PATENTOVÝ SPIS

(11) Číslo dokumentu:
307 164
(13) Druh dokumentu: **B6**
(51) Int. Cl.:

G06Q 20/40	(2012.01)
G06Q 20/28	(2012.01)
G07F 7/08	(2006.01)
G06Q 20/00	(2012.01)
G06Q 30/00	(2012.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2015-562**
(22) Přihlášeno: **20.08.2015**
(40) Zveřejněno: **26.04.2017**
(Věstník č. 17/2017)
(47) Uděleno: **03.01.2018**
(24) Oznámení o udělení ve věstníku: **14.02.2018**
(Věstník č. 7/2018)

(56) Relevantní dokumenty:

US 6557759 A,; CN 103617531 A,; WO 2014145708 A,; CN 104680376 A,; GB 2369915 A,; EP 2975570 A,; CN 1549575 A,; WO 2010028266 A,; WO 2013115665 A,; CN 103927656 A,.

(73) Majitel patentu:
Ing. Petr Sobotka, Praha 8, CZ

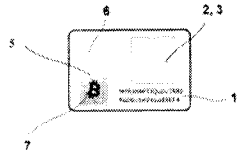
(72) Původce:
Ing. Petr Sobotka, Praha 8, CZ

(74) Zástupce:
PATENTSERVIS Praha a.s., Na Podkovce 281/10, 147 00 Praha 4

(54) Název vynálezu:

Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací a fyzický nosič šifrovacích klíčů pro digitální měnu k provádění tohoto způsobu

(57) Anotace:
Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací spočívá v tom, že na trhu distribuovaný nosič v prázdném stavu, k němuž náleží druhý autorizační faktor (5A) bezpečně uložený u výrobce nebo integrovaný do nosiče ve formě pole v tamper-evident režimu, je výstavcem pomocí SW aplikace pro vystavení nosiče načten a na základě výstavcem vygenerovaného prvního autorizačního faktoru (2A), identifikátoru nosiče a dalších údajů je odvozena a sdělena výstavci adresa pro zaslání zůstatku digitální měny o odpovídající výši shodné s nominální hodnotou nosiče, načež prostřednictvím online služby pro vydávání digitálního podpisu (3A) je na požádání při splnění všech požadovaných náležitostí, zejména autentičnosti kusu nosiče a výši zaslaného zůstatku digitální měny odpovídající nominální hodnotě nosiče, udělen digitální podpis (3A), který SW aplikace pro vystavení nosiče zkombinuje s prvním autorizačním faktorem (2A) a tato data jsou výstavcem doplněna, zejména potisknutím, popsáním nebo polepením, čímž je nosič uveden do aktivního stavu a může být předán dalšímu držiteli, a to i opakovaně, přičemž příjemce provede vizuální kontrolu a ověří nosič za použití SW aplikace pro ověření nosiče, zejména výši zůstatku digitální měny, poté je touto SW aplikací ověřena po načtení prvního autorizačního faktoru (2A) a digitálního podpisu (3A) pravost digitálního podpisu (3A), provede se validace prvního autorizačního faktoru (2A) a příjemce porovná digitálně podepsané údaje s údaji viditelnými na nosiči, načež jsou z tohoto nového řádně vystaveného fyzického nosiče v aktivním stavu příjemcem pomocí SW aplikace pro vyvedení prostředků digitální měny načteny všechny na nosiči dostupné autorizační faktory (2A a/nebo 5A) a eventuálně připojeny další příjemci známé autorizační faktory a sestavena a autorizována elektronická transakce v síti dané digitální měny pro vyvedení prostředků v elektronické podobě na soukromou adresu příjemce, přičemž výsledkem je přenos šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací a tedy uskutečnění platebního styku digitální měnou mezi výstavcem a posledním příjemcem a součástí výsledku je dále nosič ve viditelně znehodnoceném stavu. Pro realizaci způsobu přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací, slouží fyzický nosič šifrovacích klíčů.



CZ 307164 B6

Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací a fyzický nosič šifrovacích klíčů pro digitální měnu k provádění tohoto způsobu

Oblast techniky

Vynález se týká oblasti digitálních měn a elektronických platebních sítí založených na kryptografii a decentralizaci, jako je Bitcoin, Litecoin apod. Vynález se týká způsobů či postupů, jak tyto finanční instrumenty přenést do fyzického světa a vytvořit tak odpovídající fyzickou realizaci tohoto platebního prostředku ve formě nosiče šifrovacích klíčů pro digitální měnu.

Dosavadní stav techniky

Již od vzniku digitální kryptoměny Bitcoin na přelomu let 2008/2009 existovaly pokusy přenést tuto elektronickou měnu do fyzického světa. Nejjednodušším a nejrozšířenějším způsobem je vytvoření tzv. paper wallet, neboli papírové peněženky (obr. 1). Jedná se de facto o zálohu privátního šifrovacího klíče na papír pomocí běžně dostupné kancelářské techniky. Papírová peněženka obsahuje privátní šifrovací klíč v lidsky čitelném textu a většinou i ve strojově čitelném QR kódu. Dále bitcoinovou adresu (opět v textu i v QR kódu) a případně číslici s výší zůstatku, nebo pole, kam lze výši zůstatku zapsat. Vše bývá opatřeno doplňujícím textem, popř. instrukcemi a barevnou grafikou. Papírová peněženka neobsahuje žádné bezpečnostní prvky.

