پرداخت برون خط بلوکی توزیع شده
Distributed Offline Block Payment

عماد ایرانی، مدیر پروژه کیف پول الکترونیک CityPay (e.irani *at* faash.ir)

چکیده

پرداخت های خرد الکترونیکی در حال حاضر با استفاده از کارتهای بانکی صورت می‌پذیرد. در فضاهای مرتبط با حوزه حمل و نقل شهری، اقداماتی در زمینه الکترونیکی کردن پرداخت کرایه با استفاده از رسانه های هوشمند برون خط (Offline Smart Media) صورت پذیرفته است. در تمامی مدلهای پیاده شده، فارغ از نوع فناوری و رسانه مورد استفاده(اکثرا کارت هوشمند یا کارتهای حافظه)، از سرویس دهنده برخط مرکزی (Core Processor) به منظور پذیرش تراکنش های برونخط انجام شده در گذشته و تسویه مالی آنها بهره برداری شده است.

تمامی تراکنش های مالی، بعد از رخداد ذخیره می‌شوند و جهت پردازش به مرکز ارسال می‌گردند. این تراکنش‌ها حاوی اطلاعاتی در مورد پرداخت کننده و دریافت کننده وجه و سایر پارامترهای مالی می‌باشند. با توجه به اینکه رویکرد استفاده از شبکه های پرداخت خرد کاهش سربار هزینه‌های متحمل و وابستگی به شبکه برخط می‌باشد، لذا این قبیل تراکنشها به دلیل برون خط بودن کمک شایانی در این زمینه می نمایند. اما به دلیل آنکه پردازش آنها صرفا در مرکز اصلی صورت می‌پذیرد، لذا باید تراکنش های مربوطه از طریق شبکه برخط(به صورت دسته‌ای) به مرکز ارسال گردند و در این بخش هیچ کاهش هزینه ای در زمینه حجم اطلاعات وجود نخواهد داشت. در کنار این موضوع، عدم ارتباط با سرویس دهنده مرکزی موجب عدم واریز وجه نقدی‌ریالی برای دریافت کننده وجه یا پذیرنده خواهد شد.

در مدل ارائه شده در این مقاله با عنوان «پرداخت برون خط بلوکی توزیع شده» یا DOBP[1] رویکرد جدیدی در این زمینه معرفی گردیده است.

در مدل DOBP پرداخت های خرد به صورت C2C با روشهای مبتنی بر Cryptography بین رسانه های هوشمند صورت می پذیرد و وجه مورد انتظار از رسانه شخص اول در لحظه به رسانه شخص دوم منتقل می گردد و نیازی به پردازش در مرکز اصلی وجود نخواهد داشت.

مدل DOBP دارای راه‌کارهایی برای مدیریت و ضرب وجه الکترونیکی، اعتبار سنجی غیر متمرکز، تبدیل وجه الکترونیکی به وجه غیرالکترونیکی(نقدی-ریالی)، پرداخت برخط و استفاده از رسانه‌های هوشمند مختلف می‌باشد و برای هر موضوع فرآیندی فنی اجرایی ارائه نموده است.

واژگان کلیدی: پرداخت خرد، پرداخت برون خط، توزیع شده، پرداخت هوشمند، پرداخت بلوکی، رمزنگاری، وجه الکترونیکی

[1] Distributed Offline Block Payment

مقدمه

پرداخت‌های خرد الکترونیکی امروزه در همه‌جا شنیده می‌شوند. مدیریت وجوه خرد یکی از موثرترین راه‌کارهای کنترل نقدینگی در سطح جامعه است. هزینه و سربار تولید اسکناس و سکه‌های فلزی و تخریب آنها به دلیل فیزیکی بودن نیز بر این فضا سایه انداخته است.

با توجه به اینکه در این مقاله قصد بر آن است که مقایسه‌ای بین شبکه‌های پرداخت الکترونیکی صورت پذیرد لذا محدوده جغرافیایی این مقاله محدود به «کشور جمهوری اسلامی ایران» خواهد بود و کلیه سامانه‌های مالی و اقتصادی بررسی شده در این مقاله در بازه تاریخی سالهای ۱۳۹۰ شمسی به بعد خواهد بود.

مدیریت فضای پرداخت خرد الکترونیکی گرچه نگاه‌های متفاوتی را به خود جلب می‌کند و با پاسخ‌های متفاوتی در این زمینه روبرو شده است ولی به طور قطع ایجاد یکپارچگی در این فضا بدون تردید اولین قدم در رسیدن به هدف عالی «مدیریت الکترونیکی وجوه خرد» به شمار می‌رود.

جذابیت این فضا برای بازیگران مختلفی که وارد آن شده‌اند به طور خاص مربوط به کارمزدهای جذاب این حوزه بوده است. به دلیل عدم وجوه نظام پرداخت خرد الکترونیکی در کشور، سه مسیر مجزا برای حل این مسئله به کار گرفته شده است:

- استفاده از شبکه پرداخت الکترونیک شاپرک به منظور انجام پرداخت های خرد به صورت برخط
- استفاده از راه‌حل های مبتنی بر کارت بلیت برای حل فضای پرداخت الکترونیکی کرایه در حوزه حمل و نقل
- کیف پول‌های الکترونیک برخط یا برون خط ارائه شده توسط فینتک ها و بانکها

هر کدام از سه راه‌حل استفاده شده به جهت رفع نیاز پرداخت‌های الکترونیکی خرد، دارای مشکلات و نواقصی هستند که در مقالات قبلی «کیف پول مبتنی بر چیپ CityPay»[1] و «رویکرد امنیت محور در نظام پرداخت خرد»[2] به تفصیل به آنها اشاره شده است. در این مقاله سعی شده است با رویکردی جدید و منحصر به فرد یک شبکه پرداخت خرد الکترونیکی غیر وابسته و غیر متمرکز مبتنی بر توانمندی‌های برگرفته از رمزنگاری دیجیتال[۲] معرفی گردد و جهات مختلف آن بررسی شود. این مقاله پاسخی خواهد بود به بیشترین مشکلات مشاهده شده در مدیریت شبکه‌های پرداخت خرد الکترونیکی و کیف پول-های الکترونیک و راه‌کاری به منظور کاهش ریسک‌های اجرایی و عملیاتی مرتبط با آن.

در ادامه مقاله، به بررسی وضعیت فعلی شبکه پرداخت خرد و مسائل مرتبط با آن پرداخته می‌شود و در ادامه مدل DOBP با تعریف کامل ارائه می‌گردد.

ادبیات موضوع

زمانی که در مورد کیف پول الکترونیکی و مدیریت فضای پرداخت خرد الکترونیکی صحبت می‌شود، منظور راه‌کارهایی هستند که پرداخت وجوه خرد بین افراد را با استفاده از روشهای الکترونیکی و عدم وابستگی به وجوه نقد فیزیکی به انجام می‌رسانند. پرداخت خرد دارای مشخصه‌های مختلفی می باشد که برخی از آنها به شرح زیر هستند:

---

[۲] Digital Cryptography

- رقم تراکنش می بایستی بین حداقل واحد مالی ضرب شده توسط بانک مرکزی جمهوری اسلامی ایران (۲۵۰ ریالی) و حداکثر رقم ۶۰۰,۰۰۰ ریال باشد.
- تراکنش می‌بایستی بین افراد به صورت C2C صورت پذیرد و در هر معامله یک پرداخت کننده و یک دریافت کننده وجود داشته باشد.
- رقم تراکنش می‌بایستی ضریبی از ۱۰ ریال یا یک تومان باشد.

همانطور که عنوان شد فضای پرداخت خرد الکترونیکی در حال حاضر به سه روش اصلی مدیریت می گردد، استفاده از شبکه پرداخت الکترونیک شاپرک، کیف پول‌های الکترونیک برخط یا برون خط و کارت بلیت‌های مدیریت خدمات حمل و نقل شهری.

در کلیه مدل‌های فوق که مبتنی بر مدل‌های سرویس دهنده-گیرنده[۳] طراحی شده اند، تراکنش می‌بایستی به منظور ثبت شدن در مرکز صادرکنندگی مورد بررسی قرار گیرد. برای مثال در شبکه پرداخت الکترونیک شاپرک که از مدل اعتبارسنجی برخط استفاده می‌کند، به این شکل عمل می‌شود که تراکنش از تجهیز الکترونیکی به مرکز شاپرک ارسال می‌گردد و بعد از انتقال به صادر کننده از طریق شبکه‌های ملی پرداخت، اعتبارسنجی شده و پاسخ به تجهیز الکترونیکی باز می‌گردد. سه اشکال در استفاده از شبکه پرداخت الکترونیک شاپرک به جهت پرداخت‌های خرد وجود دارد. اول نظام کارمزدی فعلی که باعث ایجاد سربار هزینه‌ای غیر مفید برای بانکهای پذیرنده خواهد شد. دوم عدم سرویس دهی در صورت عدم دسترسی به مرکز پردازش و سوم هزینه بالای پردازش تراکنش در شبکه شاپرک و شبکه‌های ملی بالادستی به منظور پردازش یک تراکنش کم ارزش مالی.

