فن آوری زنجیره الواح و پول های رمزی:
یک برداشت فرگشتی از پول و سیستم های پرداخت

احمد رضا جلالی نایینی

موسسه عالی آموزش و پژوهش مدیریت و برنامه ریزی و پژوهشکده پولی و بانکی

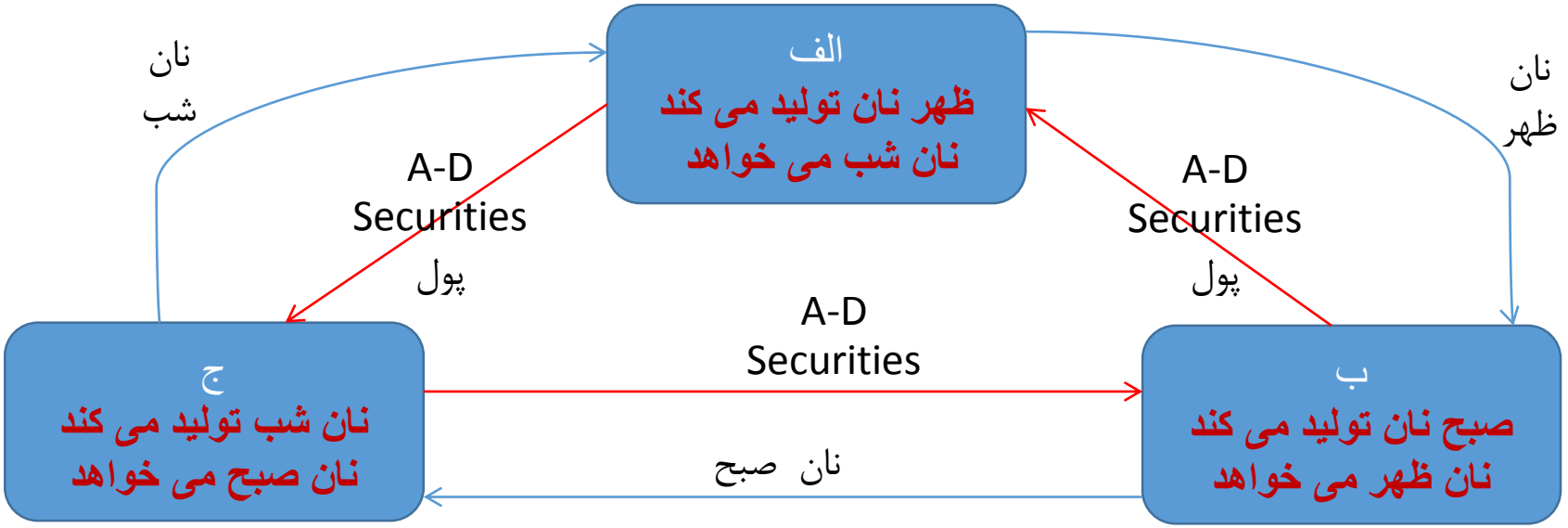
دی ماه ۱۳۹۵

نحوه مبادله کالا، ابزار مبادله و سازوکار پرداخت در طول تاریخ دستخوش تحولات زیادی بوده است: مبادله مستقیم هدیه و تهاتر؛ مبادله غیر مستقیم: پول کالایی، اعتبار، پول فرمانی، پول (اعتبار) بانکی؛ سیستم های پرداخت با واسطه بانکی؛ پول الکترونیک؛ پول های رمزی و سیستم پرداخت غیرمتمرکز.

- محرک اصلی تغییرات فوق، ملاحظات و انگیزه های اقتصادی (کارآیی، هزینه و منفعت) بوده اند. این ملاحظات هم در واکنش به تغییرات ساختارهای اقتصادی-اجتماعی در فرآیند تحول بوده است. بعضا نیز تغییرات در نحوه مبادله و مکانیسم های پرداخت خود عاملی تاثیرگذار و مشوق تغییر در ساختارها بوده است.
- از ابتدای شکل گیری اجتماعات بشری تا به امروز حجم قابل توجهی از مبادلات اقتصادی به صورت مبادله مستقیم (Direct Exchange) بوده، هر چند با گسترش جوامع و تخصصی شدن کار حجم مبادلات مستقیم بطور نسبی کاهش یافته است.
- تهاتر نوعی مبادله مستقیم (QpQ, P2P) و ابتدایی ترین مکانیسم غیر پولی برای تبادل کالا است. شیب منحنی های بی تفاوتی در بهینه پارتو قیمت نسبی کالاها و چناچه کالاها زمان دار باشند نرخ بهره واقعی را تقریب می کنند.
- اگر همه مبادلات **دو جانبه** بود نیازی برای پول (واسطه مبادله) نبود، اما اغلب نفع مبادله در **چند جانبه** بودن آن است.
- مشکل سیستم تهاتر ایجاد **هماهنگی** میان افراد با رجحان ها و خواست های هم جور با هزینه کم است. این شیوه هیچوقت غالب و پایدار نشد.

