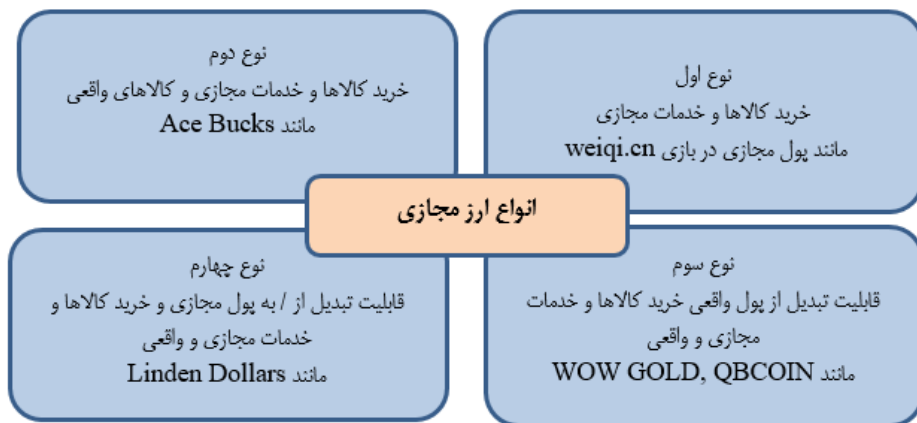
¹ Lisa Morhaim

² Virtual Currency

³ Digital Currency

⁴ Bitcoin

⁵ Cryptocurrency



شکل شماره (۱) انواع ارز مجازی

منبع: مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۹۷

در سال ۲۰۰۹ با ظهور بیت‌کوین نوع جدیدی از ارزهای مجازی به وجود آمدند که با استفاده از الگوریتم‌های رمزنگاری به جای اعتماد به یک واسطه یا شخص ثالث از دفاتر کل توزیع شده استفاده می‌کردند (رجبی، ۱۳۹۳) که به این مدل از ارزهای مجازی، رمزارز می‌گویند. ارزهای مجازی دارای دیجیتالی که برای کارکرد واسطه مبادله طراحی شده و از رمزنگاری برای ایمنی تراکنش‌ها و کنترل خلق واحدهای جدید استفاده می‌کند. (سوویتو و ۲۰۱۸). در واقع رمزپول، ارز دیجیتالی است که به جای اینکه توسط دولت تولید شود توسط یک شبکه عمومی تولید شده است و از رمزنگاری برای حصول اطمینان از ارسال و دریافت پرداخت‌ها استفاده می‌کند. (واژه‌نامه کمبریج، ۲۰۱۷). پیش از سال ۲۰۱۷ و اوایل آن، بیت‌کوین بیش از ۹۰ درصد از سهم بازار رمزارزها را تشکیل می‌داده و بارونق چشمگیر این بازار در سال ۲۰۱۷ و ورود رمزارزهای جدید، این سهم کاهش یافته و به حدود ۵۰ درصد رسیده است. سهم رمزارزهای دیگر به مرور افزایش یافته و تا حدودی تسلط کامل بیت‌کوین را بر این بازار کاهش داده است (نوری، ۱۳۹۷) بیت‌کوین نخستین پول دیجیتال غیرمتمرکز است که پشتوانه و ارزش ذاتی ندارد، در واقع ارزش ذاتی بیت‌کوین مبتنی بر اعتماد و تمایل مردم برای ادامه استفاده از آن است (تپ اسکات^۱، ۲۰۱۶).

رمزپول‌ها نیز ترجمه کریپتوکارنسی^۲ بوده که به اشتباه رایج به رمزارز ترجمه می‌شود و دارای‌های مجازی هستند که برای امنیت آنها از رمزنگاری استفاده شده است و در این تحقیق منظور رمزارز همان رمزپول می‌باشد.

¹ Tapscott

² Crypto Currency

۲-۲. اقتصاد دیجیتال، کیف پول دیجیتال

اقتصاد دیجیتال اقتصادی است که بر پایه تکنولوژی‌های دیجیتالی از جمله شبکه‌های ارتباطی دیجیتالی (اینترنت، اینترنت و شبکه‌های خصوصی ارزش افزوده) کامپیوترها، نرم‌افزار و سایر تکنولوژی‌های اطلاعات مربوطه باشد. اقتصاد دیجیتال بعضی مواقع اقتصاد اینترنتی، اقتصاد جدید یا اقتصاد وب نیز نامیده می‌شود. (نوری و طباطبایی‌نیا، ۱۳۹۸)

کیف پول دیجیتال، کیف پول الکترونیکی یا کیف پول رمزپولی به کیف پولی اطلاق می‌شود که برای نگهداری رمزپول‌ها می‌توان از آن استفاده کرد این کیف پول‌ها انواع و اقسام مختلفی دارند که بنا بر نیاز کاربر می‌توان از نمونه‌های مختلف آن بهره برد. از آنجاکه ارزهای دیجیتال از مجموعه‌ای از کدهای کامپیوتری و ساختاری دیجیتالی تشکیل شده‌اند لذا برای ذخیره، به کارگیری و انجام تراکنش‌ها توسط آن می‌بایست از ابزاری استفاده کرد که کاربر در گام نخست به راحتی بتواند از دارایی دیجیتال خود حفاظت نموده و همچنین از رمزپول‌های موجود در این کیف پول دیجیتال همچون پول نقد برای خرید کالا و خدمات بهره برد. پس با استفاده از کیف پول‌های دیجیتال استفاده‌کنندگان به راحتی و سریع و با یک فناوری ارتباطی، خریدشان را انجام می‌دهند (حاجی ملامیرزایی، ۱۳۹۷).

هر کیف پول ارز دیجیتال، دارای یک کلید خصوصی^۱ و یک کلید عمومی^۲ منحصر به فرد می‌باشد. کلید خصوصی معادل رمز عبور و کلید عمومی به مثابه شماره حساب یا آدرس کیف پول تلقی می‌گردد.

صاحب کیف پول، می‌تواند آدرس عمومی کیف پول را در اختیار اشخاصی که قصد واریز رمزپول به آن حساب را دارند، قرار دهد؛ اما کلید خصوصی کیف پول کاملاً محرمانه است و دسترسی به کلید خصوصی به معنای دسترسی کامل به موجودی حساب است و در صورت فاش شدن این کلید، احتمال سرقت دارایی بسیار زیاد خواهد بود.

به صورت کلی کیف پول بیت‌کوین و سایر رمزپول‌ها به دو نوع سرد و گرم تقسیم می‌شوند (محمدی، ۱۳۹۶).

کیف پول گرم: این اصطلاح به کیف پول‌هایی اطلاق می‌شود که همواره به بستر اینترنت متصل‌اند. این شیوه ذخیره‌سازی ارزهای دیجیتال، دسترسی به دارایی‌ها را از هر نقطه‌ای از گوشه و کنار دنیا امکان‌پذیر می‌سازد؛ اما در عوض احتمال سرقت دارایی دیجیتال توسط هکرها نیز افزایش خواهد یافت.

کیف پول سرد: کیف پول سرد به کیف پولی گفته می‌شود که به صورت مستقیم به اینترنت متصل نیست و تنها جهت جابجایی دارایی دیجیتال لازم است به اینترنت متصل شوید. کیف پول سرد انواع مختلفی دارد. کیف

¹ Private Key

² Public Key

پول کاغذی و کیف پول سخت‌افزاری از این نوع به شمار می‌روند. امنیت در این کیف پول‌ها بسیار بالاست و سازوکار انجام تراکنش در این بستر نسبت به کیف پول‌های گرم دشوارتر است.

فارغ از دسته‌بندی فوق، نوع دیگری از طبقه‌بندی کیف پول‌ها وجود دارد که این کیف پول‌ها را در ۵ دسته مختلف معرفی می‌کند. (حاجی ملامیرزایی، ۱۳۹۸)

۲-۲-۱. کیف پول تحت وب

یکی از انواع کیف پول بیت‌کوین و سایر ارزهای دیجیتال، کیف پول تحت وب است. برای استفاده از این نوع کیف پول کافی است به ثبت‌نام در وبسایت موردنظر اقدام نمود.