در سایر مدل‌های پرداخت الکترونیک که در پرداخت‌های خرد از آنها بهره گرفته شده است، می توان کیف پول های الکترونیکی برخط را نام برد که دارای مشکل عدم سرویس دهی در زمان قطعی را دارا می‌باشند اما به دلیل عدم استفاده از شبکه پرداخت ملی سرباری را برای این شبکه ایجاد نمی‌نمایند. مشکل این قبیل شبکه‌های مالی عدم نظارت بانک مرکزی بر روی آنها خواهد بود و عملیات خلق پول در ساده ترین روش آن یعنی استفاده مجدد از وجوه پشتیبان کیف الکترونیکی تولید شده صورت می پذیرد.

سومین مدل، یعنی استفاده از کارت‌های بلیت در حوزه خدمات حمل و نقل با توجه به برون خط بودن مشکلات حوزه برخط را ندارند. اما استفاده از مدل‌های ضعیف امنیتی، عدم وجود نظام یکپارچه تسویه و مسیر بسته بودن[۴] باعث شده است تا قابلیت استفاده در سایر حوزه‌های پذیرندگی خرد میسر نباشد و همچنین مدیریتی بر روی خلق پول در آنها به دلیل عدم وجود نظام نظارتی و مدیریتی مرکزی انجام نمیپذیرد.

در نظام پرداخت خرد الکترونیک DOBP سعی شده است مشکلات اصلی حوزه پرداخت خرد الکترونیکی مورد توجه ویژه واقع شود و برای آنها یک راه حل مناسب در نظر گرفته شود. مشخصه‌های اصلی نظام DOBP به شرح زیر است:

- در DOBP تنها یک نهاد (بانک مرکزی جمهوری اسلامی ایران) توانایی ضرب وجه الکترونیکی را دارد و تنها همین نهاد قابلیت تبدیل آن به وجه فیزیکی را دارا می‌باشد.

---

[۳] Client-Server

[۴] Closed loop

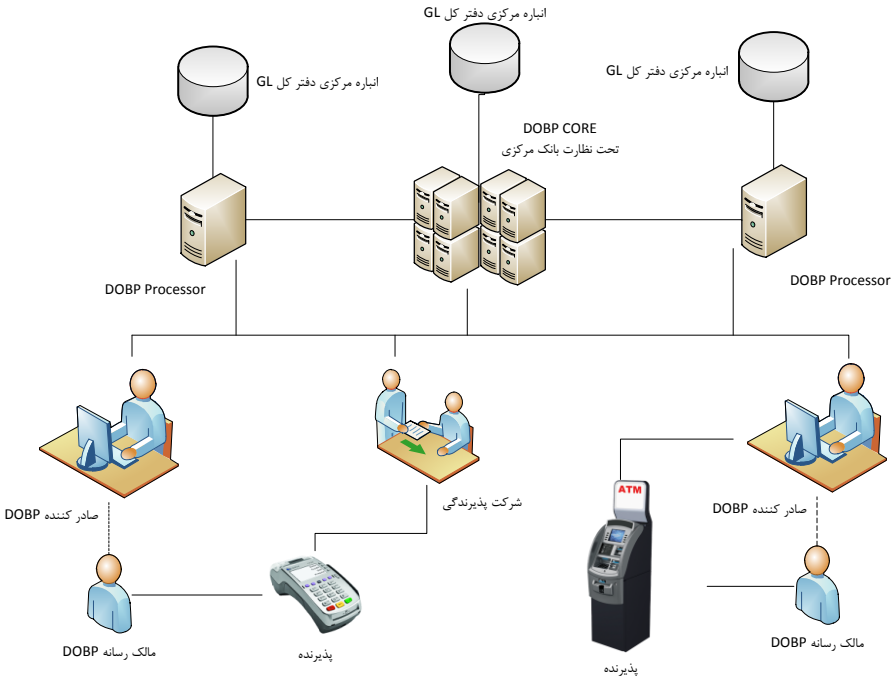
- نقل و انتقال C2C بین افراد بدون نیاز به واحد مرکزی صورت می‌پذیرد و نهاد مرکزی صرفا زنجیره ای از بلوک‌های انتقال یافته بین افراد را بعد از انجام تراکنش و بر اساس درخواست دارنده رسانه دریافت می‌کند.
- اعتبار سنجی بلوک‌های دریافتی از دارندگان رسانه به صورت توزیع شده[۵] صورت می‌پذیرد و واحدی مرکزی در این بین وجود ندارد. البته واحدهای اعتباری سنجی از قبل مورد تایید واحد مرکزی قرار گرفته اند.
- دفترکل نقل و انتقالات بین مشتریان در اختیار کلیه صادرکنندگان قراردارد و در محلی مشخص نگهداری نمی‌شود اما نسخه دراختیار بانک مرکزی مرجع تصمیم گیری ایشان خواهد بود.
- نظام DOBP همانطور که از اسم آن پیداست برونخط بوده و عملیات مالی بدون نیاز به شبکه برخط صورت می-پذیرد.
- از نظام DOBP می توان در شبکه‌های پرداخت موبایلی و همینطور پذیرنده‌های برخط اینترنتی نیز استفاده نمود.
- دریافت وجوه از رسانه‌های DOBP نیازمند ماژولهای امنیتی سخت افزاری[۶] نمی‌باشد و پذیرنده‌های DOBP نیازی به در اختیار داشتن فضای امن اطلاعاتی بر روی تجهیز خود نیستند(بر خلاف کارت بلیت و کیف پولهای برون خط فعلی).
- رسانه DOBP می تواند از انواع رسانه‌های هوشمند امن مانند کارتهای هوشمند، تلفن‌های همراه، ساعت های هوشمند، دستنبندهای هوشمند و یا ... باشد و محدودیتی در استفاده از آنها وجود ندارد.
- رسانه DOBP می‌تواند توسط صادرکنندگان مختلفی صادر شود و منحصر به یک بانک یا موسسه مالی نیست. همچنین رسانه‌های DOBP می‌توانند به صورت ناشناس[۷] صادر گردند تا محرمانگی مورد نیاز مشتریان و عدم شناسایی تراکنش‌های ایشان مقدور باشد(در صورتی که مجوزهای عملیاتی آن صادر شده باشد).
- نظام DOBP خود اصلاح می‌باشد و در بازه‌های زمانی مشخصی اقدام به اصلاح خود، شناسایی تقلب[۸]، مسدود سازی رسانه‌ها، ارتقاء سطح امنیتی رسانه‌ها و تغییر پارامترهای مرتبط با رمزنگاری دیجیتال می‌نماید.
- تجهیزات مورد نیاز جهت پذیرش DOBP تنها می‌بایستی با ساختار پذیرش آن سازگار باشند و نیازی به ارتباط با صادر کننده ندارند. در این نظام، ارتباط بین پذیرنده و صادر کننده به صورت کامل قطع شده است و صادرکنندگان و پذیرندگان هیچ شناختی از یکدیگر نخواهند داشت. در اصل زمانی که یک پذیرنده به DOBP متصل می‌گردد رسانه‌های تولید شده توسط تمامی صادر کنندگان بر روی آن به درستی فعالیت می‌نماید و چند پذیرندگی در یک محل فیزیکی برطرف گردیده است.

در بخشهای بعدی این مستند در مورد هریک از این قابلیت‌ها توضیحاتی کامل ارائه شده است.