مبادلات چند جانبه: اقتصاد هدیه ای

- با فرض اطلاعات کامل و در یک فضای همکاری جمعی (cooperative exchange) تخصیص کارآ علیرغم عدم تطابق دو-جانبه خواست‌ها و عدم نفع در مبادله دو جانبه، در مبادله چند جانبه و منفعت دار، بدون پول قابل تحقق است. **منطبق نبودن خواست دو جانبه شرط لازم و کافی نیاز به پول در مبادلات نیست.**
- شیوه رایج مبادله در اجتماعات کوچک (میان اعضای خانواده، دوستان و در جوامع بدوی) است. در اقتصادهای هدیه‌ای کار یا خدمتی که فردی برای دیگری انجام می‌دهد برای وی (**در طول زمان**) جبران می‌شود (**اعتبار**).
- این تبادلات فقط جنبه نیکوکاری ندارد (**تو نیکی می‌کن و در دجله انداز که ایزد در بیابانت دهد باز**) بلکه افراد بطور ضمنی انتظار ما به ازا دارند.
- در اجتماعات بدوی و کوچک همکاری برای زندگی اقتصادی لازم و تقسیم کار محدود است؛ به تعهدات هنجار اجتماعی پایبندی وجود دارد ؛ افراد یکدیگر را می‌شناسند و بر هم نظارت دارند؛ قول و قرارهای افراد (**گره‌ها در شبکه اجتماعی یا اینترنت**) از طریق تعامل‌های غیررسمی مانند یک شبکه توزیع شده حافظه در ذهن افراد (**شبکه توزیع‌شده اطلاعات در سرورها**) ثبت و پایش می شوند.



حافظه اجتماعی، پول و هماهنگی (coordination) فعالیت‌های اقتصادی

- در اجتماعات کوچک جمع‌آوری اطلاعات بطور غیرمتمرکز و داوطلبانه با هزینه کم انجام می‌گیرد. در جوامع بزرگ و پیچیده برای هم افزود کردن اطلاعات نیاز به فن‌آوری‌های مدرن است تا هزینه‌ها از بعد اقتصادی قابل توجیه باشند (**زنجیره الواح**).
- حافظه اجتماعی را می‌توان به ترازنامه فرضی (قول و قرار) تشبیه کرد. وقتی من کالا یا خدماتی را به شخص دیگر هدیه می‌کنم (طرف مقابل مدیون می‌شود)، ترازِ من به تناسب افزایش می‌یابد و بالعکس. بنابراین ترازنامه کارنامه‌ای از عملکرد اشخاص در گذشته و نتیجه این تبادلات است.
- روش این-به-آن و رسیدن به بهینه اجتماعی
- اگر این حافظه نادقیق و اطلاعات نامکتوب باشد، دسترسی به اطلاعات بی هزینه و نظارت دقیق درجه پایبندی به تعهدات روشن نباشد، مبادلات انجام نمی گیرد (**ارزش اقتصادی اطلاعات و نیاز به فن‌آوری‌هایی چون زنجیره الواح**).
- دو راه حل برای برطرف کردن مشکل قابل طرح است: اعتبار خصوصی و پول فرمانی.
- اگر ساختار اطلاعاتی اقتصاد بصورت فوق باشد، ناتوانی در نظارت نیاز به **پول** را ایجاد می‌کند. پول به عنوان واسطه مبادله مانند یک ابزار (دستگاه) ثبت و نگهداری رکوردها (**حافظه اجتماعی**) عمل می‌کند.
- اگر ج شهرت خوب داشته باشد و افراد بتوانند رفتار وی را نظارت و پایش کنند (بقیه نا آشنا). او با استفاده از شهرت خود می تواند با انتشار گواهی بدهی پول خصوصی برای مبادلات و پرداخت‌های غیرمستقیم در فضا و زمان ایجاد کند.
- نااطمینانی به وضعیت در چارچوب فوق قابلیت مدیریت شدن از طریق ایجاد کالاهای مشروط به وضعیت (state-contingent) یا صدور اوراق AD است.
- در صورت پایبندی به تعهدات، اعتبار (پول) خصوصی می‌تواند مبادلات چند جانبه را سامان دهی کند.
- نامتقارن بودن اطلاعات و کامل نبودن پایبندی به تعهدات، ظهور نهادهای تخصصی چون بانک‌ها را در بازار اعتبار توجیه می کند.