Existuje celá řada webových služeb/softwarových programů pro generování papírových peněženek (lit. 1, 2, 3). Držitel papírové peněženky fakticky disponuje zůstatkem digitální měny na příslušné adrese. Problém je, že kopií papírové peněženky může existovat libovolné množství a proto nelze papírové peněžence jakožto fyzickému objektu přisoudit hodnotu příslušného zůstatku digitální měny. Rovněž nelze papírovou peněženkou platit, neboť příjemce by si nikdy nemohl být jist, zda si plátce nenechal jinou kopii pro sebe. Jedná se skutečně pouze o zálohu privátního klíče, podobně, jako kdybychom si zapsali heslo k elektronickému bankovnictví tužkou na papír. Také jej nebudeme s nikým sdílet, ani se jím pokoušet platit.

V roce 2011 se na trhu objevily bitcoinové mince značky Casascius (obr. 3) a plastové karty značky Bitbills (obr. 2). Oba produkty představují fyzický předmět, který obsahuje integrovaný privátní klíč překrytý destrukční (tzv. tamper–evident) samolepkou. V roce 2013 se pak objevily bitcoinové certifikáty společnosti Bitcoin Suisse AG (obr. 4), které mají privátní klíč vlepen mezi dvě vrstvy syntetického papíru.

Všechny tyto tři produkty trpí zásadním nedostatkem: výrobce zná privátní klíče všech vyrobených kusů daného platebního prostředku. Aktuální držitel tedy není výhradním disponentem digitální měny reprezentované tímto fyzickým objektem, vždy existuje ještě druhý disponent a tím je právě výrobce. Přestože se výrobci zavazují, že informace o privátních klíčích zničili, nebo se chlubí, že při výrobě byly dodrženy vysoké bezpečnostní standardy a garantují, že informace o privátních klíčích neunikly, nelze tuto skutečnost nezávisle ověřit a vždy existuje riziko, že zpočátku čestný výrobce v budoucnu zpronevěří krytí části nebo všech vydaných kusů platebního prostředku, což se rovná okradení svých zákazníků. Odpovídající model disponibility finančními prostředky ukazuje obr. 6.

Tuto situaci se snaží řešit specifikace BIP 38 (lit. 4), která umožňuje vygenerovat privátní klíč chráněný heslem. Výrobce mincí Casascius po určitou dobu (2012-2013) umožňoval svým zákazníkům objednat si mince vyrobené na zakázku podle této specifikace. Postup byl následující: zákazník si na své straně vygeneroval privátní klíč chráněný heslem. Zaslal zaheslovaný klíč výrobci Casascius, který pro něj vyrobil minci a integroval do ní tento chráněný klíč. Mince pak

putovala ke svému objednateli–zákazníkovi. V tomto modelu výrobce nemohl prostředky zpronevěřit, neboť jediný, kdo znal heslo k privátnímu klíči, byl zákazník.

Tento model naplňuje schéma (obr. 7), takže držitel, který si minci objednal, se nemusí bát zpronevěření odpovídajícího krytí digitální měnou. Ovšem takto vydanou minci nelze použít jako platební prostředek. Důvod je prostý: případný příjemce by opět nebyl výhradním disponentem, neboť první držitel, který si minci nechal vyrobit, zná dvojici privátní klíč + heslo. Problém se tak nevyřešil, ale pouze posunul v řetězci držitelů o jeden krok dále, viz obr. 8. Vyjma prvního držitele (resp. objednatele) není aktuální držitel nikdy výhradním disponentem odpovídajícího krytí digitální měnou.

Toto výrobci předmětů založených na BIP38 vědí a své produkty proto nabízejí nikoli jako platební prostředek, ale jako tzv. offline storage (nebo cold storage), čili metodu bezpečného uložení zůstatku v digitální kryptoměně fyzickým způsobem.

Zatím není veřejně známo technické řešení, které by umožňovalo vyrobit a používat fyzický platební prostředek krytý digitální měnou, u něhož bude platit, že aktuální držitel je výhradním disponentem tohoto krytí. Tedy řešení, které by naplňovalo podstatu schématu z obr. 7 a 9.

Podstata vynálezu

Výše uvedené nevýhody existujících fyzických reprezentací digitálních měn odstraňuje způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací, jehož podstata je v tom, že na trhu distribuovaný nosič v prázdném stavu, k němuž náleží druhý autorizační faktor bezpečně uložený u výrobce nebo integrovaný do nosiče ve formě pole v tamper-evident režimu, je výstavcem pomocí SW aplikace pro vystavení nosiče načten a na základě výstavcem vygenerovaného prvního autorizačního faktoru, identifikátoru nosiče a dalších údajů je odvozena a sdělena výstavci adresa pro zaslání zůstatku digitální měny o odpovídající výši shodné s nominální hodnotou nosiče, načež prostřednictvím online služby pro vydávání digitálního podpisu je na požádání při splnění všech požadovaných náležitostí, zejména autentičnosti kusu nosiče a výši zaslaného zůstatku digitální měny odpovídající nominální hodnotě nosiče, udělen digitální podpis, který SW aplikace pro vystavení nosiče zkombinuje s prvním autorizačním faktorem a tato data jsou výstavcem doplněna, zejména potisknutím, popsáním nebo polepením, čímž je nosič uveden do aktivního stavu a může být předán dalšímu držiteli, a to i opakovaně, přičemž příjemce provede vizuální kontrolu a ověří nosič za použití SW aplikace pro ověření nosiče, zejména výši zůstatku digitální měny, poté je touto SW aplikací ověřena po načtení prvního autorizačního faktoru a digitálního podpisu pravost digitálního podpisu, provede se validace prvního autorizačního faktoru a příjemce porovná digitálně podepsané údaje s údaji viditelnými na nosiči, načež jsou z tohoto nového řádně vystaveného fyzického nosiče v aktivním stavu příjemcem pomocí SW aplikace pro vyvedení prostředků digitální měny načteny všechny na nosiči dostupné autorizační faktory a eventuálně připojeny další příjemci známé autorizační faktory a sestavena a autorizována elektronická transakce v síti dané digitální měny pro vyvedení prostředků v elektronické podobě na soukromou adresu příjemce, přičemž výsledkem je přenos šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací a tedy uskutečnění platebního styku digitální měnou mezi výstavcem a posledním příjemcem a součástí výsledku je dále nosič ve viditelně znehodnoceném stavu.