از آنجایی که این نوع از کیف پول‌ها نیز در دسته‌ی کیف پول‌های گرم قرار دارند، دارایی کیف پول همیشه در معرض خطر سرقت قرار دارد. نگهداری مبالغ بالا در این کیف پول‌های آنلاین معمولاً کار عاقلانه‌ای نیست.

وبسایت‌های مختلفی وجود دارد که برای نگهداری دارایی دیجیتال، خدمات آنلاین ارائه می‌دهند؛ اما به دلیل تحریم‌های موجود علیه برخی کشورها و گروه‌ها بعضی از این وبسایت‌ها از ارائه خدمات به هم‌وطنان ایرانی ممانعت می‌کنند.

۲-۲-۲. کیف پول موبایلی

بسیاری از کارهایی که پیش‌ازاین تنها توسط کامپیوتر انجام می‌شد امروزه به راحتی در گوشی‌ها و تبلت‌ها قابل انجام است. کیف پول‌هایی که روی تلفن همراه نصب می‌شوند نسبت به سایر کیف پول‌ها از نظر راحتی و سهولت در به‌کارگیری بسیار کاربرپسند بوده و می‌توان در هر مکانی از جمله فروشگاه‌ها، از آن‌ها استفاده نمود.

دسترسی آسان و مدیریت رمزپول‌ها برکنار سهولت در ارسال و دریافت رمزپول‌ها با استفاده از کدها را می‌توان برترین مزایای کیف پول‌های موبایلی دانست. از دست دادن رمزپول‌ها در صورت سرقت، خرابی و از دست دادن گوشی، برکنار خطر حمل دائمی سرمایه را می‌توان به‌عنوان معایب استفاده از کیف پول‌های موبایلی قلمداد کرد.

این دسته از کیف پول‌ها به‌هیچ‌عنوان جزو امن‌ترین کیف پول‌های رمزپولی به شمار نمی‌آیند؛ اما به دلیل اینکه اکثر آن‌ها کلیدهای خصوصی را تنها بر روی گوشی تلفن همراه و آن‌هم به‌صورت رمزنگاری شده ذخیره می‌کنند، از میزان امنیت بسیار بالاتری نسبت به کیف پول‌های تحت وب برخوردار هستند.

برخی از وبسایت‌های معتبر حوزه رمزپول‌های ارائه‌دهنده کیف پول تحت وب، برنامه‌هایی^۱ را نیز برای گوشی‌های هوشمند طراحی کرده‌اند که با استفاده از آن‌ها می‌توانید به کیف پول تحت وب خود دسترسی پیدا نموده و به ارسال و دریافت رمزپول پرداخت.

این برنامه‌ها به‌هیچ‌وجه به‌عنوان یک کیف پول موبایلی واقعی دسته‌بندی نمی‌شوند. چراکه کلیدهای خصوصی به‌جای این‌که بر روی گوشی ذخیره شوند، همچنان در وب ذخیره می‌شوند. اپلیکیشن موبایل این سایت‌ها درواقع تنها ارتباط گوشی با سرورهای آنلاین^۲ را برقرار می‌کند. به‌عنوان مثال اپلیکیشن موبایل وبسایت بلاک چین^۳ یک کیف پول موبایلی واقعی به‌حساب نمی‌آید اما بالاخره این کیف پول هم توسط گوشی همراه قابل‌استفاده است. کیف پول‌های موبایلی نیز از دسته کیف پول‌های گرم به شمار می‌روند. (پرانانو وایکار و همکاران، ۲۰۱۸)

۲-۲-۳. کیف پول دسکتاپ

یکی دیگر از انواع کیف پول بیت‌کوین و دارایی‌های دیجیتال، کیف پول نرم‌افزاری یا کیف پول دسکتاپ است. کسانی که لپ‌تاپ یا کامپیوتر شخصی استفاده می‌کنند، کیف پول دسکتاپ گزینه مناسبی برای ذخیره دارایی دیجیتال خواهد بود. این نوع از کیف پول‌ها همانند یک نرم‌افزار کامپیوتری دانلود و بر روی سیستم نصب خواهد شد.

این کیف پول‌ها از بسیاری از کیف پول‌های تحت وب و کیف پول‌های موبایلی ایمن‌تر می‌باشند، زیرا کلید خصوصی بر روی هارد درایو کامپیوتر خودتان ذخیره و نگهداری می‌شود و این کلید در اختیار هیچ شخص واسط یا سرور دیگری قرار نمی‌گیرد.

البته ویروسی شدن سیستم و یا هک شدن رایانه، خطرانی است که می‌تواند امنیت دارایی دیجیتال را تا اندازه‌ای تهدید کند؛ اما باین‌وجود این کیف پول گزینه‌ی مناسبی برای نگهداری مقادیر کم رمزپول‌ها به شمار می‌رود.

انواع مختلفی از کیف پول دسکتاپ وجود دارد. برخی از آن‌ها روی امنیت، برخی دیگر روی ناشناس بودن و... تمرکز نموده‌اند.

۲-۲-۴. کیف پول سخت‌افزاری

یک کیف پول سخت‌افزاری بهترین و امن‌ترین گونه از انواع کیف پول ارزهای دیجیتال به شمار می‌رود که کلید خصوصی را در یک دستگاه سخت‌افزاری همانند یک فلش مموری نگهداری می‌کند. کیف پول

¹ Application

² Online

³ Blockchain.com

سخت‌افزاری جزو کیف پول‌های سرد طبقه‌بندی می‌شود و تا به امروز هیچ گزارشی مبنی بر سرقت دارایی‌های دیجیتال از این کیف پول‌ها ارائه نشده است (پراناو وایکار و همکاران، ۲۰۱۸).

علاوه‌براین، کیف پول سخت‌افزاری در برابر ویروس‌های کامپیوتری مصون بوده و موجودی درون آن نمی‌تواند از طریق سرقت کلید خصوصی ربوده شود. استفاده از این کیف پول‌ها برخلاف سایر کیف پول‌های معرفی شده رایگان نمی‌باشند و برای تهیه این دستگاه‌ها می‌بایست هزینه‌ای را پرداخت کنید. کیف پول‌های سخت‌افزاری ترکیبی بهینه از ایمنی و سادگی را به کاربر ارائه می‌دهند. تنها محدودیت آن‌ها این است که برای ارسال رمزپول‌ها، همیشه باید این کیف پول‌ها را به همراه داشته باشید.

۲-۲-۵. کیف پول کاغذی

یک کیف پول کاغذی صرفاً یک برگه کاغذ است که کلید عمومی و کلید خصوصی کیف پول بر روی آن نوشته شده است. این کیف پول همانند پول نقد تا زمانی که در اختیار صاحب آن قرار داشته و آسیب‌ندیده باشد کاملاً امن است. کیف پول‌های کاغذی نیز نوعی کیف پول سرد (آفلاین)^۱ به شمار می‌روند.

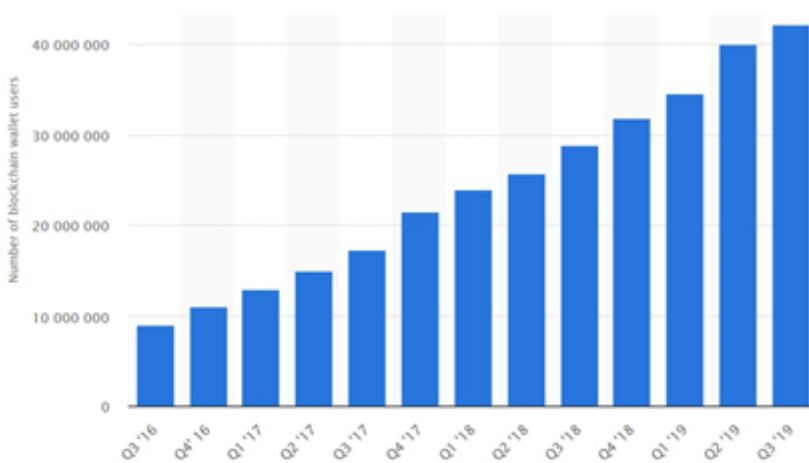
کلیدهای عمومی و خصوصی این برگه کاغذ معمولاً به شکل یک کد ترسیم می‌شود تا بتوان به سرعت از طریق اسکنرها آن را اسکن کرد و موجودی را به یک کیف پول نرم‌افزاری انتقال داده و تراکنش را انجام داد.