سوال: چرا افراد متقاضی پول (از جمله پول‌های رمزی) هستند؟ جواب: چون که به علت سایش‌های مختلف وجود پول از بعد اجتماعی سودمند است (باعث ایجاد تخصیص‌های کارآتر و فاه بیشتر برای افراد می‌شود)

- Chokerlakota AER 2002, Wallace 2001 نشان می‌دهند که دو سایش نیاز برای پول (ابزار مبادله) را ایجاد می‌کند:

1. محدودیت در جمع آوری، نگهداری و دسترسی عام به اطلاعات (مبادلات انجام شده در گذشته و حال «حافظه اجتماعی») به علت هزینه بر بودن آن (بویژه در دوران قبل از اینترنت).
2. محدودیت در تنفیذ قراردادها: جامعه برای بالا بردن هزینه عدم تعهد به قراردادها (برای ایجاد انگیزه برای التزام به اجرای قرارداد) محدودیت دارد.

If the function performed by money can be superseded by a perfect historical record of transactions, then money's only technological role must be to provide that record. In other words, money is a form of record keeping, or *societal memory.*" Chokerlakota , 1998, *P. 2.*

- عدم وجود حافظه اجتماعی و بالا بودن هزینه تنفیذ قراردادها میان افراد ناآشنا، داشتن پول فرمانی (ابزار پرداخت مورد قبول عموم) را به این جهت که با ایجاد انگیزه تبادل چندجانبه و دارا بودن خاصیت حافظه اجتماعی باعث گسترش مبادلات و بالا رفتن کارآیی در تخصیص منابع نسبت به حالتی که پول نیست می شود، توجیه می کند.
- به علت دومین محدودیت **IOU** های شخصی جایگزین نزدیکی برای پول فرمانی نبوده‌اند. **آیا پول دیجیتال (رمزی) می تواند این مشکل را برطرف کند و یک جایگزین پول فرمانی شود؟**
- به علت توانایی در تبدیل دارایی‌های غیرنقد مانند وثیقه و شهرت به دارایی نقد (پول) و نیز تبدیل بدهی با سررسید کوتاه‌مدت به دارایی بلندمدت، پول بانکی منتشر شده توسط بانک‌ها و شرکت‌های خصوصی (بدهی) در قرن نوزدهم رشد کردند و در بعضی از کشورها رایج شد.
- اما به علت نا قرینه بودن اطلاعات و نبودن **وام دهنده گزینه آخر** پول‌های خصوصی پایدار نماند و به جای آن طی یک قرن گذشته سیستم پول فرمانی همراه با بانکداری سنتی **FRB** و نظارت بانک مرکزی رایج شد.
- با توسعه این سیستم چارچوب های مناسب برای واسطه گری در سیستم پرداخت ایجاد و توسعه فن آوری (بانکداری الکترونیک) ظرفیت های و کارآیی بانک ها و موسسات مالی برای واسطه گری در سیستم پرداخت طی نیم قرن گذشته را افزایش داده اند.

سیستم پرداخت یک قاعده (پروتکل) برای بدهکار و بستانکار کردن حساب‌ها است. در این قالب پول آن چیزی است که برای بدهکار و بستانکار کردن حساب‌ها استفاده می‌شود.