Dále je výhodné, když posledním příjemcem, který provede vyvedení prostředků digitální měny a znehodnocení nosiče, je jeho původní výrobce nebo vydavatel, přičemž k sestavení a autorizaci transakce v digitální měně využije další autorizační faktory, které nejsou na nosiči uvedeny a jsou známy pouze jemu.

Dále je výhodné, když SW aplikace pro vystavení nosiče, SW aplikace pro ověření nosiče a SW aplikace pro vyvedení prostředků digitální měny jsou aplikace ve formě open–source veřejně přístupné na internetové síti. Dále je výhodné, když SW aplikace pro vystavení nosiče, SW aplikace pro ověření nosiče a SW aplikace pro vyvedení prostředků digitální měny tvoří jednu SW aplikaci.

Výše uvedené nevýhody existujících fyzických reprezentací digitálních měn dále odstraňuje pro realizaci způsobu přenosu šifrovacích klíčů digitální měny navržený fyzický nosič šifrovacích klíčů pro digitální měnu, jehož podstata je v tom, že je tvořen základovým tělesem ve formě plochého rovinného objektu libovolného tvaru vytvořeným z kompaktního materiálu, přičemž jedna z jeho hlavních rovinných ploch je označena unikátním alfanumerickým identifikátorem, přičemž fyzický nosič je podle konkrétního provedení opatřen aplikacemi ochranných prvků proti padělání, přičemž na jedné nebo na obou hlavních rovinných plochách jsou dále pole pro umístění prvního autorizačního faktoru a dále pole pro doplnění digitálního podpisu.

Dále je výhodné, když základová tělesa ve formě plochého rovinného objektu jsou ve tvaru geometrického obrazce, výhodně ve tvaru čtverce, obdélníku nebo kruhu.

Dále je výhodné, když fyzický nosič šifrovacích klíčů pro digitální měnu je ve tvaru standardizovaných platebních karet, mincí nebo bankovek.

Dále je výhodné, když fyzický nosič šifrovacích klíčů na jedné z obou stran je opatřen informací o nominální hodnotě a jednotce měny.

Dále je výhodné, když aplikace ochranných prvků proti padělání u listinného provedení jsou bezpečnostní papír s vodoznakem nebo metalickými proužky, opticky variabilní prvky, velmi jemné grafické prvky, tzv. giloše, irisové barevné přechody, barvy s UV nebo IR luminiscencí nebo chemicky reagentní barvy.

Dále je výhodné, když aplikací ochranných prvků proti padělání v případě provedení ve formě plastových karet jsou hologramy.

Dále je výhodné, když aplikací ochranných prvků proti padělání v případě provedení ve formě kovových mincí je difrakční bezpečností prvek kinegram nebo elektronický RFID čip.

Dále je výhodné, když unikátní alfanumerický identifikátor je proveden ve formě chráněného prvku, jako je přelakování iridiscentním lakem, jako je děrování nebo jako opticky variabilní prvek.

Dále je výhodné, když pole pro umístění prvního autorizačního faktoru a pole pro doplnění digitálního podpisu tvoří jedno společné pole.

Dále je výhodné, když na jedné nebo na druhé hlavní rovinné ploše je dále pole pro druhý autorizační faktor vyvedený v tamper–evident režimu.

Dále je výhodné, když kompaktní materiál pro zhotovení fyzického nosiče šifrovacích klíčů je plast a/nebo papír a/nebo kov a/nebo slitiny kovů.

Navržený způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče a fyzický nosič šifrovacích klíčů pro digitální měnu k provádění tohoto způsobu mají společně tyto následující klíčové výhodné vlastnosti:

1. Jedná se o velmi obtížně padělatelnou fyzickou reprezentaci digitální měny.

2. Aktuální držitel je výhradním disponentem digitální měny použité na krytí daného kusu nosiče. Jinými slovy má jistotu, že nikdo z předchozích držitelů, ani subjekt vydavatele nemá možnost krytí zpronevěřit.

3. Pokrýt (vystavit) jej může kdokoli za pomocí běžně dostupné kancelářské a výpočetní techniky a připojení k internetu.

4. Ověřit jej může kdokoli za pomocí běžné dostupné mobilní výpočetní techniky a předem nainstalovaného softwaru, a to i bez připojení k internetu.

5. Ve variantě řešení využívající druhý autorizační faktor vyvedený v tamper-evident režimu může zrušit krytí a vyvést finanční prostředky kdokoli za pomocí běžně dostupné (mobilní) výpočetní techniky a přístupu k internetu, ovšem pouze za současného znehodnocení/evidentního poničení nosiče.

Oproti existujícím fyzickým produktům zaměřeným na uchování zůstatku digitálních měn vynález představuje zásadní kvalitativní posun vpřed, a to především díky bodům 2 a 4.