مزیت اصلی کیف پول‌های کاغذی، عدم ذخیره‌سازی کلیدها در فضای دیجیتال و آنلاین است. به این ترتیب خطر هک شدن و به سرقت رفتن کلید خصوصی از طریق بدافزارها و هرگونه دزدی از طریق فضای دیجیتال تقریباً برابر صفر است. با این وجود، برای ساخت کیف پول کاغذی نیز باید اقداماتی امنیتی را رعایت کرد.

کلید خصوصی روی یک کاغذ چاپ می‌شود و هرکس این کاغذ را داشته باشد می‌تواند همه موجودی آن را خالی کند؛ بنابراین در صورت از بین رفتن، گم شدن یا دزدیده شدن آن تکه کاغذ، همه موجودی دیجیتالی که ذخیره کرده‌اید از بین خواهد رفت و به هیچ‌عنوان امکان بازیابی آن وجود نخواهد داشت. (پراناو وایکار و همکاران، ۲۰۱۸)

^۱ Offline

نمودار زیر تعداد استفاده کنندگان از کیف پول های رمز پول در بستر بلاک چین را در کل دنیا نشان می دهد.



نمودار شماره (۱) تعداد کیف های رمز پول تا سال ۲۰۱۹

Source: statista.com

۲-۲-۶. کیف پول بومی

این کیف پول می تواند فقط رمز پول ملی را پشتیبانی کند و یا با رمز پول های دیگر در ارتباط باشد و می بایست به گونه ای توسعه داده شود که کنترل کامل بر روی آن داشته باشیم. برای مثال قابلیت اعمال محدودیت، مدیریت، دریافت، انتقال و ذخیره هر رمز پول از طریق کیف پول امکان پذیر است و کیف پول ملی می تواند کمک بزرگی در این امر باشد. کیف پول به حاکمیت این امکان را می دهد تا رمز پول ها را مدیریت کند، نکته مهم اینجاست که رقیب کیف پول های رمز پول ملی کیف پول های دیگر هستند و باید شرایطی پیش آید که کیف پول ملی برای رمز پول ها استفاده شود (حاجی ملامیرزایی، ۱۳۹۸)

با توجه به شرایط کشور ما در رابطه با تحریم ها، استفاده از کیف پول بومی در اولویت قرار می گیرد و در همین راستا دو پیام رسان داخلی اقدام به ارائه کیف پول ارز دیجیتال نموده اند. انتشار ارز دیجیتال توسط اپلیکیشن های پیام رسان، پدیده جدیدی نیست. تلگرام نخستین پیام رسانی است که به فکر طراحی یک شبکه مستقل و انتشار ارز دیجیتال ویژه خود بانام «گرام» افتاد. پس از تلگرام نیز فیس بوک و واتس اپ به این جریان پیوست. اما در حوزه داخل، ابتدا گپسی به عنوان ارز رمزنگاری شده پیام رسان گپ ارائه شده که برای پرداخت و تبادلات مالی در زمان تحریم با توجه به عدم ردیابی تراکنش ها یک فرصت برای کشور است. این کیف پول مبتنی بر فناوری بلاک چین از ارزهای رمزنگار پشتیبانی می کند و دارای رمز پول پایه گپسی با پشتوانه ریال به عنوان

یک استیبل کوین^۱ (ارزهای دیجیتالی که قیمت ثابتی دارند) است؛ این کیف پول قابلیت پشتیبانی از تعداد زیادی واحد پولی و برخورداری از ۱۲۰ درگاه پرداخت دارد که باعث شده تا زیرساخت بی نظیری برای فعالیت‌های مالی در بستر پیام‌رسان گپ وجود داشته باشد و بتوان از روش‌های مختلف کیف پول را شارژ و از آن برای پرداخت استفاده کرد.

دومین پیام‌رسانی داخلی که به عرصه کیف پول رمزپول پا گذاشته است پیام‌رسان بله است. این پیام‌رسان کیف پول ارز دیجیتال «پیمان» را ارائه داده که با پشتوانه طلا بوده و از سوی کنسرسیوم ققنوس صادر می‌شود. این کنسرسیوم با همکاری چهار بانک داخلی و همچنین چند شرکت و استارت‌آپ شکل گرفته و در مراسمی اولین توکن خود با پشتوانه طلا را عرضه کرده و قرار است یک میلیارد ارز دیجیتال خود بانام پیمان را با پشتوانه طلا صادر کند.

۳-۲. پیشینه تحقیق

امروزه استفاده از کیف پول دیجیتال در دنیا روندی صعودی دارد، یک روش پرداخت آسان و با ریسک پایین. کیف پول رمزپول‌ها نیز با تولد بیت‌کوین به‌عنوان اولین رمزپول، در سال ۲۰۰۹ استفاده شده است. مسلماً اولین کیف پول رمزپول از نوع کاغذی بوده و فقط به‌صورت یادداشتی برای کلید عمومی و کلید خصوصی بوده است اما امروزه این کیف پول‌ها انواع، طبقه‌بندی و اقسام گوناگونی دارند که هر کدام دارای قابلیت‌هایی بیش از نگهداری کلیدها است.

در بررسی‌های پیشینه‌های به‌عمل‌آمده مشخص شد که در داخل کشور مقاله، کتاب و یا اسناد منتشر شده که صرفاً در حوزه کیف‌های رمزپول باشد، وجود ندارد و بیشتر در کنار توضیح مبانی رمزپول‌ها به فرصت‌ها و تهدیدهای آن پرداخته و درنهایت شاید به آشنایی مختصر با انواع کیف پول پرداخته شده است. در کتاب پول مجازی پس از توضیحاتی در مورد اکوسیستم پول‌های مجازی و انواع کیف پول ارزهای دیجیتال و کاربردهای آن، به شرح فرآیند تراکنش‌ها از منظر کاربر و از دید فنی پرداخته است سپس مبانی فقهی رمزپول‌ها را موشکافی کرده و درنهایت وضعیت موجود آن‌ها را در کشورهای پیشرو تبیین نموده است.

سیستم الکترونیکی کیف پول به کاربر اجازه می‌دهد تا با قدرت کامل بر روی ارزهای خود مدیریت کند. در این مقاله پس از اشاره به الگوریتم‌های استخراج^۲ رمزپول و رمزنگاری کلید عمومی و خصوصی چنین آمده است نیازمندی یک معامله یا ارز مبادله بدون نیاز به نقطه مرکزی وجود دارد. ما یک رمزنگاری از ابتدا ایجاد کرده‌ایم که می‌تواند با استفاده از کیف پول الکترونیکی کنترل شود. (پراناو وایکار و همکاران، ۲۰۱۸)

^۱ Stable coin

^۲ به طور کلی ماینینگ فرآیندی است که در آن تراکنش‌ها مورد تایید قرار می‌گیرند؛ با این فرآیند بلاک جدیدی که متشکل از تعدادی تراکنش است به زنجیره بلاک‌های پیشین افزوده و به سبب آن کوین‌های جدیدی ایجاد می‌شود (نوری و نجفی، زیر چاپ)