نقشه ارتباط فیزیکی در DOBP

[۵] Distributed
[۶] Security Access Module (SAM)
[۷] Anonymous
[۸] Fraud Detection

به منظور درک هرچه بهتر ارتباطات در DOBP، نقشه کلی این نظام به این شکل ترسیم گردیده است:



تصویر ۱ - شمای کلی نظام DOBP

نقشهای معرفی شده در تصویر بالا، هر کدام دارای وظایفی هستند که در جدول زیر آمده است:

جدول ۱ - نقشهای نظام DOBP

ردیف	نقش	وظیفه
۱	DOBP Core	نقش واحد مرکزی ضرب وجه الکترونیکی به معنی تبدیل وجه فیزیکی به وجه الکترونیکی می باشد. در فعالیتی دیگر این واحد اقدام به تبدیل وجه الکترونیکی به وجه فیزیکی و واریز به حساب نقدی-ریالی دارندگان رسانه می‌نماید. همچنین

		وظیفه رگولاتوری و مدیریت فضای صادرکنندگی و پذیرندگی در اختیار این نهاد می‌باشد.
۲	DOBP Processor	واحدهای پردازش بلوکهای اطلاعاتی دریافت شده از رسانه‌ها هستند. این واحدها به صورت مستقل عمل می‌نمایند و هرکدام دارای یک انباره دفترکل مرکزی GL هستند. هر رسانه می تواند به صورت دلخواه به یکی از آنها متصل شود و پردازشگران، بلوک‌های دریافت شده را دراختیار یکدیگر قرار می‌دهند. واحد مرکزی یا DOBP Core هم دارای یک انباره مرکزی می‌باشد که خود را دائما با سایر DOBP Processorها که به صورت توزیع شده وجود دارند همگام سازی می-نماید.
۳	صادرکننده	وظیفه صادرکنندگان ارائه رسانه هوشمند DOBP به مشتریان می‌باشد. این رسانه‌ها با همکاری DOBP Core صادر می‌شوند و سپس در اختیار مشتری قرار می‌گیرند. همچنین با توجه به اتصال دستگاه های خودپرداز به صادرکنندگان وظیفه مدیریت و ارسال تراکنش‌های دریافتی بر روی آنها و همچنین وظیفه ارائه خدمت تبدیل وجه الکترونیکی به وجه فیزیکی با ایشان است.
۴	شرکت پذیرندگی	شرکت پذیرندگی وظیفه ارسال تراکنش‌های دریافتی بر روی پایانه‌های فروشگاهی را بر عهده دارد. تراکنش‌های DOBP در زمان انجام عملیات صرفا بر روی پایانه ذخیره می‌گردند و سپس به صورت Batch به یکی از مراکز ارسال خواهند شد.
۵	مالک رسانه	مالک رسانه یک شخص حقیقی می‌باشد که اقدام به دریافت رسانه از یکی از صادرکنندگان DOBP نموده است. رسانه به صورت بانام یا بی نام در اختیار ایشان قرار داده می‌شود. رسانه بعد از فعال‌سازی قابلیت ذخیره وجوه الکترونیکی و یا پرداخت وجوه الکترونیکی را خواهد داشت.
۶	پذیرنده	هر واحد فیزیکی که قابلیت پذیرش DOBP را داشته باشد پذیرنده نامیده می-شود. پذیرنده وجوه DOBP را به شکل تراکنش های امضا شده دریافت می‌نمایند و بعد از درخواست تبدیل به وجه فیزیکی، وجه آن‌را در حساب نقدی-ریالی خود دریافت خواهد نمود.

عملیات انتقال وجه بین رسانه‌ها

یکی از مشکلات شبکه‌های پرداخت خرد فعلی آن است که تراکنش صورت گرفته بین یک رسانه و پایانه، می‌بایستی جهت نقد شدن به مرکز واحد کنترل و پردازش تراکنش ارسال گردد و سپس وجه معادل آن توسط یک سامانه تسویه به پذیرنده پرداخت می‌گردد.

در DOBP عملیات نقل و انتقال مالی به صورت C2C صورت می‌پذیرد و رسانه‌ها قادر هستند به یکدیگر وجوهی را انتقال دهند. به این معنی که عملیات در DOBP یکباره نیست(به ازای هر تراکنش نیازی به ارسال تراکنش به مرکز نیست) و

شامل مراحلی به شکل زیر است. به منظور افزایش موجودی الکترونیکی رسانه دو اتفاق می‌تواند روی دهد:

- ارائه وجه فیزیکی به بانک مرکزی و درخواست وجه الکترونیکی به صورت برخط.
- دریافت وجه الکترونیکی از یک رسانه دیگر به صورت برون خط(انتقال وجه بین رسانه‌ها).

ضرب وجه الکترونیکی

ضرب وجه الکترونیکی به معنی خارج نمودن وجه فیزیکی از چرخه مالی کشور و تبدیل آن به وجه الکترونیکی می‌باشد. این عملیات صرفا توسط نهاد مرکزی تحت کنترل بانک مرکزی جمهوری اسلامی ایران صورت می‌پذیرد. زمانی که یک مشتری یک رسانه DOBP دریافت می‌کند، موجودی رسانه ایشان صفر خواهد بود.

در مدل اول، فرد با مراجعه به یکی از مراکز مالی، دستگاه‌های خودپرداز و یا از طریق سایر کانال‌های بانکی، وجهی را از طریق شبکه شتاب و کارت بانکی خود یا از طریق برداشت مستقیم از حساب نقدی، دریافت می کند. این عملیات طی درخواستی به مرکز DOBP Core صورت خواهد پذیرفت.

در DOBP Core وجه نقدی ابتدا تایید می‌گردد(برداشت یا انتقال) و سپس به حساب مرکزی بلوکه نزد نهار مرکزی منتقل می‌شود. در این مرحله وجه فیزیکی از چرخه مالی کشور خارج شده است. یک تراکنش ویژه به نام انتقال از مبدا صفر به رسانه DOBP ارسال می‌شود و بر روی رسانه ثبت خواهد شد. این تراکنش با کلید خصوصی DOBP Core که بخش عمومی آن در زمان صدور بر روی رسانه‌ها قرار گرفته است امضا می‌شود. در این مرحله وجه الکترونیکی ضرب شده است.

Debit Card => Cash or Bank Transaction => Money Transfer to CBI => Sign[PrivateKey](New Zero Base Transaction with Amount) => DOBP Terminal => DOBP Media

بعد از انجام تراکنش یک رکورد در دفتر روزنامه داخلی DOBP ثبت می‌شود و همان رکورد در DOBP Core نیز ثبت می‌گردد. اکنون رسانه دارای موجودی است و وجه متناظر با آن از چرخه مالی خارج شده است. این روش موثرترین راه در زمینه کنترل خلق پول الکترونیکی خواهد بود زیرا ورود وجه به کل شبکه صرفا از طریق خروج وجه فیزیکی میسر است.

انتقال وجه بین رسانه‌ها

یکی دیگر از راه‌های افزایش موجودی رسانه DOBP انتقال وجه بین رسانه‌ای می‌باشد. در این روش وجه از یک رسانه به رسانه دیگر منتقل می‌شود. عملیات انتقال وجه بین رسانه‌ها باعث کسر موجودی رسانه پرداخت کننده و افزایش موجودی رسانه دریافت کننده خواهد شد. در این عملیات دفتر روزنامه داخلی هر دو رسانه تاثیر می‌پذیرد و جداگانه در زمان تسویه تراکنش‌ها، این تراکنش خاص از دو مسیر متفاوت به مراکز پردازشی متفاوتی منتقل می‌گردند.

عملیات انتقال وجه بین رسانه‌ها از طریق یک عامل سوم که یک ابزار الکترونیکی می‌باشد صورت می‌پذیرد. این ابزار می‌تواند پایانه فروشگاهی، خودپرداز، تلفن همراه، دستگاه کامپیوتر متصل به کارتخوان و یا هر ابزار دیگری با قابلیت ایجاد ارتباط با رسانه DOBP باشد. مراحل این عملیات به شکل زیر است:

- ابتدا رسانه درخواست کننده وجه یک Challenge تصادفی تولید می‌کند. سپس با اضافه نمودن شماره تراکنش داخلی، رقم(دریافت شده از عامل سوم) و سایر پارامترهای مورد نیاز، درخواست را با کلید خصوصی خود امضا نموده

و به همراه گواهینامه الکترونیکی خود در اختیار رسانه دوم قرار می‌دهد(از طریق عامل سوم).

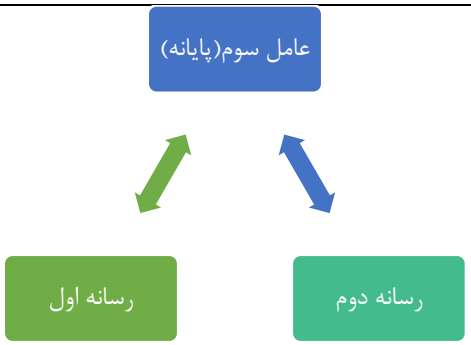
- رسانه پرداخت کننده وجه ابتدا گواهینامه درخواست کننده را مورد بررسی قرار می‌دهد و امضای دیجیتال آن را تایید می‌کند.
- سپس اقدام به بررسی پارامترهای ریسک مرتبط با تراکنش می‌نماید(مبلغ درخواست، نوع گواهینامه، رمز مالک رسانه و ...)
- در صورت موافقت با پرداخت، تراکنشی مبتنی بر پرداخت وجه از رسانه خود شامل رقم، شماره تراکنش داخلی، مقدار Challenge در خواست کننده، شماره تراکنش داخلی درخواست کننده، ساعت و تاریخ تراکنش(دریافت شده از عامل سوم) و سایر پارامترهای کنترلی تولید می‌نماید.
- تراکنش تولید شده با کلید خصوصی پرداخت کننده رمز شده و به همراه گواهینامه در اختیار دریافت کننده وجه قرار داده می‌شود(از طریق عامل سوم).
- دریافت کننده وجه با بررسی گواهینامه، امضا، شماره تراکنش داخلی و مقدار Challenge و رقم تراکنش، اقدام به افزایش سطح موجودی خود می نماید.
- هر دو رسانه اقدام به ثبت تراکنش در دفتر روزنامه خود می‌نمایند.