- پول و به طور کلی ابزار پرداخت، فرم ثابتی ندارد. سیستم پرداخت نمونه‌ای از بازار دو سمتی است: وقتی شرایط محیطی و پیشرفت فن‌آوری در شیوه خرید مصرف‌کنندگان تغییر ایجاد می‌کنند و کسب و کارها تغییرات در فرم پرداخت‌ها را می‌پذیرند، فرم سیستم پرداخت نیز دستخوش تغییر می‌شود.
- سیستم کنونی پولی در جهان بر پایه «پول‌های فرمانی» بنا شده که منشأ نشر آن تراز بانک مرکزی است.
- حجم پول=اسکناس و مسکوک + ریال‌های دیجیتالی=اسکناس و مسکوک + سپرده (بدهی) بانکی («پول خصوصی»)
- اطمینان و اعتماد برای پول فرمانی توسط حکومت‌ها تأمین می‌شود و قیمت پول دیجیتالی به واحد پول فرمانی قفل شده است. اعتماد برای پول خصوصی می‌باید توسط سیستم بانکی با پشتیبانی بانک مرکزی تأمین شود.
- مدیریت ناصحیح سیستم پولی و اعتباری نیز زمینه برای ابداع پول‌های جدید را فراهم می‌کند (افزایش تقاضا برای بیت کوین در پی بحران مالی اخیر).
- در نظام موجود بانک‌ها یا موسسه‌های مالی واسطه سیستم‌های پرداخت هستند.
- ابداع شیوه‌های پرداخت الکترونیکی (کارت بانکی یا کارت اعتباری A2A یا P2P) کارآیی و سرعت نظام سنتی با واسطه‌گری سیستم بانکی را افزایش داده است (مثال، سامانه تسویه ناخالص آنی RTGS).

اینترنت، مشکل پرداخت و فن‌آوری زنجیره الواح

- فن آوری‌های جدید مانند اینترنت نه فقط سرعت بالایی برای ارسال متن، پیام، اطلاعات و کپی اسناد دارند بلکه قابلیت ارسال به گیرندگان پرشمار با هزینه نازل دارند و از این جهت مقرون به صرفه‌اند.
- اگر یک کیسه برنج با یک برند برای فروش بر خط اینترنت به شما عرضه شده، آیا می‌دانید این جنس اصیل است؟ وقتی برخط اینترنت با شخصی چت می‌کنید آیا او واقعا همان شخصی است که خود را معرفی کرده؟
- برای این که مطمئن شوید لازم است که پایگاه اطلاعاتی، مدارک و رکوردهای مربوطه را نگهداری کند و شما و دیگران آزادنه باید به آن دسترسی داشته باشید تا بتوانید آن را تایید کنید. این فن‌آوری «حافظه اجتماعی» را در ابعاد حافظه‌های مجازی و شبکه اینترنت تولید می‌کند.
- آیا می‌توان از فن‌آوری‌هایی چون تلفن موبایل یا اینترنت (ایمیل یا وبس میل) که برای رسانیدن پیام و اطلاعات بسیار سریع و کارا هستند برای انجام پرداخت‌های مالی و خرید دارایی‌ها بدون واسطه‌هایی چون سیستم بانکی استفاده کرد؟ **خیر**.
- بطور مثال، برای خرید کالا باید پول (اسکناس، چک یا الکترونیکی) پرداخت کرد ولی نمی‌توان کپی پول را برای فروشنده جهت خرید ایمیل کرد.
- این فرم پرداخت مشکل دو (یا چند) هزینه **(double spending)** دارد. در این شرایط افراد می‌توانند کپی‌های پول را برای خرید ارسال کنند که عرضه پول به شدت افزایش می‌یابد و به علت کاهش بهای آن دیگر نمی‌تواند مورد قبول و جاری باشد.
- برای خرید کالا و خدمات یا انتقال پول در شبکه اینترنت احتیاج به یک نهاد واسطه است.
- زنجیره الواح دستگاهی است برای ثبت وقایع (تراکنش‌ها) یا **نگهداری حافظه اجتماعی** و چنانچه قبلا اشاره شد از وظایف اصلی پول ثبت اطلاعات است.

سازوکار زنجیره بلوک

- سیستم‌هایی که بتوانند اطلاعات را با هزینه کم جمع‌آوری، حفظ، به روز کنند و در دسترس عام گذارند طی دهه اخیر ابداع و تبدیل به یک **الگوی کسب و کار** شده و به چرخه استفاده رسیده‌اند. نام فرضی مبدع ایده **Natashi Nakamoto (2008)** است که پروتکل (نرم افزار) زنجیره الواح را در محیط اینترنت بانی شد.
- زنجیره الواح یک دفتر عمومی توزیع شده (مشترک) است که از طریق تلاش گره‌های ویژه که به آنها استخراج‌گر (**miner**) گفته می‌شود مرتبا به هنگام می‌گردد. هر لوح یا دفتر ثبت وقایع تاریخ ایجاد ثبت شده دارد و با لوح‌های قبلی مرتبط است.
- پردازشگرهای غیرمتمرکز **miners**، تلاش می‌کنند براساس الگوریتم‌های محاسباتی مربوطه، از ترکیب تراکنش‌ها، الواح جدید ایجاد کنند. در صورت وجود خطا در دستور تراکنش (برای مثال اگر مبلغ تراکنش بیش از موجودی آدرس مبدا باشد) الواح ساخته شده براساس آن قابل اضافه شدن به زنجیره الواح نخواهند بود و لذا تراکنش تایید نمی‌شود.
- زنجیره الواح، اطلاعات از شبکه کامپیوترهای شخصی را بطور غیرمتمرکز ذخیره ونیز توزیع می‌کند. اطلاعات فقط درسرور مرکزی ذخیره نمی‌شود بلکه در دسترس همگان است. پس نه فقط مشکل «**اطلاعات خصوصی**» وامکان مخدوش کردن اطلاعات و زمین زدن سیستم توسط یک شخص یا شرکت برطرف شده بلکه با نظارت همگانی صحت رکوردها بطور شفاف تایید می‌شود. هیچ شرکت یا شخص مالک آن اطلاعات نیست («**اطلاعات خصوصی**» وجود ندارد).