ارزش بیت کوین به طور مداوم تغییر می کند و مانند سهام در مبادلات مختلف معامله می شود. بیت کوین ها با استفاده از کیف پول ذخیره می شود. بیت کوین ها، مزایایی چون آزادی پرداخت، کنترل و امنیت، اطلاعات شفاف و معیایی مانند از بین رفتن کیف پول ها دارند همچنین تهدیدات امنیتی مانند حمله به کیف پول ها متصور است. امروزه پنج نوع اصلی از کیف پول مانند کیف پول دسکتاپ، کیف پول موبایل، کیف پول وب، کیف پول کاغذی و کیف پول های سخت افزاری وجود دارد که هر کدام دارای خواص و ویژگی هایی با توجه به جامعه هدف خود می باشند (آرچانا ناوارا، ۲۰۱۶) و هر کس با توجه به نوع نیاز خود می تواند کیف پول مناسب را انتخاب کرده و به تعادلی بین امنیت، هزینه و سایر مشخصات کیف پول برسد لیکن امنیت همیشه بالاترین اولویت را در تبادلات مالی به خود اختصاص داده است به طور مثال در سال ۲۰۱۳، یک مرد بریتانیایی یک هارد دیسک سخت حاوی کلیدی برای باز کردن ۷۵۰۰ بیت کوین خود، با ارزش ۷٫۵ میلیون دلار در آن زمان را برای همیشه از دست داد و همچنین در ۲۰۱۴ از کیف پول های صرافی ام تی گاس^۱ در ژاپن مبلغ ۳۵۰ میلیون دلار بیت کوین به سرقت رفت. در این تحقیق عنوان شده که کاربران باید مسئولیت نگهداشتن بیت کوین خود را در کیف های مجازی بر روی هارد دیسک خود را بپذیرند چرا که اگر رایانه دارای اتصال به اینترنت باشد هکرها می توانند به کیف پول کاربر دسترسی داشته باشند. (راجی لطیفا و همکاران، ۲۰۱۷)

ارائه دهندگان کیف پول از بازیگران کلیدی این عرصه هستند چرا که یک کلید رمزنگاری شده کاربر را نگهداری می کنند لذا برای توانمندسازی کیف پول ها پیشنهاد می شود که یک پایگاه داده مرکزی جهت ثبت نام هویت کاربران و آدرس های کیف پول با قابلیت دسترسی برای نیروهای پلیس ملی راه اندازی شود. (رابی هوبن، ۲۰۲۰)

در یک تحقیق مرجع دیگری با عنوان رمز پول جهانی در دانشگاه کمبریج انجام شده است این مرکز از طریق مصاحبه های امن وب، چهار نظرسنجی آنلاین را از سپتامبر ۲۰۱۶ تا ژانویه ۲۰۱۷ انجام داد. هر نظرسنجی به سازمان ها و افراد در بخش خاصی از صنعت رمز پول توسط سیستم طبقه بندی ها (به ویژه مبادلات، کیف پول، ارائه دهندگان خدمات و استخراج کنندگان) ارسال شده است. شرکت ها و سازمان های رمز پولی در ۳۸ کشور و پنج منطقه جهان در یک یا چند مورد از چهار نظرسنجی بخش مبادلات، کیف پول ها، پرداخت ها و معدن شرکت کردند. در بخش دیگری از این تحقیق، کیف پول ها را به دسته های کیف پول شامل نرم افزار و یا سخت افزاری، کیف پول نگهدارنده / نگهدارنده، کیف پول خود میزبان، کیف پول بزرگ / کوچک و کیف پول با مبادله یکپارچه تقسیم بندی کرده است سپس آمار کاملی از چگونگی پراکندگی کیف ها در سراسر جهان، درصد کیف پول های مجوز دار، درصد کیف های منبع باز و بسته و همچنین تعداد کیف پول های فعال ارائه داده و ویژگی های هر کدام از آن را به طور مشروح توضیح داده است. (گاریک هیلمن و میشل راجز، ۲۰۱۷)

¹ Mt.Gox

۳. روش شناسی پژوهش

روش بکار رفته برای این پژوهش از نوع توصیفی - پیمایشی است. داده‌های پژوهش با حضور در جامعه و یا نمونه آماری با ابزار پرسشنامه جمع‌آوری می‌گردد. پرسشنامه یکی از ابزارهای رایج و روشی مستقیم برای کسب داده‌های پژوهش است. پرسشنامه‌ی این تحقیق خود شامل دو بخش می‌باشد که حاوی سؤالاتی نظیر مشخصات شخصی پاسخگویان از قبیل جنسیت، سطح تحصیلات و تجربه استفاده و نیز سؤالات مرتبط با عنوان پژوهش می‌باشد. سؤالات مورد استفاده در پرسشنامه با مطالعه منابع موجود داخلی و خارجی در خصوص ویژگی‌های کیف پول به دست آمده و سپس با نظر خبرگان و کارشناسان مربوطه تکمیل و تغییر یافت. برای هر پرسش تعدادی گزینه و پاسخ انتخاب شده است که فرد پاسخ‌دهنده باید یکی از آن‌ها را به‌عنوان پاسخ انتخاب نماید. پاسخ‌ها طبقه‌بندی شده در طیف لیکرت از یک تا پنج می‌باشد.

جامعه آماری موردنظر این پژوهش، خبرگانی هستند که در مقوله موضوع موردپژوهش، از اطلاعات و تجارب کافی برخوردار می‌باشند. این افراد کسانی هستند که در زمینه بلاک چین و رمپول‌ها در دانشگاه‌ها، مؤسسات آموزش عالی، پژوهشکده‌ها و مؤسسات علمی کشور فعالیت داشته و در مسئولیت‌های اجرایی کشور دارای تجارب عملی بوده و یا در مراکز تصمیم‌گیری کلان کشور قرار داشته و در این زمینه مسئولیت داشته‌اند. این افراد با توجه به جدید بودن موضوع رمپول‌ها به‌خصوص کیف پول این حوزه، بسیار محدود بوده و محقق موفق به شناسایی ۲۰ نفر شد؛ بدین ترتیب حجم نمونه نیز همان ۲۰ نفر در نظر گرفته شد.

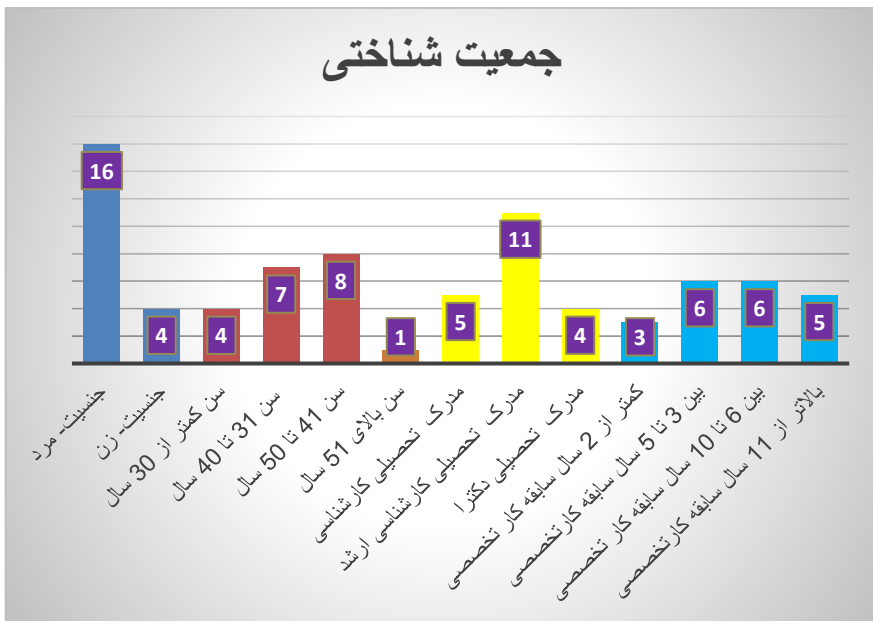
در این پژوهش برای تعیین روایی پرسشنامه از روش خبرگی بهره گرفته شده است. بدین ترتیب که نگاهت اول در جمع خبرگی متشکل از اعضای کارگروه حوزه بلاک چین و رمپول و با نظر آن‌ها اصلاحات لازم در پرسشنامه اعمال گردید

برای تعیین پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شده است که مشهورترین ضریب اعتبار از طریق یکبار اجرای آزمون می‌باشد. با توجه به واریانس هریک از متغیرها، ضریب آلفای کرونباخ با استفاده از نرم‌افزار اس پی اس^۱ ۲۶ محاسبه گردید و پایایی سؤالات پرسشنامه با ضریب ۰/۸۱، تأیید گردید که نشان دهنده همگون بودن مناسب گویه‌ها با یکدیگر به منظور سنجش متغیر هدف است.