Při srovnání s běžně dostupnými platebními prostředky, které jsou produktem bank a/nebo států (bankovky, mince, šeky) přináší předložené technické řešení rovněž zásadní inovaci. Běžné dostupné platební prostředky jsou přímo založeny na důvěře (obr. 5) a pokud se vytratí důvěra ve vydavatele, platební prostředek okamžitě ztrácí svoji funkci i hodnotu. Držitel není přímým (faktickým) disponentem příslušného krytí daného platebního prostředku. Jeho postavení vůči vydavateli není rovné a v případě úpadku vydavatele nebo např. měnové reformy zpravidla držitel o hodnotu reprezentovanou těmito substituty zcela přichází.

Technické řešení fyzického nosiče šifrovacích klíčů pro digitální měnu popisuje platební prostředek, který uchovává hodnotu bez ohledu na ekonomický stav vydavatele. Ve variantě, kdy fyzický nosič obsahuje i druhý autorizační faktor vyvedený v tamper–evident režimu dokonce ani úpadek a případná likvidace subjektu vydavatele nemají žádný vliv na hodnotu vystavených nosičů.

Vynalezený fyzický nosič šifrovacích klíčů pro digitální měnu má na rozdíl od zmíněných peněžních substitutů svoji vnitřní hodnotu ekvivalentní zůstatku v digitální měně. Vnitřní hodnota ho připodobňuje např. situaci, kdy je jako platidlo používán přímo drahý kov (zlato, stříbro). Takovéto platidlo, zpravidla mince, má také svoji vnitřní hodnotu, která je nezávislá na subjektu vydavatele.

Předložený vynález umožňuje metamorfózu mezi elektronickou a fyzickou reprezentací peněz provádět v pohodlí domova a bez prostředníka (banky). Stačí mít potřebné množství nekrytých kusů popsaného nosiče a za pomocí běžné kancelářské a výpočetní techniky a připojení k Internetu můžeme změnit elektronickou reprezentaci měny na fyzickou. Ve variantě řešení, kdy fyzický nosič obsahuje i druhý autorizační faktor vyvedený v tamper–evident režimu, je bez prostředníka možná i opačná změna a postačí k ní připojení k Internetu a chytrý mobilní telefon nebo tablet.

Souhrnně lze říci, že absolutní výhodu tohoto vynálezu je, že umožňuje vytvořit fyzický nosič šifrovacích klíčů pro digitální měnu a používat ho k realizaci způsobu přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování tohoto fyzického nosiče, kdy bude platit, že aktuální držitel je výhradním disponentem krytí digitální měnou.

Objasnění výkresů

Obrázek 1 Paper Wallet (papírová peněženka)

Obrázek 2 BitBills

Obrázek 3 Casascius mince

Obrázek 4 Bitcoin Certificates

Obrázek 5 Nepřímá disponibilita krytím

Obrázek 6 Nevýhradní disponibilita krytím

Obrázek 7 Výhradní disponibilita krytím

Obrázek 8 Držitelé vs. disponenti

Obrázek 9 Výhradní disponibilita aktuálního držitele

Obrázek 10 Pouhý vznik fyzické reprezentace

Obrázek 11 Přechod mezi elektronickou a fyzickou reprezentací

Obrázek 12 Tvary nosiče šifrovacích klíčů

Obrázek 13 Mince – lícová strana

Obrázek 14 Mince – rubová strana

Obrázek 15 Bankovka

Obrázek 16 Plastová karta

Obrázek 17 Životní cyklus nosiče šifrovacích klíčů digitální měny

Obrázek 18 Postup vystavení nosiče šifrovacích klíčů

Obrázek 19 Postup ověření nosiče šifrovacích klíčů

Obrázek 20 Postup znehodnocení nosiče šifrovacích klíčů

Příklady uskutečnění vynálezu

Definice základních pojmů

K popisu a vysvětlení činnosti využití fyzického nosiče šifrovacích klíčů pro digitální měnu je potřeba nejprve definovat či ozřejmit některé pojmy. Bitcoin je digitální měna a platební síť, někdy taky označována jako virtuální měna, nebo přesněji jako kryptoměna. Funguje na základě decentralizované P2P sítě počítačových programů s distribuovanou datovou strukturou označovanou jako blockchain a používá asymetrickou kryptografii pro autorizaci transakcí.

Digitálními (krypto)měnami máme v tomto textu na mysli celou rodinu systémů, jako je Bitcoin. Tedy všechny měny a platební sítě fungující jako Bitcoin, měny a platební sítě z něho odvozené, případně měny a platební sítě postavené na stejných principech. Například tedy Litecoin, DogeCoin, PrimeCoin a mnohé další.

Platební prostředek – pokud není uvedeno jinak, tak jde o hmotný předmět vyskytující se v reálném světě sloužící k uchování a transferu hodnoty při platebním styku. Může být označen nominální hodnotou a jednotkou měny. V kontextu tohoto dokumentu se typicky jedná o mince, bankovky, šeky nebo přímo o popsaný vynález.

Fyzický platební styk – úkon, při kterém dojde mezi dvěma subjekty k předání hmotného platebního prostředku o určité nominální hodnotě. Např. zaplacení bankovkou v obchodě.

Fyzický nosič šifrovacích klíčů pro digitální měnu je předmět, jenž je spjat s určitým finančním zůstatkem v platební síti příslušné digitální měny. Je plně legitimní zpravidla pouze tehdy, garantuje-li, že je jediným existujícím nástrojem k manipulaci s příslušným zůstatkem, tzn., že neexistuje více kopií tohoto předmětu se stejným sériovým číslem.

Adresa digitální měny je obdoba čísla bankovního účtu v konvenčním finančním systému.