همانطور که در عملیات بالا مشاهده شد، عامل سوم که یک ابزار کنترلی می‌باشد با وجود اینکه در بین تراکنش قرار گرفته-است قادر به تغییر پارامترهای تراکنش نخواهد بود و در صورت انجام این عمل، تراکنش به صورت موفقیت آمیز در رسانه‌ها ذخیره نمی‌گردد.

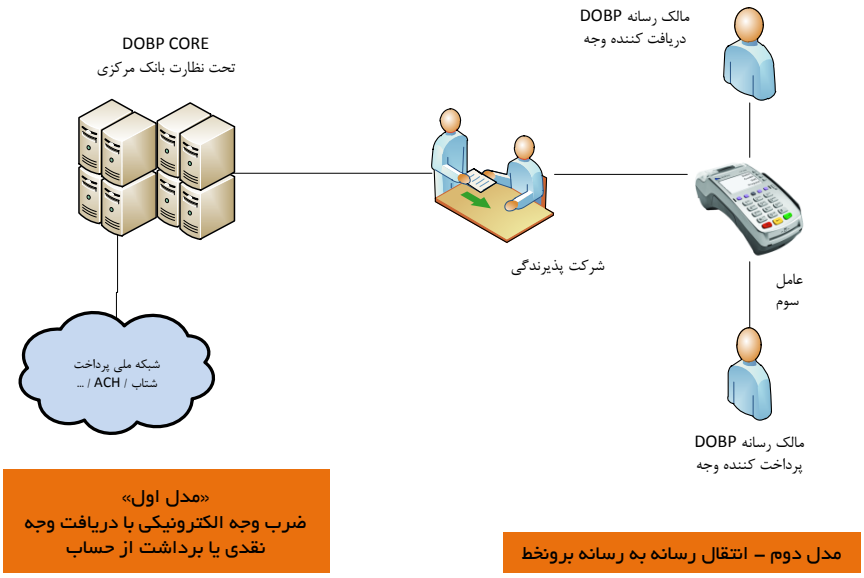
نکته: امکان این وجود دارد که بعد از پرداخت وجه توسط رسانه پرداخت کننده، تراکنش به دلایلی مانند قطع ارتباط با رسانه، امکان ارسال به رسانه دوم را نداشته باشد. برای این موضوع راه‌کاری در نظر گرفته شده است. رسانه‌های DOBP همیشه آخرین تراکنش ارسالی را در خود ذخیره می‌نمایند و در تمام اوقات این تراکنش با تمامی اطلاعات قبلی قابل بازیابی خواهد بود. مقدار Challenge نیز در رسانه‌های DOBP صرفا زمانی تعویض می‌گردند که یک تراکنش به درستی بر روی رسانه ثبت گردد. در صورتی که عدم ارتباط با رسانه دریافت کننده ایجاد شود، عامل سوم می‌بایستی از دارنده رسانه درخواست کند که مجددا رسانه خود را به پایانه ارتباط دهد. در این هنگام با توجه به اینکه مقدار Challenge در رسانه تغییر نکرده است، مجددا می‌توان تراکنش را جهت ثبت به رسانه دریافت کننده وجه ارسال نمود.

نکته: قابلیت بازمصرف[۹] تراکنش‌ها در عامل سوم وجود ندارد. باز مصرف به این معناست که تراکنشی جهت افزایش اعتبار مجدد به یک رسانه ارسال گردد. با توجه به اینکه بعد از اولین ثبت تراکنش در رسانه دریافت کننده مقدار Challenge از بین می‌رود و شمارنده تراکنش یک شماره افزایش خواهد یافت، لذا امکان ارسال مجدد تراکنش به منظور تقلب و بازمصرف در نظام DOBP وجود ندارد و امضای دیجیتال آن معتبر نخواهد بود.

[۹] Double Spend



همانطور که در این بخش توضیح داده شد، در کنار راه‌کار افزایش اعتبار از طریق ضرب وجه الکترونیکی، راه‌کار انتقال بین رسانه‌ای نیز وجود دارد. با استفاده از این قابلیت می‌توان با در اختیار داشتن یک رسانه با اعتبار مشخص، اقدام به دریافت وجه نقد از مالکان رسانه‌های دریافت کننده وجه نمود و در مقابل عمل انتقال بین رسانه‌ای برای ایشان انجام گردد. به معنی واضح-تر تنها راه افزایش نقدی اعتبار رسانه‌های DOBP استفاده از شبکه برخط و ضرب وجه الکترونیکی نیست. در ضمن در این روش به دلیل اینکه از اعتبار ضرب شده داخلی شبکه بهره برداری می‌شود هیچگونه عملیات خلق پول شکل نخواهد گرفت، اما قابلیت واریز نقدی به رسانه‌ها به صورت برون خط میسر خواهد شد.



تصویر ۲ - مدلهای انتقال وجه در DOBP

رسانه و پایانه‌های فروشگاهی

در بخش قبلی توضیحاتی در رابطه با مدل C2C انتقال وجه بین رسانه‌ای و مدل ضرب وجه الکترونیکی توسط نهاد قانونی توضیحاتی داده شد. یکی از نیازهای پرداخت خرد الکترونیکی در کشور، انجام عملیات پرداخت خرد در حمل و نقل شهری و پایانه‌های فروشگاهی پذیرندگان خرد است.

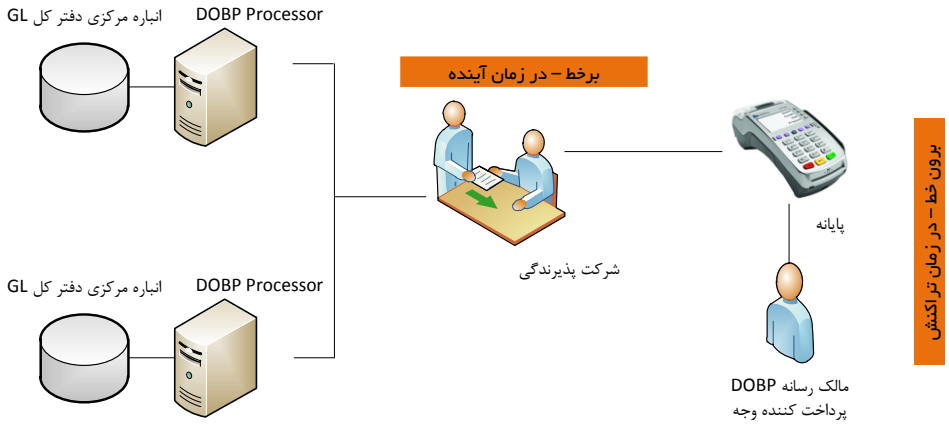
در این شرایط، طرف دریافت کننده وجه DOBP یک رسانه نخواهد بود و درخواست تراکنش از طریق یک ابزار الکترونیکی پذیرش وجه، پایانه فروشگاهی یا دستگاه خود پرداز می‌باشد. نظام DOBP برای این قبیل تراکنش‌ها راه‌کاری را در نظر

گرفته است. فرض کنید یک پایانه فروشگاهی در یک کیوسک روزنامه فروشی، اقدام به پذیرش DOBP نماید. در این شرایط یک کلید خصوصی بر روی پایانه مذکور تولید می‌گردد و بخش عمومی آن جهت تولید گواهینامه پذیرش به مرکز صدور ارسال می‌شود.

با توجه به اینکه فضای اطلاعاتی پایانه فروشگاهی از نظر صادر کننده دارای امنیت کافی نمی‌باشد، لذا امکان انجام عملیات به شکل بین رسانه‌ای برای این پایانه وجود ندارد. در ضمن این مورد در گواهینامه تولید شده برای پایانه فروشگاهی در نظر گرفته می‌شود تا امکان تقلب برای آن وجود نداشته باشد. توضیح بیشتر به این شکل خواهد بود که در صورتی که گواهینامه استاندارد برای پایانه فروشگاهی در نظر گرفته شود، با توجه به اینکه فضای داده‌ای پایانه در اختیار برنامه‌نویس خواهد بود، در زمان دریافت وجه از سایر رسانه‌های DOBP امکان تغییر مقدار برای ایشان میسر خواهد شد. لذا گواهینامه‌های حوزه پذیرش که به این شکل به مرکز صدور ارسال می‌گردند با پارامترهای کنترلی ویژه در محتوای گواهینامه مشخص خواهند شد.