۴. تجزیه و تحلیل داده‌ها و یافته‌های پژوهش

همان‌طور که بیان گردید در پژوهش حاضر از پرسشنامه بهره گرفته شد و بر اساس تعداد ۲۰ پرسشنامه تکمیل شده توسط خبرگان سایبری و کارشناسان حوزه بلاک چین و رمپول، تحلیل آماری نتایج صورت گرفت. در نتیجه آمار جمعیت شناختی نمونه آماری و پاسخ‌گویان به تحقیق به‌صورت زیر بوده است.

^۱ SPSS 26



نمودار شماره (۲) جمعیت شناختی جامعه هدف

در دنیای امروز هرروزه بر تنوع ارزهای دیجیتال افزوده می شود و با توجه به اینکه این ارزها زیر نظر هیچ دولت، نهاد و سازمانی نمی باشند، رعایت نکات ایمنی برای حفظ آن ها ضروری است. بدون شک بهترین و امن ترین راه برای نگهداری از ارزهای دیجیتال کیف پول رمزپول است چرا که همیشه صرافای ها هدف خوبی برای هکرها بوده و اخبار زیادی در نفوذ هکرها و سرقت دارایی های آنان وجود دارد.

کیف پول الکترونیک^۱، دستگاه الکترونیکی یا خدمات آنلاین است که امکان تراکنش های آنلاین را برای افراد فراهم می کند. کیف پول الکترونیک می تواند شامل آیتم های خرید از فروشگاه آنلاین توسط رایانه یا تلفن همراه هوشمند^۲ باشد. همچنین، می توان حساب بانکی را به کیف پول الکترونیکی متصل کرد. مدارک شناسایی از قبیل گواهینامه رانندگی، کارت سلامت و کارت های امتیاز الکترونیکی نیز می توانند به کیف پول الکترونیکی متصل شوند اما کیف پول رمزپول^۳ یا کیف رمزنگاری، نوعی کیف پول الکترونیکی است که در آن کلیدهای خصوصی برای رمزپول هایی مانند بیت کوین تعبیه شده است.

¹ e-wallet یا Digital wallet

² Smart Phone

³ Crypto currency wallet

کیف پول رمزپول، درست مثل حساب بانکی است که برای ذخیره، دریافت و ارسال رمزپول به سایر حساب‌های کیف پول یا برای خرید استفاده می‌شود. چه برای تجارت و چه به‌عنوان ذخیره دارایی خود، باید از یک حساب کیف پول استفاده کرد.

نگهداری، استخراج و خریدوفروش رمزپول‌ها در هر کشوری دارای قوانین مختلفی است بنابراین، هنگام انتخاب کیف پول دیجیتال، باید مراقبت لازم را به خرج داد. چراکه اگر یک کیف پول رمزپول به‌اشتباه انتخاب شود، ممکن است تمام دارای فرد از دست برود و اگر ابتدا برای درک تفاوت بین کیف پول‌های مختلف، دقت کافی صرف شود، باعث محافظت در برابر کلاهبرداری و تقلب و همچنین سهولت در تراکنش‌های رمزپول خواهد شد.

در این تحقیق مهم‌ترین پارامترهای انتخاب یک کیف پول جهت ذخیره‌سازی رمزپول‌ها از بررسی مقالات و منابع معتبر به‌دست‌آمده و سپس به کمک پرسشنامه نیز اولویت هر کدام برای جامعه هدف مشخص گردید. این پارامترها به‌قرار زیر است:

پشتیبانی از انواع رمزپول‌ها:

قبل از تهیه کیف پول دیجیتال باید از پشتیبانی نوع رمزپول موردنیاز توسط کیف پول مطمئن شویم. در گذشته هر کیف پول فقط یک نوع رمزپول را پشتیبانی می‌کرد و با بلاک چین آن سازگاری داشت اما امروزه کیف پول‌های دیجیتالی وجود دارد که می‌تواند صدها رمزپول را در خود ذخیره کند و نیاز نیست برای ذخیره یک رمزپول خاص کیف پول جدیدی تهیه شود و یا کیف پول‌های سخت‌افزاری وجود دارد که از بیشتر آنان پشتیبانی می‌کنند یعنی با بیش از هزار نوع رمزپول سازگاری دارند

دسترس پذیر بودن کیف پول‌ها:

در دسترس بودن یک کیف پول از مواردی است که نمی‌توان اهمیت آن را انکار کرد. اخیراً شرکت تلگرام رمزپول جدید خود بانام گرام را ارائه کرده است اما این رمزپول برای ایران و چند کشور دیگر ممنوع اعلام‌شده است به‌غیر از آن چندین تولیدکننده کیف پول رمزپول با گسترش تحریم‌ها به کاربران برخی کشورهای خود ضرب‌الاجلی برای خارج کردن دارایی‌های خود داده‌اند بنابراین دسترسی به کیف پول‌های نرم‌افزاری بر روی گوشی‌های هوشمند، رایانه‌های خانگی و یا اینکه تحت چه سیستم‌عاملی پشتیبانی شود (اندروید، ویندوز، آی او اس، مک و لینوکس) از دیگر نکات مهم در انتخاب یک کیف پول مناسب است

امنیت کیف پول‌ها:

ویژگی غیرمتمركز بودن فناوری بلاک چین باعث شده است که همه سازندگان انواع کیف پول‌ها، مسئولیت مدیریت و حفظ امنیت حساب‌ها را بر عهده خود کاربر گذارند و در ابتدای ساخت هر کیف پول، شرکت‌ها اعلام می‌دارند که توانایی بازیابی دارایی‌ها را نخواهند داشت و کمکی از جانب آنان برای باز نشایی دارایی‌ها بر

نخواهد آمد؛ بنابراین در صورت گم شدن اطلاعات ورود، ممکن است کاربر دیگر نتواند به ارزهای خود دسترسی پیدا کند.

نگهداری و انتقال رمزپول‌ها، با نگهداری پول در حساب‌های بانکی و استفاده از خدمات مؤسسات مالی متفاوت است. رمزپول‌ها کاملاً دیجیتالی هستند و ماهیت فیزیکی ندارد و هرکس به‌طور مستقیم و روی کیف پول، دارایی‌های خود را کنترل می‌کند. به‌عبارت دیگر، دارنده کیف پول مالک حقیقی رمزپول‌ها است و به جز او، سازمانی مثل بانک، نقشی در نگهداری از دارایی‌ها ایفا نخواهد کرد. از این رو، نگهداری و تأمین امنیت رمزپول‌ها باید در اولویت اول قرار گیرد. کیف پول‌های سرد^۱ معمولاً بهترین مکان برای نگهداری امن ارزهای دیجیتال هستند. این امنیت از آن جهت تأمین می‌شود که فضایی که کلید خصوصی در آن ذخیره شده، به‌صورت فیزیکی در اختیار کار برقرار دارد. این کیف پول‌ها در خصوص سرمایه‌گذاری‌های بلندمدت و سنگین، بهترین گزینه به‌حساب می‌آیند. کیف پول‌های سخت‌افزاری و کیف پول‌های کاغذی از نوع سرد هستند که غالب آن‌ها از متدهای رمزنگاری و امنیتی در ساختار خود استفاده می‌کنند و همچنین در برخی از آنان از سامانه‌های تأیید هویت چندمرحله‌ای به‌وسیله ابزارهای سخت‌افزاری برای احراز هویت صاحب کیف پول استفاده می‌شود که می‌تواند امنیت آن را بسیار بالا ببرد.

قیمت کیف پول‌ها و هزینه های تراکنش:

هزینه کیف پول دیجیتال از مواردی است که در انتخاب نوع کیف پول برای بسیاری از کاربران اهمیت بالایی دارد اگرچه بیشتر کیف‌های پول رمزپولی رایگان و بدون هزینه در اختیار کاربران قرار می‌گیرد اما هستند کیف پول‌هایی که کاربر برای استفاده از آن بایستی هزینه پرداخت کند به‌طور مثال کیف پول‌های سخت‌افزاری باقیمت حدود یک‌صد دلار قابل دسترسی می‌باشد و یا اینکه کیف پول‌ها همراه با یک تجهیز جانبی دیگر باشد مثلاً اخیراً یک شرکت سوئیسی اقدام به ارائه ساعت‌هایی باقابلیت ذخیره رمزپول‌ها باقیمت بیش از ده هزار دلار نموده است و یا اینکه برخی گوشی‌های تلفن همراه نیز قابلیت ذخیره‌سازی رمزپول‌ها را به‌صورت سخت‌افزاری دارند.