تجارت و مبادلات اقتصادی نیازمند سیستم‌های پرداخت امن و قابل اعتماد است.

چهار نقش کلیدی که فن‌آوری زنجیره الواح مانند واسطه‌های بانکی و مالی درسیستم‌های پرداخت موجود قابلیت ایفا دارد:

1. **ایجاد اطمینان**: زنجیره بلوک یک دفتر کل جهانی (international public ledger)، مشتمل بر کلیه رکوردها و تراکنش‌ها است. مراجعین به شبکه یک نسخه به هنگام شده آن را در اختیار دارند. زمان صدور دستور تراکنش، جزئیات آن: آدرس مبدا، مقصد و مبلغ برای همه قابل رویت است. داده‌های ثبت شده درهر لوح را نه می‌توان عوض و یا حذف کرد. تا آنجایی که نتوان در اطلاعات دست برده و تغییر داد، اطلاعات در شبکه امن است و برای استفاده‌کنندگان «اعتماد» ایجاد می‌شود. مشابه **سیستم بانکی که با مدیریت دفترها (ledgers) و حساب‌ها افراد از صحت تراکنش‌ها اطمینان دارند و تراکنش‌ها قابل ردیابی هستند.**
2. **شناسایی و تایید** طرفین تراکنش یا پرداخت‌ها
3. **تهاتر و تسویه** تراکنش‌ها
4. **نگه‌داری رکورد** تراکنش و پرداخت‌ها

- **چون پایه های هر سیستم پرداخت ثبت رکوردها و انتقال اطلاعات میان دینفعان است، نظام های پرداخت همراه با پیشرفت های فنی توسعه یافته اند. هر چند فن‌آوری کنونی سیستم های پرداخت قابلیت‌های خوب و متنوعی برای تراکنش و پرداخت‌ها دارد اما در دهه‌های هفتاد و هشتاد اختراع شده‌اند و بزودی نسل جدیدتر فن آوری وارد این صنعت خواهد شد.**
- **سیستم پول‌های رمزی با استفاده از فن آوری های جدیدتر، پلاتفرم زنجیره و شبکه اینترنت، پرداخت میان اشخاص(حقیقی و حقوقی) را بدون نیاز به واسطه‌گری سیستم بانکی و موسسات مالی با هزینه کمتر انجام می‌دهد.**
- **چون فن‌آوری زنجیره الواح چهار نقش کلیدی سیستم‌های پرداخت قابل اتکا را به طور امن تامین می‌کند، این فن‌آوری را برای فعالیت‌های متنوعی چون پول‌های رمزی، بلکه نیز خرید دارایی‌ها، مبادلات مالی، ثبت رکوردهای سلامت و ... مناسب ساخته است.**
- **زنجیره الواح فن‌آوریی است با پروتکل مشخص و شفاف برای پرداخت و انتقال پول رمزی و معامله دارایی‌ها بدون واسطه‌گری شخص یا سیستم مالی با هزینه نسبتا کم راه حل برای پرداخت درسیستم‌های امن را فراهم اورده است.**

تصویر دولوح پیاپی: اگر لوح دوم نشان دهد که من تعداد پول دیجیتالی بیشتری نسبت به لوح قبلی دارم، باید رکوردی برای فرستاده شدن آن ها به حساب وجود داشته باشد. اگر چنین تراکنشی ثبت نیست این لوح تایید نمی شود. همینطور شما که تعداد ۲ واحد کمتر در لوح دوم دارید باید رکورد فرستادن آن دو به حساب دیگر وجود داشته باشد در غیر اینصورت این الواح تایید نمی شود.