در زمان عملیات انتقال وجه، کلیه فرآیندها دقیقا مانند یک رسانه DOBP انجام می‌پذیرد. پایانه موجودی داخلی خود را افزایش می‌دهد. اما با توجه به نوع گواهینامه پایانه و عدم پذیرش موجودی توسط پردازشگران مرکزی، کل بلاک امضا شده ارسال کننده وجه می‌بایستی بر روی پایانه ذخیره سازی گردد. به منظور کاهش حجم ذخیره سازی تراکنش‌های دریافتی، بعد از بررسی اصالت تراکنش و گواهینامه رسانه پرداخت کننده وجه، نیازی به ذخیره سازی گواهینامه ارسالی از سمت رسانه نمی‌باشد. دلیل این موضوع آن است که کلیه گواهینامه‌های صادر شده در مرکز صدور در اختیار کلیه پردازشگران قرار گرفته-است و صرفا ذخیره سازی سریال منحصر به فرد رسانه به همراه تراکنش امضا شده کافی خواهد بود.

در نهایت می‌بایستی کلیه تراکنش‌های ذخیره شده بر روی پایانه فروشگاهی به منظور انجام عملیات تسویه به یکی از مراکز پردازش تراکنش ارسال گردد. انتخاب مرکز پردازش به دلخواه پایانه بوده و می‌تواند در صورت عدم دسترسی به یکی از آنها بخشی از تراکنش‌ها را برای پردازشگر دیگر ارسال نماید. همچنین امکان ارسال تراکنش‌ها بر روی رسانه‌های فیزیکی مانند دیسک سخت، فلش دیسک، شبکه‌های WIFI محلی جهت تولید فایل و ... نیز وجود دارد.



تصویر ۳ - انجام تراکنش بر روی پایانه

رسانه و پذیرنده‌های اینترنتی

با وجود رشد پذیرنده‌های اینترنتی و افزایش تراکنش‌های الکترونیکی پرداخت از طریق شبکه اینترنت، در DOBP قابلیت پرداخت وجه از طریق اینترنت نیز تعبیه شده است.

با توجه به ماهیت رسانه‌های DOBP که همگی برون‌خط هستند، عملیات انتقال وجه اینترنتی دقیقا مطابق با عملیات انتقال وجه الکترونیکی بر روی پایانه‌های فروش صورت می پذیرد. به این منظور در سمت مشتری می‌بایستی یک ابزار الکترونیکی به جهت پذیرش فیزیکی رسانه موجود باشد. درخواست تراکنش همانند روش پذیرنده فیزیکی تولید می‌گردد و از طریق رابط پذیرش فیزیکی رسانه (کارتخوان‌های کارت هوشمند یا NFC) تراکنش در داخل رسانه DOBP امضا شده و به پذیرنده اینترنتی منتقل می‌گردد. سایر فرآیندهای این حوزه دقیقا مانند پذیرنده فیزیکی خواهد بود و تراکنش‌ها می‌بایستی بعد از ذخیره سازی جهت تسویه‌مالی به یکی از پردازشگران توزیع شده انتقال یابد.

تسویه تراکنش‌های مالی

همانطور که در بخش‌های قبلی عنوان شد، کلیه تراکنش‌های انتقال وجه، در دفتر روزنامه داخلی رسانه ذخیره سازی می‌گردد. گنجایش این دفتر بر اساس توان فیزیکی رسانه و پارامترهای ریسک تعیین شده در مرکز صدور خواهد بود. برای مثال در زمان صدور یک رسانه تعداد حداکثر ۱۰۰ تراکنش تسویه نشده برای رسانه‌ها در نظر گرفته می‌شود.

در این شرایط در زمانی که رسانه به حدمجاز خود برسد، نه قابلیت انتقال وجه خواهد داشت و نه قابلیت دریافت وجه. در این شرایط می‌بایستی جهت انجام عملیات تسویه به یکی از پایانه‌های برخط شامل پایانه‌های فروشگاهی یا دستگاه‌های خودپرداز مراجعه نماید.

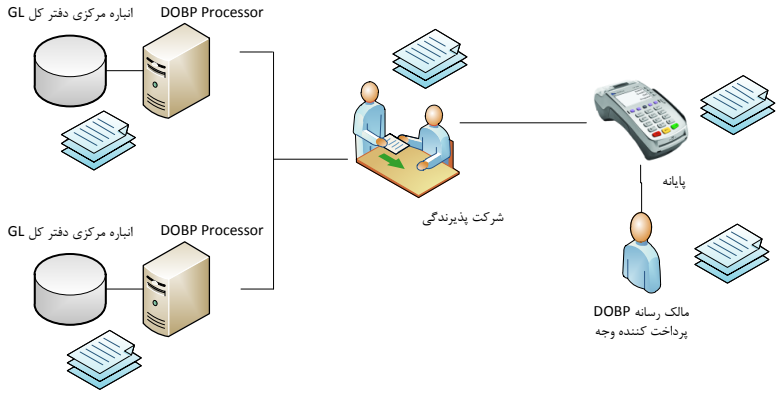
عملیات تسویه به درخواست مالک رسانه انجام می‌گیرد. البته در زمان ضرب وجه الکترونیکی یا تبدیل وجه الکترونیکی به وجه غیر الکترونیکی، با توجه به برخط بودن عملیات، پایانه‌ی رابط، این عملیات را بدون درخواست مالک رسانه انجام خواهد داد. در این فرآیند به شکل زیر عمل می‌شود:

- پایانه برخط متصل به یکی از پردازشگران تراکنش، درخواست تسویه را به رسانه اعلام می دارد.
- رسانه کلیه تراکنش‌های ذخیره شده در دفتر روزنامه خود را جمع بندی کرده، مقدار Challenge تصادفی تولید می‌نماید و به همراه امضای دیجیتال و گواهینامه خود و مشخص نمودن اولین و آخرین شمارنده تراکنش داخلی طی چند بسته اطلاعاتی به پایانه ارسال می‌نماید.
- کلیه داده‌های دریافت شده برای مرکز پردازش ارسال می‌گردند و بعد از بررسی امضا و گواهینامه، کلیه تراکنشها در بلاک‌های ارسال شده جداسازی شده و در انباره دفتر کل ذخیره سازی می‌شوند. در صورتی که تعداد تراکنش‌ها و محتویات آن مقادیر صحیحی باشند و پایانه ارسال کننده ایرادی در اطلاعات ارسالی ایجاد نکرده باشد، درخواست تسویه به مرکز صدور ارسال می‌گردد.
- در مرکز صدور بررسی می‌شود که آیا رسانه مورد نظر قادر به ادامه فعالیت است یا خیر. در صورتی که در بازه زمانی بین دو تسویه، مرکز صدور تصمیم به معدوم سازی یک رسانه نماید، در این مرحله مسدودسازی را از رسانه درخواست می‌نماید.
- سامانه صدور مرکزی در هر دو صورت، یعنی مجوز تسویه یا مسدود سازی رسانه، یک پیام رمز شده و امضا شده

برای پردازشگر درخواست کننده ارسال می کند. این پیام توسط پردازشگر قابل بازگشایی نیست.

- پیام به پایانه درخواست کننده و سپس به رسانه DOBP ارسال می‌گردد.
- بر روی رسانه عملیات رمز گشایی و بررسی امضای مرکز صدور و Challenge تولیدی انجام می‌پذیرد و در صورت صحت اطلاعات، دستور مرکز که شامل تایید عملیات تسویه یا معدوم سازی رسانه است اجرا می‌گردد. در صورتی که عملیات درخواستی تسویه باشد، رسانه شمارنده تسویه خود را صفر نموده و اجازه انجام ۱۰۰ تراکنش دیگر را به مالک رسانه خواهد داد. همچنین مرکز صدور در این تراکنش می‌تواند پارامترهای کنترلی رسانه را تغییر دهد، درخواست تعویض کلید داشته باشد و یا سایر فرآیندهای تعریف شده در آینده را به رسانه ابلاغ نماید.

با استفاده از فرآیند بالا، کلیه تراکنش‌های صورت گرفته بر روی رسانه‌های برون خط DOBP در پردازشگر تراکنش‌ها ذخیره‌سازی می گردد.