در مواردی نیز بآنکه خود شرکت ارائه‌دهنده کیف پول برای ارائه‌ی خدمات هیچ کارمزدی دریافت نمی‌کند، اما صرافی‌ها برای ارائه‌ی خدمات به کاربران، کارمزدهای مخصوص به خودشان را به تراکنش اضافه می‌کنند و یا اینکه برخی از آنان جهت ذخیره رمزپول، درصد کمی از همان رمزپول را داخل کیف به‌طور ثابت نگهداری می‌کنند که قابل برداشت و یا انتقال نیست بنابراین انتخاب اولیه یک کیف پول با توجه به نوع رمزپول و یا هدف خرید آنان می‌تواند برای جلوگیری از متضرر شدن کاربران حائز اهمیت باشد.

^۱ Cold wallet

رابط کاربری کیف پول‌ها:

از دیگر ویژگی‌های یک کیف پول مناسب، استفاده‌ی آسان و رابط کاربری ساده می‌باشد تا برای هرکسی و با هر دانشی به راحتی قابل استفاده بوده و از پیچیدگی‌ها به دور باشد بنابراین رابط کاربری یک کیف پول باید به گونه‌ای باشد که حتی بی تجربه‌ترین کاربران و آنانی که با رمزپول آشنایی زیادی ندارند نیز به راحتی و بدون هیچ نگرانی بتوانند با این برنامه‌ها به مبادله رمزپول بپردازند.

شرکت‌های سازنده کیف پول دیجیتال بایستی شفافیت خود را تثبیت کرده و اگر برای کاربری مشکلی پیش بیاید، کاربر بتواند مشکل خود را به راحتی با شرکت در میان بگذارد و آن شرکت‌ها نیز با احترام متقابل به مشتری خود در جهت رفع نیازهای آنان اقدام نمایند.

پشتیبان گیری از کلیدهای خصوصی کیف پول‌ها:

یکی از ویژگی‌های یک کیف پول مناسب، پشتیبان گیری از کلیدهای خصوصی یک کاربر است زیرا در دنیای رمزپول‌ها به دلیل ویژگی‌های بلاک چین، در صورت مفقود شدن کلیدهای خصوصی رمزپول، دارایی‌ها دیگر قابل دسترسی نیستند و به هیچ عنوان امکان دسترسی به سرمایه مربوطه میسر نیست بنابراین داشتن نسخه پشتیبان از این کلیدها بسیار حائز اهمیت است و کیف پول‌هایی هستند که به صورت خودکار اقدام به این کار می‌کنند و در محل‌هایی که کاربر برای آن مشخص کرده کلیدهای خصوصی را ذخیره می‌کنند این محل‌ها ممکن است حافظه‌های داخلی و یا جانبی رایانه‌ها، تلفن همراه و یا حتی به صورت چاپ بر روی کاغذ باشد.

پشتیبانی از زبان‌های مختلف:

پشتیبانی از زبان‌های مختلف یک کیف پول می‌تواند برای انتخاب آن جهت ذخیره‌سازی رمزپول‌ها اهمیت داشته باشد. اگرچه این اهمیت از درجه بالایی برخوردار نیست ولی شرکت‌های ارائه‌دهنده کیف پول جهت کاربری آسان و نفوذ در همه کشورها، اقدام به تولید کیف پول با زبان‌های مختلف هر کشور کرده‌اند و اکنون کیف‌های سخت‌افزاری زیادی وجود دارند که علاوه بر پشتیبانی از زبان انگلیسی از زبان‌های روسی، چینی و ... حمایت می‌کنند.

پشتیبانی از سیستم‌عامل‌ها و پلتفرم‌های مختلف:

دسترسی به یک رمزپول در سکوه‌های نرم‌افزاری مختلف و سیستم‌عامل‌های موجود، همواره مورد توجه کاربران کیف پول‌ها بوده است لذا آگاهی از پشتیبانی پلتفرم‌های مختلف کیف پول می‌تواند ما را در رساندن به آنچه دقیقاً نیاز داریم کمک کند زیرا برای بسیاری از کاربران دسترسی به دارایی‌های خود از طریق سیستم‌عامل‌های اندروید، مکینتاش، ویندوز، بلک بری و یا لینکوس از اهمیت بالایی برخوردار است بنابراین شرکت‌های کیف پول معتبر سعی در ارائه خدمات خود بر روی انواع پلتفرم‌ها کرده و با راه‌اندازی اپلیکیشن‌های مخصوص به خود به دنبال جذب مشتری هستند زیرا امروزه کیف پول‌هایی که فقط در یک سیستم‌عامل کار می‌کنند جایگاه خود را در ذخیره‌سازی رمزپول‌ها از دست خواهند داد.

متن باز بودن کیف پول:

برخی کیف پول ها از ساختار متن باز استفاده می کنند متن باز بودن یعنی کدهای آن موجود بوده و کاربران می توانند آن ها را مشاهده و کپی کنند و امکان دسترسی و دست کاری آن ها نیز وجود دارد. متن باز بودن به معنای آن است که کاربر کنترل بهتری بر حریم شخصی، سرمایه ها و امنیت آن دارد.

برنامه های متن باز معمولاً به صورت مداوم توسط جامعه برنامه نویسان آن به روزرسانی می شود و یا در صورتی که کاربر اطلاعاتی در خصوص برنامه نویسی بلاک چین داشته باشد، می تواند نسبت به نیاز و سلیقه خود، آن را دست کاری کند بنابراین متن باز بودن یک کیف پول همیشه به عنوان یک مزایا در نظر گرفته می شود.

آفلاین یا آنلاین بودن کیف پول:

در مقابل کیف پول های سرد، انواع داغ آن ها وجود دارد. علت این نام گذاری لزوم وجود اتصال به اینترنت برای دسترسی به آن هاست. کیف پول های موبایل، تحت وب و دستکاپ از نوع کیف پول داغ هستند. داغ بودن کیف پول لزوماً به این معنی نیست که کلیدهای خصوصی روی فضای اینترنت نگهداری می شوند، بلکه به معنی امکان ارتباط کلیدهای خصوصی با فضای آنلاین است.

کیف پول های تحت وب در پوشش یک وبسایت فعالیت می کنند. دسترسی به این کیف پول، تنها از طریق اتصال به اینترنت امکان پذیر است. این کیف پول ها در بستری آنلاین اجرا می شوند و می توان از آن ها با هر دستگاهی و در هر جایی به کیف پول خود دسترسی پیدا کنید. با وجود اینکه، دسترسی به این کیف پول ها راحت است، اما کلیدهای خصوصی در فضای آنلاین تبادل می گردند

کیف پول های موبایل اغلب «سرویس گیرنده های لایت» نامیده می شوند، زیرا برای اجرای آن ها نیازی به دانلود کل بلاک چین نخواهید داشت. در عوض، برای دریافت اطلاعات دقیق در مورد وضعیت کنونی شبکه، به ماینرها یا نودها متکی هستند. این نوع کیف پول ها بهترین گزینه برای استفاده آنلاین هستند، زیرا هر زمان که به اینترنت دسترسی داشته باشید می توانید به رمزپول هایتان دسترسی پیدا کنید ولی با کیف پول های سرد همچون کیف های سخت افزاری و کاغذی، محدودیت در دسترسی وجود دارد.

۵. نتیجه گیری

اگرچه بیش از ده سال از ظهور رمزپول ها در دنیا می گذرد اما ذخیره سازی رمزپول ها بحث جدیدی است که در کشور ما و حتی در دنیا، کمتر به آن پرداخته شده است. دو راه کلی برای ذخیره سازی رمزپول وجود دارد؛ یکی استفاده از صرافی های مخصوص و دیگری استفاده از کیف پول های رمزپولی.