Veřejný a soukromý (privátní) šifrovací klíč je pár informací, které umožňují realizovat asymetrickou kryptografii.

Tamper–evident je označení pro obecný princip a rodinu technologií, které umožňují detekovat průnik do chráněného prostředí. Jejich cílem není průniku zabránit, jen ho spolehlivě detekovat. Příkladem může být pečeť na dopise, pečetě používané policií pro zajištění dveří nemovitostí, pečetě používané výrobci elektroniky pro detekci neautorizovaného zásahu do zařízení, stírací pole losu atp.

Vydavatel fyzického nosiče šifrovacích klíčů pro digitální měnu je subjekt, který uvádí nosič pod svým jménem/značkou na trh. Může jít o obchodní společnost, banku nebo státní instituci.

Výstavce je uživatel/držitel, který použije nekrytý kus fyzického nosiče šifrovacích klíčů a vystaví jej. Podobně, jako se vystavuje např. šek.

Životní cyklus platebního prostředku

Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací si názorně předvedeme na příkladu životního cyklu platebního prostředku ve formě fyzického nosiče šifrovacích klíčů pro digitální měnu.

Popsaný platební prostředek je na trh distribuován prázdný (nekrytý). Tento stav je na první pohled viditelný, neboť pole 2 pro první autorizační faktor 2A a pole 3 pro digitální podpis 3A jsou prázdná, případné pole 5 pro umístění druhého autorizačního faktoru 5A nepoškozené. V tomto stavu má hodnotu pouze prodejní ceny. Ta může být oproti vyznačené nominální hodnotě zlomková. Nejlepší metaforou pro tento stav je přirovnání k nevyplněnému šeku.

Zákazník může platební prostředek vystavit, neboli pokrýt zůstatkem v digitální měně. Viz oddíl Vystavení fyzického nosiče šifrovacích klíčů. V tento moment nabývá nosič hodnotu odpovídající nominální hodnotě. Vzhledem k tomu, že je nyní doplněna informace prvního autorizačního faktoru 2A a digitální podpis 3A, nosič je na první pohled odlišitelný od předchozího, prázdného stavu.

V krytém stavu lze s nosičem realizovat platební styk, což vyžaduje provést ověření pravosti a krytí nosiče stranou příjemce. Viz oddíl Ověření fyzického nosiče šifrovacích klíčů.

Platebních styků může nosič absolvovat řadu. Při styku nedochází k žádné modifikaci.

Držitel, který si přeje prostředky krytí uvolnit a nadále s nimi nakládat jen elektronicky, přistoupí ke znehodnocení nosiče. Tento proces je popsán v oddíle Znehodnocení fyzického nosiče šifrovacích klíčů. Tím nosič svůj životní cyklus končí. Použití je v tomto smyslu jednorázové a není možná jeho funkční recyklace. V závislosti na použitém materiálu může být ekologicky zlikvidován. Životní cyklus je ilustrován na stavovém diagramu na obr. 17.

Nutná softwarová infrastruktura

K přechodu od prázdného (nekrytého) do krytého stavu, k ověřování a k přechodu z krytého do znehodnoceného stavu (přesněji řečeno k vyvedení krytí znehodnoceného nosiče šifrovacích klíčů pro digitální měnu) je potřeba pomocná softwarová infrastruktura.

a) SW aplikace pro vystavení fyzického nosiče šifrovacích klíčů.

Jejím úkolem je pomoci zákazníkovi sestavit první autorizační faktor 2A, zkombinovat jej s identifikátorem nosiče a případně dalšími údaji za účelem sestavení výsledné adresy, kam bude složen zůstatek v digitální měně určený pro krytí konkrétního kusu fyzického nosiče šifrovacích klíčů pro digitální měnu. Dále aplikace komunikuje s online službou pro vydávání digitálních podpisů 3A a konečně má za úkol připravit podklady pro vhodnou fyzickou realizaci prvního autorizačního faktoru 2A a digitálního podpisu 3A (např. sestavit tisková data pro dotištění na nosič).

b) Online služba pro vydávání digitálních podpisů 3A.

Vydavatel nosiče šifrovacích klíčů provozuje prostřednictvím sítě Internet veřejně dostupnou službu pro vydávání digitálních podpisů 3A. V procesu vystavení nosiče na straně zákazníka dochází k automatické komunikaci s touto online službou a po kontrole všech náležitostí (autenticita fyzického nosiče šifrovacích klíčů s konkrétním identifikátorem, skutečná výše krytí, apod.) je vydavatelem vystaven digitální podpis 3A a zaslán sítí Internet zákazníkovi.

c) SW aplikace pro ověření fyzického nosiče šifrovacích klíčů.

Jejím úkolem je pomoci účastníkovi platebního styku ověřit pravost fyzického nosiče šifrovacích klíčů digitální měny a dále ověřit, že je řádně kryt odpovídajícím zůstatkem digitální měny. Může být určena např. pro mobilní zařízení (jako telefon nebo tablet) vybavené fotoaparátem, nebo pro platební terminál obchodníka vybavený čtečkou čárových kódů, apod. Slouží k facilitaci strojového načtení a vyhodnocení příslušných informací z konkrétního kusu fyzického nosiče šifrovacích klíčů v momentu platebního styku.

d) SW aplikace pro vyvedení prostředků digitální měny.

Slouží k načtení prvního a eventuálně dostupného druhého autorizačního faktoru 5A na znehodnoceném nosiči a sestavení příslušné elektronické transakce v síti dané digitální měny za účelem vyvedení prostředků na soukromou adresu držitele. Jediným úkolem je asistence a facilitace při změně formy měny z fyzické zpět na elektronickou.