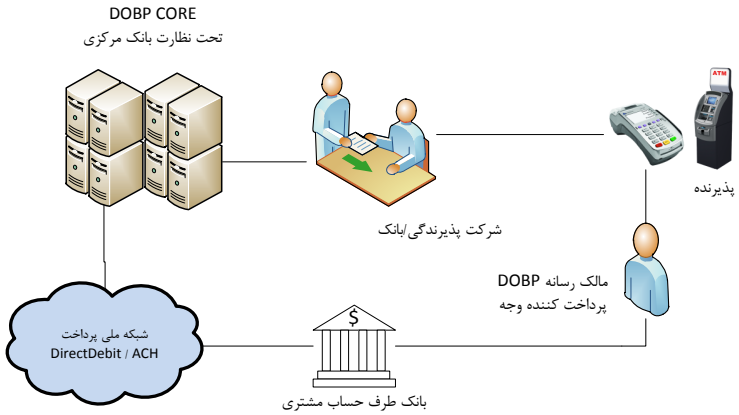
تصویر ۴ - تسویه تراکنشهای رسانه

در رابطه با پایانه‌های فروشگاهی و پذیرندگان اینترنتی نیز به همین صورت عمل می‌گردد. در آنها به دلیل اینکه اعتماد از عملکرد وجود ندارد، کلیه تراکنش‌ها همانطور که گفته شد می‌بایستی با امضای دیجیتال پرداخت کننده وجه ارسال گردند. بعد از دریافت تراکنش ها، گزارشی مبنی بر عملکرد پذیرنده در سامانه تسویه ثبت می‌گردد و در بازه‌های زمانی مشخصی بخشی از وجه بلوکه شده نقدی-ریالی به حجم مجموع تراکنش‌های تسویه شده پایانه برای پذیرنده واریز می‌گردند. در این عملیات که شبیه به تبدیل وجه الکترونیکی به وجه غیر الکترونیکی می‌باشد، مبلغ مشخص شده از چرخه DOBP خارج می‌گردد و نهایتا از حساب مرکزی کسر خواهد شد.

تبدیل وجه الکترونیکی به وجه غیر الکترونیکی

در زمان‌هایی به دلخواه دارندگان DOBP این قابلیت تعبیه شده است که بخشی از وجه ذخیره شده در رسانه، تبدیل به وجه غیر الکترونیکی گردد. در این فرآیند که بر روی پایانه‌های الکترونیکی(پایانه فروشگاهی یا خودپرداز) متصل به DOBP Core Processor صورت می‌پذیرد، ابتدا عملیات تسویه رسانه صورت می‌گیرد. سپس به میزان دلخواه مالک رسانه، تراکنشی به مقصد رسانه مرکزی صورت می‌پذیرد. رسانه مرکزی همانند یک رسانه اینترنتی عمل می‌کند با چند تفاوت اصلی:

- رسانه مرکزی صرفا در اختیار نهاد ناظر خواهد بود و سایر پردازشگران دسترسی به آن ندارند.
- مبلغ تراکنش کمی بیشتر از مبلغ تبدیل درخواست شده است که شامل مبلغ تبدیل و کارمزد تبدیل خواهد بود.
- بعد از انجام تراکنش، مقدار مشخص شده به همراه کارمزد از وجوه بلوکه شده DOBP کسر می‌گردد و از طریق شبکه پایا(ACH) به حساب بانکی مشخص شده مالک رسانه منتقل می‌گردد.



تصویر ۵ - تبدیل وجه الکترونیکی به وجه غیر الکترونیکی

همگام‌سازی تراکنش‌های دریافتی

با توجه به اینکه عملیات تسویه رسانه‌ها یا پذیرندگان با پردازشگران متفاوتی صورت می‌پذیرد، این تراکنش‌ها می‌بایستی جهت مدیریت و پیگیری با هم تجمیع گردند. به این منظور یک پروتکل ارتباطی بین پردازشگران وجود خواهد داشت. طی این پروتکل ارتباطی، کلیه تراکنش های دریافتی توسط یک پردازشگر، با سایر پردازشگران توزیع شده به اشتراک گذاشته خواهد شد. همچنین یک پردازشگر می‌تواند تراکنشی را با آدرس‌دهی خاص شامل رسانه و شمارنده از یک پردازشگر دیگر درخواست نماید.

در رابطه با تراکنشهای فیزیکی پذیرنده و یا اینترنتی، تنها زمانی وجه یک تراکنش به پذیرنده پرداخت می‌گردد که تراکنش به پردازشگر مرکزی رسیده باشد. در این شرایط پردازشگر مرکزی به جز بررسی اصالت تراکنش، شمارنده و آدرس رسانه را جهت جلوگیری از ارسال چندباره تراکنش بررسی می کند. البته پردازشگران توزیع شده نیز، در صورت دریافت تراکنش به صورت تکراری از یک پایانه، در صورتی که در انباره خود تراکنش مربوطه را دریافت کنند، به جای ذخیره سازی تراکنش پیام خطای تکراری بودن را به پایانه مذکور ارسال می‌نمایند. در نهایت وجه یک تراکنش حتی در صورت ارسال برای پردازشگران غیر یکسان، تنها یکبار به پذیرنده پرداخت خواهد شد.

عملیات تایید تراکنش و امضای دیجیتال یک عملیات زمان‌بر خواهد بود، به همین دلیل این عملیات بر روی پردازشگر دریافت کننده وجه صورت می‌پذیرد. سایر پردازشگران وظیفه دارند در صورت دریافت یک تراکنش با مبلغی بالاتر از پارامترهای ریسک تعیین شده توسط پردازشگر مرکزی، اقدام به بررسی مجدد تراکنش نمایند. همچنین پردازشگران دیگر وظیفه دارند برای سایر تراکنش‌ها عملیات تایید تراکنش را به صورت تصادفی و گزینشی انجام دهند.

برای مثال فرض کنید سیاستی به این شکل به پردازشگران اعلام شود:

رقم‌های بالای ۲۵۰،۰۰۰ ریال تایید مجدد و نسبت تصادف یک از ده.

در این شرایط پردازشگران موظف هستند تمامی تراکنشهای دریافتی خود، تراکنشهایی با رقم بالاتر از ۲۵۰،۰۰۰ ریال دریافت شده از دیگر پردازشگران و همینطور یک دهم سایر تراکنش‌های دریافتی را به صورت تصادفی مورد بررسی قرار دهند و در صورت یافتن مغایرت مرکز پردازش مرکزی و سایر مراکز را از این موضوع مطلع نمایند.

امنیت در نظام پرداخت DOBP

با توجه به استفاده از رسانه‌های برون‌خط، حفظ موضوعات مرتبط با امنیت اطلاعات در بالاترین سطوح طراحی DOBP تعبیه گردیده است. این موارد در چند عنوان مجزا تبیین می‌گردد.

ایجاد اصالت در زمان صدور

کلیه رسانه‌های مورد استفاده در DOBP می‌بایستی از نوع هوشمند و دارای قابلیت‌های کلیدی امضای دیجیتال باشند. به همین دلیل در DOBP از کارتهای هوشمند جاوا با قابلیت امضای دیجیتال ECDSA[3] استفاده شده است. همچنین در تلفن‌های هوشمند نیز می توان از سیم‌کارتهای SWP[۱۰] یا از Secure Element بهره‌برداری نمود.

دلیل استفاده از ECDSA کوتاه بودن طول امضای دیجیتال در مقابل کلیدهای هم وزن در RSA می‌باشد.

کلید خصوصی در زمان صدور بر روی رسانه تولید می‌گردد و هیچگاه به بیرون از رسانه درز نخواهد کرد. صرفا کلید عمومی رسانه به منظور تولید گواهینامه در اختیار سامانه صدور قرار خواهد گرفت و سپس گواهینامه امضا شده مجددا بر روی رسانه ثبت می‌گردد.

عملیات صدور در سایت‌های امنیتی مورد تایید DOBP صورت خواهد گرفت تا قابلیت قراردهی Backdoor در نرم افزار رسانه وجود نداشته باشد.

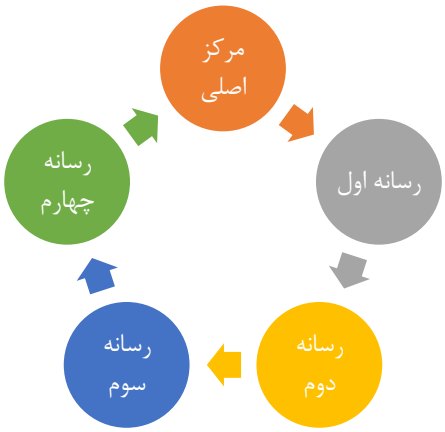
عملیات انتقال وجه

در عملیات انتقال وجه بین دو رسانه یا بین رسانه و پایانه فروشگاهی از امضای دیجیتال مبتنی بر کلید خصوصی رسانه بهره برداری شده است. در عملیات انتقال وجه، از یک شمارنده تراکنش افزایشی غیر بازگشتی به همراه تاریخ و ساعت استفاده می‌گردد که باعث عدم وجود تراکنش تکراری در کل شبکه خواهد بود و بازمصرف تراکنش را به صورت کامل کنترل می‌نماید. همچنین از تابع SHA-256 به منظور تولید HASH مرتبط با امضای دیجیتال استفاده خواهد شد.