شنبه ۱ دی ساعت: ۱۱	
من	۴
شما	۲

شنبه ۱ دی ساعت: ۱۱:۱۵	
من	۱۸
شما	۰

شنبه ۱ دی ساعت: ۱۱	
من	۴
شما	۲

شنبه ۱ دی ساعت: ۱۱:۱۵	
من	۱۸
شما	۰

چگونه افراد رکورد واحد های پول دیجیتالی را برای یکدیگر می فرستند؟ از زیر مجموع ای از ریاضی (cryptography) برای فرستادن و دریافت اطلاعات تراکنش ها استفاده می شود. در الواح حساب ها بر اساس اسامی افراد رد گیری نمی شوند، بلکه با crypto-alfa-numeric=CAN شناسایی، رد گیری و تنظیم می شوند.

اگر شما بخواهید برای پیراهنی که برایتان خریده ام بیت کوین برایم بفرستید من آدرس CAN خود را برایتان میفرستم و به این آدرس از کیف پول دیجیتالی خود می پردازید. این تراکنش در لوح بعدی ثبت می شود. هر شخص دو آدرس (نشانی) دارد. نشانی عمومی که برای همه قابل رویت است. مانند آدرس زیر. نشانی خصوصی که طولانی تر است را فقط صاحبش میداند.

من	x 2 5 0 b b 8 3 7 2 b y w c w c 1 8
شما	x 5 7 8 9 h b c b w c 5 h b w y w c

پول دیجیتال راهکار آینده؟

- هر قدر که پول غیر ملموس تر و مجازی تر شود اهمیت اطمینان و درک مشترک از واقعیت آن بیشتر می شود.
- یکی از APP های مهم فن آوری زنجیره الواح پول های رمزی است که معروف ترین آنها بیت کوین است و اولین پول دیجیتالی است که مشکل چند بار هزینه کردن را حل کرده است. پول های رمزی مانند اسکناس بی نام (نا شناس) هستند.
- **کاربرد های تجاری فن آوری زنجیره الواح فراتر از پول های رمزی است.**
- پول های رمزی (**اعتبار نیستند**) شامل چند جزء اساسی هستند: سکه های مجازی، دفتراطلاعات تراکنش ها، پروتکل مشخص برای سیستم پرداخت و قاعده کنترل کمیت سکه ها (سیاست پولی).
- پول های رمزی از زنجیره الواح و فعالیت غیر متمرکز **استخراج گر** ها برای ثبت و پایش رکورد تراکنش و مالکیت پول دیجیتال برای شناسایی صاحب آن در یک زمان معین استفاده می کنند. بدین ترتیب امکان این که افراد نتوانند دو یا چند بار آن را خرج کنند فراهم میشود—مشابه سیستم های نظارتی و پایش دولتی برای جلوگیری از انتشار پول فرمانی تقلبی.
- پول های رمزی (**بیت کوین ~ پول نقد دیجیتالی**) گزینه مناسبی برای مبادلات P2P و راهکاری امن برای پرداخت است. به تفسیری این ساختار دارای پایه های لازم برای پول بودن و داشتن یک سیستم پرداخت است.
- فرم پرداخت پول های رمزی با سیستم هایی چون Paypal یا کارت های اعتباری متفاوت است زیرا که از نهاد های واسطه مانند بانک ها یا موسسات مالی استفاده نمی کنند.هزینه نهایی استفاده از پول رمزی برای پرداخت در مقایسه با سیستم سنتی کمتراست.
- در شرایط کنونی پول رمزی علیرغم مرتفع کردن مساله دسترسی عمومی و بدون هزینه به اطلاعات و تنفیذ خودکار اجرای تعهدات و امنیت آن همچنان جایگزین نزدیکی برای پول فرمانی نیست. به علاوه در پول های رمزی فعلی ظرفیت خلق پول از طریق ایجاد اعتبار وجود ندارد، اما استفاده تجاری از آن ها محدود به جایگزین شدن برای پول های فرمانی نیست.
- پول های رمزی مانند پول کالایی و اسعار خارجی به قیمت پول فرمانی ثابت نیستند. نوسانات متوسط نوسانات قیمت بیت کوین طی دوره بیش از طلا و شاخص های سهامی چون بوده است. از این جهت برای نگه داشتن ذخیره ارزش در کوتاه مدت در اقتصاد هایی با نرخ های تورم پایین مناسب نیست.