در صورتی که دارندگان ارزهای دیجیتال به صرافی‌های رمزیولی اطمینان داشته و یا بتوانند یک صرافی مطمئن پیدا کنند قادر خواهند بود رمزیول‌های خود را در آن نگهداری کنند لیکن صرافی‌ها همیشه هدف خوبی برای هکرها بوده و هستند و همیشه خبرهایی مبنی بر سرقت رمزیول از صرافی‌ها به چشم می‌خورد به‌طور مثال در سال ۲۰۱۹ از یک صرافی در ژاپن ۳۲ میلیون دلار انواع رمزیول به سرقت رفت که ۲۳ میلیون دلار آن متعلق به مشتریان خود بوده و یا در سال ۲۰۱۸ از یک صرافی دیگر ۵۲۰ میلیون دلار رمزیول به سرقت رفت بنابراین استفاده از کیف پول دیجیتال بهترین راه ذخیره‌سازی رمزیول‌ها خواهد بود. این کیف پول‌ها انواع و اقسام مختلفی دارند و بسته به نیاز کاربران متفاوت می‌باشند. در یک طبقه‌بندی کلی کیف پول‌های رمزیولی به دو بخش سرد و گرم تقسیم می‌شوند؛ کیف پول‌های سرد^۱ بهترین مکان برای نگهداری امن سرمایه‌های دیجیتال هستند. این امنیت از آن جهت تأمین می‌شود که فضایی که کلید خصوصی ذخیره‌شده به‌صورت فیزیکی در اختیار کار برقرار دارند. این کیف پول‌ها در خصوص سرمایه‌گذاری‌های بلندمدت و سنگین، بهترین گزینه به‌حساب می‌آیند. کیف پول‌های سخت‌افزاری و کیف پول‌های کاغذی از نوع سرد هستند.

در مقابل کیف پول‌های سرد، انواع کیف پول گرم^۲ وجود دارد. علت این نام‌گذاری لزوم وجود اتصال به اینترنت برای دسترسی به آن‌هاست. کیف پول‌های موبایل، تحت وب و دسکتاپ از نوع کیف پول داغ هستند. گرم بودن کیف پول لزوماً به این معنی نیست که کلیدهای خصوصی روی فضای اینترنت نگهداری می‌شوند، بلکه به معنی امکان دستیابی به کلیدهای خصوصی با فضای آنلاین است. کیف پول‌های داغ برای استفاده روزمره، انجام معامله و سرمایه‌گذاری‌های کوچک یا متوسط گزینه خوبی هستند اما به‌طور کلی کیف پول‌های سرد از کیف پول‌های داغ امنیت بیشتری دارند اما این بدان معنی نیست که کیف پول‌های داغ امن نیستند.

با توجه به یافته‌های تحقیق درمی‌یابیم که در جهت انتخاب یک کیف پول مناسب برای ذخیره رمزیول‌ها طبق اولویت‌های جدول ذیل عمل می‌کنیم.

جدول شماره (۱) اولویت‌های انتخاب کیف‌های پول دیجیتال

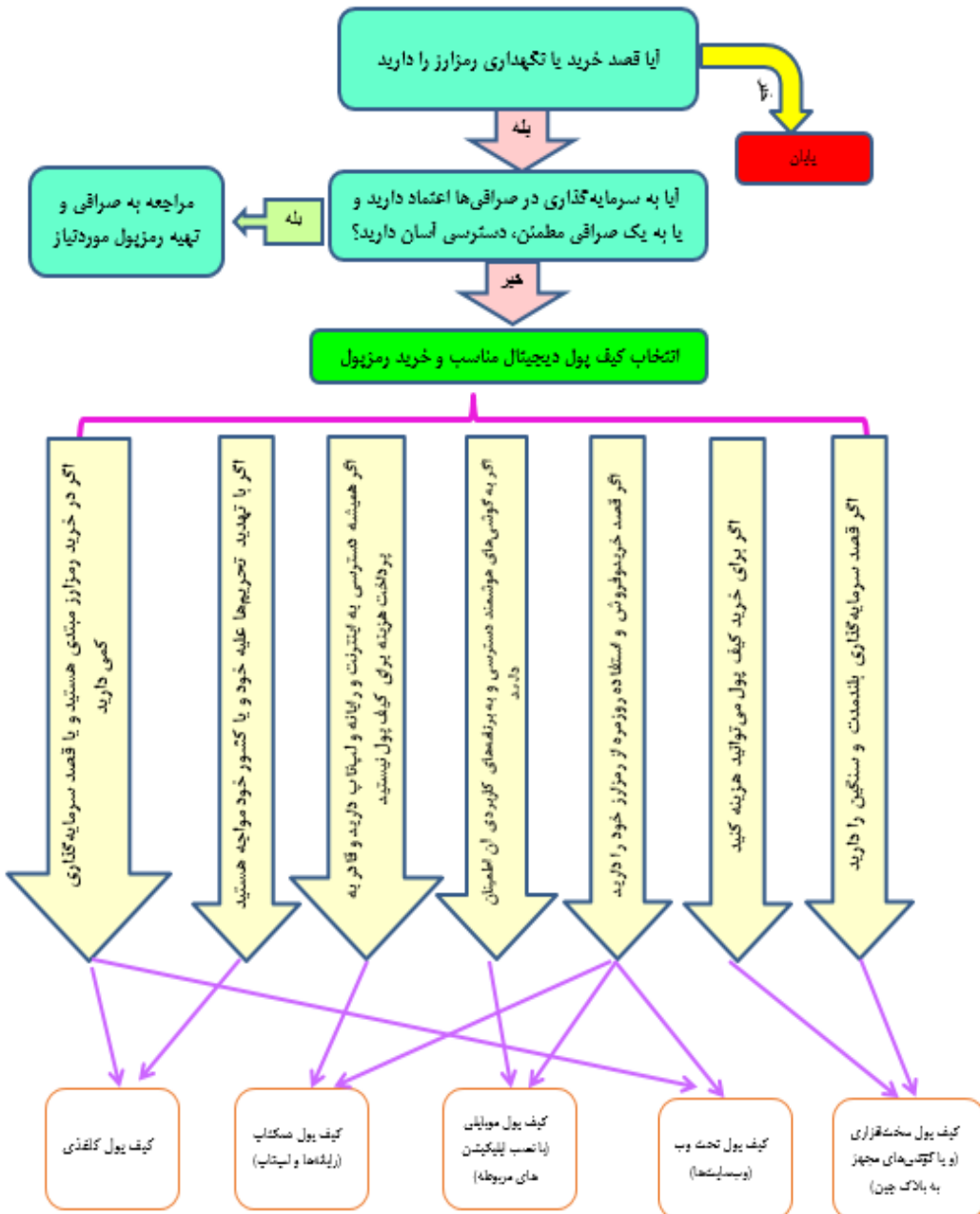
اولویت	ویژگی کیف پول	توضیحات
۱	امنیت کیف پول	امنیت بالاترین اولویت در دارایی‌های دیجیتال به‌خصوص رمزیول‌ها دارد
۲	دسترس‌پذیر بودن کیف پول	دسترسی به کیف پول با توجه به وجود تحریم‌های مختلف علیه کشور ما باید مدنظر قرار گیرد
۳	آفلاین یا آنلاین بودن کیف پول	هدف از ذخیره‌سازی رمزیول (سرمایه‌گذاری بلندمدت یا خریدوفروش آن) در انتخاب آنلاین یا آفلاین بودن کیف پول حائز اهمیت است.

¹ Cold Wallets

² Hot Wallets

اولویت	ویژگی کیف پول	توضیحات
۴	پشتیبانی از انواع رمزپول ها	با توجه به تکرر رمزپول ها، استفاده از کیف پولی که چندین نوع رمزپول را ذخیره کند برای کاربران دارای اولویت است
۵	قیمت کیف پول و هزینه تراکنش ها	کیف پول های سخت افزاری و برخی از کیف پول های نرم افزاری فقط با پرداخت هزینه قابل دسترسی هستند ضمن اینکه برخی کیف پول ها جهت انجام تراکنش هزینه دریافت کرده و یا بخشی از رمزپول داخل خود را بلوکه می کنند
۶	رابط کاربری کیف پول	دوری از پیچیدگی و راحت بودن کار با کیف پول های دیجیتال می تواند کاربران را در جهت استفاده از آن ترغیب کند
۷	پشتیبان گیری از کلیدهای خصوصی کیف پول ها	در صورت مفقود شدن کلید خصوصی رمزپول امکان دسترسی به دارایی ها وجود ندارد
۸	پشتیبانی از سیستم عامل ها و پلتفرم های مختلف	امکان دسترسی به کیف پول در سیستم عامل های مختلف و به کمک برنامه های کاربردی آنان می تواند حائز اهمیت باشد
۹	متن باز بودن کیف پول	متن باز بودن یک کیف پول دیجیتال یعنی شفافیت و امنیت بیشتر
۱۰	پشتیبانی از زبان های مختلف	کاربران کشورهای مختلف تمایل به استفاده از کیف پولی با پشتیبانی از زبان کشور خود دارند.