Distribuce SW vybavení

Lze vycházet z předpokladu, že vydavatel fyzického nosiče šifrovacích klíčů uvolní aplikace pro vystavování, aplikaci pro ověřování i aplikaci pro vyvedení prostředků ve formě open-source veřejně na Internetu, aby dosáhl větší transparentnosti celého řešení a získal případnou zpětnou vazbu od SW odborníků.

Dále lze předpokládat, že se může objevit veřejně nezávislá implementace uvedené funkcionality pocházející od třetí strany s cílem diverzifikace SW infrastruktury. Tato skutečnost vynález nijak neohrozí, naopak, může posílit robustnost celého řešení.

Softwarová infrastruktura není předmětem ochrany průmyslového vlastnictví a neobsahuje žádnou podstatnou invenci. Slouží hlavně k automatizaci a usnadnění operací s fyzickým nosičem šifrovacích klíčů – vykonává vesměs běžné a dobře zdokumentované výpočetní úkony jako jsou

vystavení digitálního podpisu, ověření digitálního podpisu 3A, komunikace s P2P sítí digitální měny atp.

Způsob realizace dvoufaktorové autorizace

Lze použít více způsobů technické realizace. Buď je privátní klíč rozdělen do více částí, nebo je k jeho sestavení potřeba více informací (viz princip známý jako Shamir Secret Sharing Scheme (lit. 8)), nebo je použita tzv. multisig a/nebo P2SH transakce (lit. 9), která vyžaduje k manipulaci se zůstatkem digitální měny znalost dvou a více privátních klíčů.

Je vhodné podotknout, že kryptografická bezpečnost celého řešení nezávisí na kvalitě prvního autorizačního faktoru 2A vygenerovaného výstavcem. Za předpokladu, že vydavatel garantuje kryptografickou sílu druhého autorizačního faktoru 5A a zavazuje se, že druhý autorizační faktor 5A bude pro každý kus ceniny unikátní a dále za předpokladu, že zřetězení obou faktorů 2A, 5A bude definováno pouze jedním možným způsobem, pak i v případě, že výstavce použije pro více kusů platebního prostředku stejný první autorizační faktor 2A, případně pokud použije kryptograficky slabou informaci s nízkou mírou entropie, neohrozí to bezpečnost řešení ve smyslu potenciálního útoku třetí stranou.

Způsob realizace digitálního podpisu

Konkrétní schéma digitálního podpisu 3A není pro realizaci vynálezu podstatné. Jeví se jako žádoucí použít digitální podpis 3A založený na asymetrické kryptografii a tzv. Public Key Infrastructure (PKI). Konkrétní algoritmy mohou být např. DSA, ECDSA.

Vystavení fyzického nosiče šifrovacích klíčů

Postup vystavení je vyobrazen na obr. 18. Nejprve si musí zákazník-výstavce opatřit prázdný (nekrytý) kus nosiče šifrovacích klíčů. Dále potřebuje výpočetní techniku s přístupem na Internet a SW aplikaci pro vystavení. Pomocí ní vygeneruje, nebo z jiného zdroje načte první autorizační faktor. Dále z fyzického nosiče šifrovacích klíčů digitální měny načte jeho identifikátor, případně další pomocné informace určené k sestavní adresy krytí. Aplikace odvodí adresu krytí a sdělí ji výstavci. Ten následně na tuto adresu zašle krytí o odpovídající výši (shodné s nominální hodnotou platebního prostředku). Poté požádá prostřednictvím aplikace pro vystavení online službu vydavatele o vystavení digitálního podpisu 3A. Pokud jsou všechny náležitosti splněny (jde o autentický kus platebního prostředku, výše zaslaného krytí odpovídá nominální hodnotě, a další), digitální podpis 3A je udělen. Aplikace pro vystavení jej pak vhodně zkombinuje s prvním autorizačním faktorem 2A a připraví do formátu, který může výstavce použít pro vhodný způsob doplnění na nosič. Např. připraví tiskový podklad pro dotisk.

Jakmile jsou potřebné informace na nosič doplněny, je proces vystavení u konce a vznikl nový řádně krytý fyzický nosič šifrovacích klíčů. Výstavce si jej může pro svoji vlastní kontrolu ověřit, viz níže.

V tuto chvíli výstavce nemůže disponovat prostředky, které na krytí poskytl, jinak, než znehodnocením nosiče (viz níže). Nemůže stejnými prostředky pokrýt jiný kus, nebo s nimi platit v digitální formě v jiném platebním styku. Prostředky jsou pevně vázány na konkrétní kus nosiče a jeho aktuální držitel je výhradním disponentem příslušného krytí v digitální měně.

Ověření fyzického nosiče šifrovacích klíčů

Postup ověření je zobrazen na obr. 19. Ověřitel (zpravidla příjemce fyzického nosiče šifrovacích klíčů) použije softwarovou aplikaci pro ověření. Může ji volně získat ze sítě Internet. V momentě ověřování však již připojen k Internetu být nemusí, a to bez ohledu na počet ověřovaných nosičů. Ověřitel nejprve vizuálně zkontroluje nosič a zjistí, zda není nekrytý (čili zda nejsou pole 2 pro

první autorizační faktor 2A a pole 3 pro digitální podpis 3A prázdná). Pokud se mu dostane do ruky evidentně nekrytý, tj. prázdný kus nosiče, odmítne jej rovnou jako plnění přijmout. Dále pokračuje ve vizuální kontrole a v závislosti na konkrétní realizaci vynálezu kontroluje ochranné prvky, např. v případě papírového provedení vodoznak, hologram atp.