ضرب وجه الکترونیکی و عدم خلق پول

[۱۰] Single Wire Protocol

همانطور که در بخشهای قبلی توضیحاتی داده شد، عملیات تبدیل وجه غیر الکترونیکی به وجه الکترونیکی صرفا توسط نهاد ناظر که به پیشنهاد، بانک مرکزی جمهوری اسلامی ایران خواهد بود انجام می پذیرد. در این عملیات وجوه غیر الکترونیکی از چرخه مالی کشور خارج می‌شود و نزد نهاد مربوطه یا بانکهای مورد توافق آن ذخیره سازی می‌گردد. لذا تبعات خلق پول یا افزایش نقدینگی، وجود نخواهد داشت.



پیگیری تراکنش‌های مالی

کلیه تراکنش‌های صورت گرفته در نظام DOBP که به صورت برون خط انجام می‌پذیرند، در زمان تسویه با یکی از مراکز پردازش تسویه می‌گردند و در نهایت در اختیار نهاد ناظر بالا دستی قرار خواهند گرفت. با استفاده از تراکنش‌های دریافت شده در بلاک‌های اطلاعاتی تسویه، قابلیت ردیابی[۱۱]، شناسایی[۱۲] و کنترل جریان نقدینگی[۱۳] وجود خواهد داشت. این ردیابی از زمان تولید وجه در بانک مرکزی خواهد بود و تا آخرین رسانه دریافت کننده ادامه خواهد داشت. حتی در صورت استفاده از رسانه‌های ناشناس در نظام DOBP بازهم امکان کنترل و ردیابی عملیات بدون شناسایی مالک رسانه امکان خواهد داشت.

یافتن تقلب در عملیات

تقلب در DOBP در سه شکل صورت می‌پذیرد:

- رسانه‌ای خارج از حجم دریافت شده اقدام به توزیع وجه نماید: در زنجیره بلوک‌های تراکنشی دریافتی از رسانه، همیشه حجم وجه دریافت شده می بایستی بزرگتر یا مساوی حجم وجه ارسال شده‌باشد. در صورت مشاهده مغایرت که نشان دهنده عدم فعالیت صحیح رسانه می‌باشد، در اولین درخواست تسویه رسانه معدوم می‌گردد.
- پایانه فروشگاهی با تعداد زیاد تراکنش تکراری: پایانه‌ای سعی بر آن دارد که در تعداد بالا، تراکنش‌هایی را به شکل چندباره ارسال نماید. با وجود اینکه تراکنش‌های ارسالی پایانه اشکالی در شبکه ایجاد نمی‌نمایند و با پیام خطا از مرکز پردازش توزیع شده یا مرکز پردازش اصلی روبرو می‌شوند، اما پایانه در صورت عدم اصلاح فرآیندهای خود در لیست سیاه قرارخواهد گرفت و هیچکدام از پردازشگران، تراکنش‌های آن را دریافت نخواهند نمود.

---

[۱۱] Trace
[۱۲] Identification
[۱۳] Cash Flow Control

- پذیرش تراکنش‌های تقلبی توسط یکی از پردازشگران: پردازشگران توزیع شده در DOBP، بر اساس استانداردی مجوز فعالیت خواهند گرفت. با این‌حال این امکان وجود دارد که یک پردازشگر اقدام به ارسال تراکنش‌های غیر صحیح به سایر پردازشگران نماید. در این شرایط در صورتی که توسط یکی دیگر از پردازشگران شناسایی شود، این موضوع به مرکز اصلی پردازش اعلام می‌گردد و پردازنده تراکنش خاطی، از شبکه بیرون رانده خواهد شد. در این شرایط، کلیه تراکنش‌های ارسالی پردازشگر خاطی در گذشته بررسی می‌گردد و خسارت‌های مالی ایجاد شده بر عهده ایشان خواهد بود. در کنار پردازشگران توزیع شده، پردازشگر مرکزی در زمان‌های Off-time یعنی بعد از پذیرش تراکنش تبدیل یا تسویه پذیرنده، اقدام به بررسی موردی تمامی تراکنش‌ها خواهد نمود. زمان سپری شده برای این موضوع با توجه به اینکه بعد از عملیات مالی تراکنش‌ها خواهد بود، تاثیری در عملکرد کل شبکه نخواهد داشت. در صورت زیاد بودن تعداد تراکنش‌ها و افزایش طول صف تراکنش‌های بررسی نشده، سیاستهایی در این زمینه توسط پردازشگر مرکزی به صورت هوشمند اخذ می‌گردد که شامل بررسی تصادفی یا حجم ریالی تراکنش‌ها خواهد بود.

تعویض رسانه‌های DOBP

وجوه فیزیکی تولید شده توسط کشورها که به صورت اسکناس یا سکه یا اوراق بهادار عرضه می‌گردد بعد از مدتی تعویض می‌گردند. این عملیات به منظور کنترل مجدد وجوه و ایجاد اطمینان از عدم جعل آنها می‌باشد.

در DOBP نیز این موضوع به روشی ویژه تعبیه شده است. رسانه‌های DOBP دارای شناسه خاص Wallet Version هستند که در گواهینامه و رسانه هوشمند ایشان درج شده است. فرض کنید بانک مرکزی تصمیم بر آن بگیرد که کلیه رسانه‌های DOBP را به دلایل امنیتی و محافظت بیشتر از شبکه، تعویض نماید. این تعویض به سه شکل خواهد بود:

- تعویض فیزیکی رسانه به دلایل خاص امنیتی
- به روز رسانی نرم افزار رسانه به منظور ایجاد قابلیت‌های جدید و یا استفاده از الگوریتم های امنیتی جدید تر
- به روز رسانی کلید موجود بر روی رسانه و ایجاد گواهینامه جدید

در صورتی که هریک از تصمیمات بالا اخذ شود، عملیات تعویض یا به روز رسانی صورت می‌پذیرد. عملیات تعویض فیزیکی رسانه به این شکل است که رسانه در آخرین تسویه خود مسدود سازی می‌گردد و از مالک آن درخواست می‌شود که جهت دریافت رسانه جدید به صادر کننده خود مراجعه نماید.

در دو مدل به روز رسانی بعدی، عملیات کاملا به صورت نرم افزاری صورت خواهد پذیرفت و مالکان رسانه نمی‌بایستی به محل فیزیکی خاصی مراجعه نمایند، در این فرآیند که به صورت برخط انجام می‌پذیرد، دستورات مرکز به رسانه ارسال می‌گردد و تغییرات مورد نیاز بر روی آن ایجاد می‌شود. دراین فرآیند کلید و گواهینامه رسانه تعویض خواهد شد و Wallet Version جدید بر روی آن نقش خواهد بست.

به دلیل برون خط بودن DOBP عملیات تعویض یا به روز رسانی نمی تواند در یک مرحله و با اجبار صورت پذیرد. لذا برای این موضوع سه مرحله اصلی در نظر گرفته شده است:

- اخطار: در مرحله اخطار، در زمان تسویه و یا برروی پایانه فروشگاهی، اخطاری مبنی بر اینکه هرچه سریعتر رسانه خود را تعویض یا به روز رسانی نمایید ارائه میگردد. در این صورت به دلخواه مشتری عملیات تعویض مورد نیاز

صورت می‌پذیرد و وجوه موجود در رسانه قبلی (فیزیک، نرم افزار یا کلید قبلی) مجددا به صورت یک تراکنش به رسانه فیزیکی جدید یا Wallet جدید منتقل خواهد شد.

- اجبار: در مرحله اجبار، رسانه قابلیت تسویه یا تبدیل را ندارد مگر آنکه رسانه خود را تعویض یا به روز رسانی نماید. البته در این مرحله، انتقال وجه برون خط با نمایش اخطار انجام خواهد پذیرفت. در صورت تعویض یا به روز رسانی رسانه، وجوه مانند مرحله قبلی به Wallet جدید منتقل می‌گردند.
- انکار: در مرحله انکار که با بازه زمانی طولانی از زمان اعلام اخطار انجام می‌پذیرد، رسانه‌های قدیمی نه در محیط برون خط و نه در محیط برخط قابلیت پذیرش نخواهند داشت. این شرایط به دلیل ریسک‌های عملیاتی در نظر گرفته شده است و صرفا زمانی اعمال می‌گردد که کلید خصوصی پردازشگر مرکزی افشا شده باشد یا زمان زیادی از دستور تعویض یا به روز رسانی گذشته باشد. در این شرایط فرد می‌بایستی به صورت فیزیکی به صادر کننده خود مراجعه نماید. تراکنش‌های رسانه به صورت دستی توسط نماینده صادرکننده بررسی می‌گردد و وجوه ذخیره شده در یک رسانه جدید به ایشان ارائه می‌گردد. در این فرآیند کارمزدی به عنوان جریمه اخذ می‌گردد و در ضمن صرفا در مورد رسانه‌های بانام انجام پذیر خواهد بود.