در شکل زیر یک روندنما، جهت خرید و نگهداری رمزیول‌ها ارائه می‌شود.



شکل شماره (۲) روند خرید و نگهداری رمزیول‌ها

منابع و مأخذ

منابع فارسی

- الوانی، سید مهدی؛ خنیفر، حسین و حاجی ملامیرزایی، حامد (۱۳۹۳). تدوین الگوی خطمشی گذاری فضای مجازی کشور، فصلنامه راهبرد اجتماعی فرهنگی، دوره ۴، شماره ۱۳، ۹۳، ص ۷۵-۱۰۰.
- جمشیدی بروجردی، علیرضا (۱۳۹۷). طراحی چهارچوب مفهومی خطمشی‌های تنظیمی در حوزه محتوای فضای مجازی جمهوری اسلامی ایران، فصلنامه علمی پژوهشی سیاست‌گذاری عمومی، دوره ۴، شماره ۱، ص ۹۹-۱۲۵.
- حاجی ملامیرزایی، حامد. (۱۳۹۸). پول مجازی. تهران: انتشارات دانشگاه عالی دفاع ملی.
- خوشبخت، سعید (۱۳۹۶). پیشنهاد مدل رگلاتوری رمزیول در کشور با توجه به رویکرد رگلاتوری جهانی، بانک داری الکترونیک و نظام‌های پرداخت.
- رجبی، ابوالقاسم (۱۳۹۷). فناوری دفاتر کل توزیع‌شده فراتر از فناوری زنجیره بلوکی، مرکز پژوهش‌های مجلس شورای اسلامی.
- رنجبر فلاح، محمدرضا. (۱۳۹۷). ایجاد پول دیجیتال اکومانی مبتنی بر فناوری زنجیره بلوک براساس پیمان چندجانبه پولی منطقه‌ای. فصلنامه اقتصاد دفاع. سال ۳، شماره ۷، ص ۹۳-۱۰۵.
- محمدی، جعفر. (۱۳۹۷). زنجیره بلوکی؛ چالش‌ها و فرصت‌ها، مرکز تحقیقات راهبردی دفاعی.
- مرادی، محمدعلی و هدایتی، محمدرضا. (۱۳۹۷). طراحی مدل تکاملی گذار ایران به اقتصاد دیجیتال، پژوهشنامه اقتصادی، دوره ۱۸، شماره ۶۸، ص ۲۱۹-۲۵۶.
- مرکز پژوهش‌های مجلس شورای اسلامی، (۱۳۹۷). ارز مجازی: قانون‌گذاری در کشورهای مختلف و پیشنهادها برای ایران.
- میرزاخانی، رضا. (۱۳۹۶) بیت‌کوین و ماهیت مالی- فقهی پول مجازی- مرکز پژوهش، توسعه و مطالعات اسلامی.
- نوری، مهدی و نجفی جزه، حامد. (زیر چاپ). بررسی سیاست‌گذاری ماینینگ رمزیول‌ها در اقتصاد ایران. در حال چاپ.
- نوری، مهدی (۱۳۹۷). تحلیل ماهیت پولی رمزارزها در اقتصاد؛ با تأکید بر مقایسه نوسانات رمزارزهای منتخب با نوسانات یورو- دلار و طلا. فصلنامه اقتصاد دفاع. دوره ۳، شماره ۱۰، ص ۱۰۹-۱۳۰.
- نوری، مهدی و طباطبایی‌نیا، سید بهزاد. (۱۳۹۸). عوامل مؤثر بر رشد اقتصاد دیجیتال، فرصت‌ها و تهدیدات آن و راهبردهای مناسب جمهوری اسلامی ایران در قبال آن. فصلنامه اقتصاد دفاع. دوره ۴، شماره ۱۱، ص ۱۱۷-۱۴۷.

منابع لاتین:

- Archana Navara. (2016) Money in the digital age: what role for central banks? - Bank for International Settlements -House of Finance, Goethe University -Frankfurt,
- Dr Garrick Hileman & Michel Rauchs. (2018). GLOBAL Cryptocurrency Benchmarking Study. University of Cambridge.
- Er-raji latifa. (2017). Blockchain: bitcoin wallet cryptography security, challenges and countermeasures. Journal of Internet Banking and Commerce.
- Everette J, Kyle Bartrem (2019). Cryptocurrency as a Payment Method. Analytic exchange program.
- Hanna Hałaburda. (2019). Central Bank Digital Currencies: A Framework for Assessing Why and How- SSRN Electronic Journal- The Bank of Canada.
- Helms, Kevin. Venezuela Will Pre-Mine Its Cryptocurrency Petro and Launch in 6 Weeks. venezuela-pre-mine-petro-launch/. (2018).
- Lisa Morhaim. Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond. (2019)
- Michael Casey. (2018). The Impact of Blockchain Technology on Finance: A Catalyst for Change- International Center for Monetary and Banking Studies (ICMB).
- Pranav Waikar, Pratik Deshmukh, Rohan Patel, Aditi Kulkarni, Sudam Pawa. (2018). A Survey on Blockchain based Cryptocurrency & an e-Wallet. International Journal of Innovative Research in Science, Engineering and Technology
- Prof. Dr. Robby HOUBEN, Alexander SNYERS. (2020). Cryptocurrencies and blockchain. Policy Department for Economic, Scientific and Quality of Life Policies.
- Tapscott, D. and A. Tapscott, (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.: Penguin.

An Introduction to Various Types of E-wallets for the Storage of Cryptocurrencies

Mohammad Babak^{*1}

Amir Masoud Saadatmand²

Mohammad Reza Moradi³

Abstract

Strategic challenges facing blockchain technology in general _and therefore, products that utilize this technology such as cryptocurrencies_ include issues relating to maintenance and storage which poses some concerns for activists in the field in terms of the security of assets and investors identity. Cryptocurrencies are often done stored through tools called digital wallets. The purpose of the present paper is to identify the various types of digital wallets and specify their characteristics according to user needs, so that they can better manage their cryptocurrencies.

This paper can be categorized as a descriptive-survey. The data were collected through obtaining answers to a questionnaire, and thereafter, the answers were classified in the Likert range from one to five. The statistical population include experts working in universities, banks, and research institutes who actively use the blockchain and cryptocurrencies technologies. Considering the novelty of cryptocurrencies, and especially digital wallets, the researcher was only able to base his study on a sample volume of 20. The validity of the questionnaire was confirmed by experts in the field, and its reliability was confirmed through obtaining the Cronbach's alpha coefficient using the spss26 software.

The findings show in choosing a digital wallet out of the 5 available types (hardware, web, mobile, desktop and paper, the security of the wallet, its availability, offline or online features, support for a variety of cryptocurrencies, the price of the wallet and the cost of transactions, user interface and the backing of private keys are highly prioritized by the users. The paper ends with a flowchart in order to help the user choose the appropriate wallet for based on their needs.

Keywords: cryptocurrency, digital wallets, storage.

¹ PhD Student in Cyber Strategic Management, Faculty of Strategic Management, USupreme National Defense University, Tehran, Iran. Author. (m.babak@sndu.ac.ir).

² PhD Student in Cyber Strategic Management, Faculty of Strategic Management, Supreme National Defense University, Tehran, Iran. (a.saadatmand@sndu.ac.ir).

³ PhD Student in Cyber Strategic Management, Faculty of Strategic Management, Supreme National Defense University, Tehran, Iran. (mrmoradi20009@gmail.com).