Poté spustí softwarovou aplikaci, načte z nosiče první autorizační faktor 2A a digitální podpis 3A a aplikace mu sdělí, zda je digitální podpis 3A pravý a ke kterému kusu nosiče a ke které nominální hodnotě se vztahuje. Ověřitel vizuálně zkontroluje, že kus, který drží v ruce skutečně je označen touto nominální hodnotou a opatřen shodným identifikátorem a pokud dojde k závěru o shodě, přijme nosič. Pokud by zjistil rozdíl v identifikátoru nebo nominální hodnotě, nosič odmítne jako plnění přijmout.

Součástí kontroly pomocí softwarové aplikace je i validace prvního autorizačního faktoru 2A. Pokud by kus obsahoval chybný, poškozený nebo zcela neodpovídající první autorizační faktor 2A, aplikace na tuto skutečnost ověřitele upozorní a ověření skončí negativním výsledkem.

Znehodnocení fyzického nosiče šifrovacích klíčů

Postup znehodnocení je zobrazen na obr. 20. V tomto momentě máme na mysli znehodnocení se záměrem převedení odpovídajícího krytí zpět do elektronické podoby. Samozřejmě, že existují široké možnosti, jak prostředek v závislosti na použitém materiálu zničit, např. žárem, chemickými rozpouštědly atp. Pouhé fyzické zničení bez předchozího načtení prvního a eventuálně druhého autorizačního faktoru 2A event. 5A by se však rovnalo kompletnímu nevratnému zničení odpovídajících jednotek digitální měny. (Obdobou je např. spálení platné bankovky). Očekáváme, že většina uživatelů bude vedena racionálními pohnutkami a motivací ke zničení bude právě získání použité digitální měny.

Uživatel načte první autorizační faktor 2A, v případě, že je přítomen i druhý autorizační faktor 5A v tamper–evident režimu, odstraní tamper–evident ochranný prvek tak, aby se dostal k informaci o druhém autorizačním faktoru 5A. V praxi se může jednat o setření stíracího pole, odlepení destrukční samolepky, rozlomení nebo roztržení těla prostředku apod. Následně uživatel použije SW aplikaci pro vyvedení prostředků na svoji soukromou adresu.

Konstrukční podstata navrženého řešení fyzického nosiče

V textu příkladů a připojených obrázcích si nejprve uvedeme základní prvek způsobu přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací, tedy konstrukci fyzického nosiče šifrovacích klíčů pro digitální měnu. Ten je tvořen základovým tělesem ve formě plochého rovinného objektu libovolného tvaru, zejména geometrického obrazce, vytvořený z kompaktního materiálu, zejména plastu, papíru či kovů a jejich slitin, přičemž jedna z jeho hlavních rovinných ploch je označena unikátním alfanumerickým identifikátorem 1, přičemž tento fyzický nosič šifrovacích klíčů pro digitální měnu je podle konkrétního provedení opatřen aplikacemi ochranných prvků proti padělání, přičemž na jedné nebo na obou hlavních rovinných plochách jsou pole 2 pro umístění prvního autorizačního faktoru 2A, pole 3 pro doplnění digitálního podpisu 3A, případně dále pole 5 pro umístění druhého autorizačního faktoru 5A vyvedeného v tamper–evident režimu.

Základové těleso ve formě plochého rovinného objektu je s výhodou ve tvaru čtverce, obdélníku nebo kruhu, případně je výhodně ve tvaru standardizovaných platebních karet, mincí nebo bankovek. Na jedné z obou stran základového tělesa je informace 4 o nominální hodnotě a jednotce měny. Na fyzickém nosiči šifrovacích klíčů v případě listinného provedení jsou aplikace ochranných prvků proti padělání, zejména speciální bezpečnostní papír s vodoznakem nebo metalickými proužky, opticky variabilní prvky, použití velmi jemných grafických prvků, tzv. gilošů, irisových barevných přechodů, použití barev s UV nebo IR luminiscencí nebo chemicky reagentních barev či použití nedostupných tiskových metod, v případě provedení ve formě plastových karet aplika-

ce ochranných prvků proti padělání jsou zejména hologramy a v případě provedení ve formě kovových mincí aplikací ochranných prvků proti padělání je výhodně difrakční bezpečností prvek kinegram nebo elektronický RFID čip. Unikátní alfanumerický identifikátor 1 je vyveden ve formě chráněného prvku, zejména přelakováním iridiscentním lakem, provedením jako děrování nebo jako opticky variabilní prvek.

Jednou z variant řešení je pole 2 pro umístění prvního autorizačního faktoru 2A a pole 3 pro doplnění digitálního podpisu 3A, která tvoří jedno společné pole.

Technické řešení fyzického nosiče šifrovacích klíčů pro digitální měnu využívá tyto základní stavební kameny: ochranné ceninové prvky, vícefaktorovou autorizaci, digitální podpis a eventuálně tamper–evident vlastnosti.

Předmětem vynálezu je fyzický objekt, který je chráněn proti padělání ochrannými prvky a je identifikován jedinečným alfanumerickým identifikátorem 1. Zároveň obsahuje pole 2 pro doplnění prvního autorizačního faktoru 2A, který po řádném vystavení nosiče tvoří nejvýše polovinu informace, která je nutná k disponibilitě digitálním krytím, a dále objekt obsahuje pole 3 pro doplnění digitálního podpisu 3A. Doplnění těchto dvou informací se děje až na straně zákazníka, zákazník také poskytne prostředky v digitální měně, které jsou na krytí nosiče potřeba. Dále je výhodné, když objekt fyzického nosiče šifrovacích klíčů obsahuje pole 5 druhého autorizačního faktoru 5A chráněného ochranným prvkem s tamper–evident vlastnostmi, jinými slovy čitelného pouze za současného evidentního znehodnocení/poničení celého objektu.