پارامترهای ریسک

به دلخواه مالکان رسانه، چندین پارامتر ریسک بر روی رسانه ایشان در نظر گرفته می‌شود. این پارامترهای ریسک به منظور کنترل سطوح دسترسی به رسانه در صورت مفقودی خواهد بود. البته پارامترهای ریسکی برای پایانه‌ها نیز در نظر گرفته شده است که همگی آنها به شکل جدول زیر می‌باشند:

عنوان پارامتر ریسک	تعویض توسط مالک	تعویض توسط پذیرنده	تعویض توسط مرکز صدور
حداکثر رقم تراکنش انتقال بین رسانه‌ها یا پذیرنده	X(1)	X(1)	X
حداقل رقم تراکنش انتقال بین رسانه‌ها یا پذیرنده	X(2)	X(2)	X
حداکثر رقم انتقال بدون رمز	X		
حداکثر تعداد تراکنش پذیرفته شده بدون تسویه با مرکز		X	
حداکثر تعداد تراکنش بدون عملیات تسویه برخط			X
ساعت مجاز کاری		X	

۱- نمی‌بایستی بیشتر از رقم تعیین شده توسط مرکز صدور باشد

۲- نمی بایست کمتر از رقم تعیین شده توسط مرکز صدور باشد

یافته ها و نتایج

به منظور بررسی عملکرد شبکه DOBP یک سامانه ناظر شبیه‌سازی گردید و تعدادی رسانه مجازی تولید و مورد آزمون قرار گرفتند. در این آزمون فرآیندها به شکل زیر صورت پذیرفت:

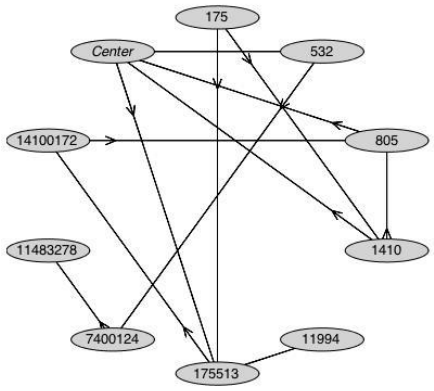
۱- با توجه به عدم نیاز به شبکه برخط تعداد ۲۰۰,۰۰۰,۰۰۰ تراکنش بین ۲۰,۰۰۰,۰۰۰ رسانه جابجا گردید.

۲- پردازش هر تراکنش در زمان تسویه با توجه به استفاده از ECDSA SECP256R1 [4] بر روی یک سرور XEON DUAL 3.4Ghz با ۶۴ گیگابایت RAM زمان 0.004 ثانیه بر روی هر Thread و مجموعا با 24 Thread به مدت ۳۷,۳۵۲ ثانیه معادل ۱۰ ساعت و بیست دقیقه انجام پذیرفت.

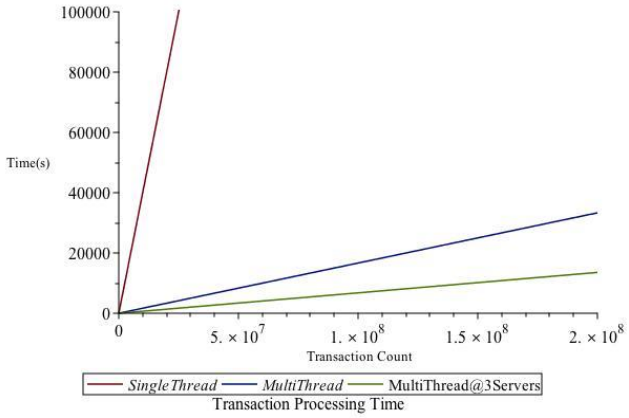
۳- با توجه به طراحی خطی[۱۴] شبکه و قابلیت مقیاس پذیری[۱۵] آن، از سه سرور موازی به صورت توزیع شده بهره برداری گردید. بر اساس پیش بینی صورت گرفته، مدت زمان کل پردازش به دلیل استفاده از تاییدهای مجدد در کل به ۱۴,۷۹۱ ثانیه معادل ۴ ساعت و ۶ دقیقه رسید.

۴- مجموعا به ازای هر ۱۰۰ تراکنش در یک بلوک، حجم ۶۴۸۲ بایت اطلاعات از رسانه‌ها به پردازشگران ارسال گردیده است که مجموع آن در کل شبکه حجم اطلاعاتی ۱۲,۹۶۴,۰۰۰,۰۰۰ بایت بوده است.

با توجه به داده‌های ثبت شده توسط تراکنش‌ها، با وجود تنها سه پردازشگر توزیع شده ، ۲۰۰ میلیون تراکنش خرد در روز تنها نیازمند ۴ ساعت پردازش می‌باشد که با توجه به برون خط بودن تراکنش‌ها این زمان تاثیری در عملیات اصلی تراکنش مالی نخواهد داشت. در ضمن با توجه به اینکه تراکنش‌ها در طی روز توزیع شده می‌باشند، لذا این مدت زمان در طی ۲۴ ساعت توزیع خواهد شد و عملیات تسویه برخط دارندگان رسانه یا پذیرندگان با وجود ۲۰۰ میلیون تراکنش در روز با سرعت بالا در لحظه(با وجود داشتن تنها ۳ پردازشگر) صورت خواهد پذیرفت.



تصویر ۶ - گراف نمایشی چند تراکنش بین رسانه‌ها



تصویر ۷ - مدت زمان صرف شده جهت تایید تراکنشها

[۱۴] Linear

[۱۵] Scalability

جمع‌بندی

کیف پول‌های الکترونیکی طراحی شده در کشور، بدون توجه به برخط یا برون خط بودن نیازمند ارتباط با یک سرویس دهنده مرکزی جهت ارسال تراکنش‌های خود هستند. عدم سرویس دهی مناسب این سرویس دهنده میتواند مشکلاتی را به همراه داشته باشد. با توجه به رشد روز افزون تراکنش‌های خرد و عدم تناسب شبکه شاپرک و شتاب با این تراکنش‌ها ایجاد یک راه-کار C2C بدون نیاز به ارتباط با واحد مرکزی و کاملا برون خط بین رسانه‌ها، میتواند مشکلات این حوزه را به حد بسیار زیادی برطرف نماید.

حذف عملیات شارژ و دشارژ در DOBP نگاه جدیدی به این حوزه است. در کیف پول‌های الکترونیکی همیشه مشکلات مرتبط با شارژ رسانه‌ها از طریق کارتهای بانکی و اعمال هزینه بالا به منظور انجام شارژ با رقم‌های خرد، گریبان گیر این حوزه بوده است. در DOBP عملیات شارژ و دشارژ به صورت کامل حذف شده است و به جای آن انتقال رسانه‌ای به صورت امن در نظر گرفته شده است. همچنین با توجه به محدود نبودن عملیات انتقال وجه، نیازی به اطلاع رسانی کلیه تراکنش‌ها به مرکز اصلی نیست و افراد می‌توانند بعد از ضرب الکترونیکی وجوه آنها را به دفعات بین یکدیگر انتقال دهند و صرفا در صورت نیاز به وجه فیزیکی آنها را در عملیات برخط تبدیل نمایند.

به نگاه ساده‌تر، شارژ یک رسانه DOBP می‌تواند توسط یک رسانه دیگر و به صورت کاملا برون‌خط صورت پذیرد و این مهمترین نکته در کل نظام DOBP به شمار می‌رود.

حذف روشهای تولید وجوه الکترونیکی غیر امن و غیر کنترل پذیر در DOBP به صورت کامل از خلق پول جلوگیری به عمل می‌آورد و در قبال آن نه تنها کنترل کاملی بر روی شبکه اعمال می‌دارد بلکه با استفاده از زنجیره تراکنش‌های مالی قابلیت ردیابی وجوه از زمان تولید در بانک مرکزی تا بازگشت به بانک مرکزی جهت تبدیل پذیری را به صورت کامل مدیریت می-نماید و به نمایش در می‌آورد.

عدم ارسال تراکنش‌های مالی به صورت تک به تک به مرکز اطلاعات، باعث کاهش حجم ترافیک شبکه، پردازش مرکزی، نیاز به برخط بودن و بسیاری منافع دیگر خواهد شد که در نتیجه باعث می‌شود تا DOBP به عنوان یک نظام مستحکم وجه خرد الکترونیکی در داخل جامعه به گردش درآید و بدون توجه به اختلالات شبکه‌ای یا پردازشی در سامانه‌های بالادستی به صورت کامل نیاز روزمره پرداخت خرد را همانند اسکناس و سکه‌های فیزیکی به انجام برساند.

منابع

[1] "CityPay Chip Money e-wallet," *5th Annual Conference on Electronic Banking and Payment Systems*, 2015.

[2] "رویکرد امنیت محور در نظام پرداخت خرد," *6th Annual Conference on Electronic Banking and Payment Systems*, 2016.

[3] "Elliptic Curve Digital Signature Algorithm," [Online]. Available: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

[4] "SECP Crypto Curves," [Online]. Available: http://www.secg.org/sec2-v2.pdf.