Podrobný popis věci

Rozměry, hmotnost, materiál a tvar: konkrétní realizace nosiče šifrovacích klíčů pro digitální měnu může teoreticky nabývat libovolných rozměrů, nicméně aby bylo jeho užití při fyzickém platebním styku mezi osobami praktické a pohodlné, lze předpokládat, že by měly jednotlivé kusy nabývat rozměrů v jednotkách až desítkách centimetrů, přičemž jejich objem by měl být minimalizován, aby byly nenáročné na prostor pro skladování.

Podobně i hmotnost by neměla překročit několik jednotek gramů, neboť manipulace s výrazně hmotnějšími kusy nosičů šifrovacích klíčů by jistě vedla ke snížení ergonomie platebního styku. Teoreticky však nic nebrání výrobě libovolně hmotného kusu nosiče.

Materiál opět není přesně stanoven. Lze však předpokládat použití takového materiálu, který zajistí trvanlivost, rozumnou odolnost proti opotřebení a který bude nabízet přijatelné výrobní náklady i ve velkých množstevních sériích. Typicky se jedná o papír, plast nebo kov.

Ani tvar předmětného vynálezu není nijak určen, lze však předpokládat, že půjde o rovinný (přesněji řečeno plochý) útvar.

Rozměry, hmotnost, materiál ani tvar nejsou pro realizaci vynálezu podstatné, nesmí však bránit použití v textu uvedených klíčových prvků, které fyzický nosič šifrovacích klíčů musí obsahovat.

V tomto textu pracujeme se třemi možnými fyzickými realizacemi, které se rozměry, hmotností, materiálem i tvarem nejvíce podobají existujícím etablovaným platebním prostředkům, jedná se o minci, bankovku a plastovou kartu (obr. 12). Znovu však zdůrazňujeme, že možné realizace předmětného vynálezu nejsou na tyto tři varianty omezeny a teoreticky lze vyrobit i zcela jiné variace materiálů, hmotností, rozměrů a tvarů.

Ochrana proti padělání a napodobení

Nosič šifrovacích klíčů musí maximálně ztížit případné pokusy o padělání. V případě listinného (papírového/polymerového) provedení se použije ceninový tisk, což je souhrnný název pro vý-

robní procesy vedoucí k výrobě a aplikaci nejrůznějších ochranných prvků, které známe např. z bankovkové produkce. Jedná se např. o speciální bezpečnostní papír s vodoznakem a/nebo metalickými proužky, aplikaci tzv. opticky variabilních prvků ("hologramy", iridiscentní lak, speciální barvy), použití běžně nedostupných tiskových metod jako je např. hlubotisk nebo vysoce přesný offsetový tisk, použití velmi jemných geometrických grafických prvků (tzv. gilošů), irisových barevných přechodů, barev s UV nebo IR luminiscencí, termochromních barev, chemicky reagentních barev atp. Ochranných prvků a metod existuje velmi mnoho a jejich konkrétní výběr závisí na volbě a výrobních možnostech výrobce platebního prostředku.

Plastové karty lze taktéž vybavit opticky variabilními prvky ("hologramy"), případně potisknout speciálními barvami, embosovat atd. Kovové mince lze vybavit opticky variabilním prvkem KINEGRAM (lit. 5), nebo elektronickým RFID čipem (lit. 6).

Rozlišitelnost a jedinečnost

Každý jednotlivý kus nosiče musí být označen jedinečným alfanumerickým identifikátorem 1. Jedinečnost zajišťuje sám výrobce výběrem vhodné množiny identifikátorů, přičemž množina nemusí tvořit spojitou řadu, naopak se jeví jako výhodné použít dostatečně dlouhé řetězce, které se na první pohled tváří náhodné, např. takto:

4DaFvf3RumoW67B2rXAMdx72VycebHksU

KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM

NH9od4H3XQupviN8pRGQ6uteVm1qd9KF4, atd.

Takovéto identifikátory, pokud mají dostatečnou délku a poskytují tedy dostatečně velký kombinatorický prostor, v podstatě vylučují, aby se je případný padělatel pokusil odhadnout a vyrobil tak padělky i těch kusů, které nemá k dispozici. Ověření pravosti (viz dále) zahrnuje automatizovanou kontrolu identifikátoru, a padělek s nevyhovujícím, např. vymyšleným, identifikátorem by byl ihned odhalen.

Příklady použití alfanumerických identifikátorů 1 jsou na obr. 13, 15 a 16.

Ochrana proti pozměnění identifikátoru

Vzhledem k podstatě vynálezu, kdy se na volném trhu vyskytují jak nekryté (prázdné) kusy nosiče, tak řádně kryté, a tudíž není pravda, že by každý kus ceniny měl za všech okolností hodnotu odpovídající vyznačené nominální hodnotě, je potřeba maximálně ztížit případné snahy o pozměnění identifikátoru, neboť touto cestou by bylo možné z nekrytého kusu vyrobit imitaci kusu krytého. Na konkrétním případě uveďme, že kdyby byl identifikátor vyveden jako obyčejné číslo ze spojité řady a vytištěné běžnou tiskovou technikou, stačilo by útočníkovi opatřit si dva originální nekryté kusy opatřené po sobě jdoucími identifikačními čísly. Jeden by řádně pokryl digitální měnou a vystavil tak platný nosič šifrovacích klíčů, druhý kus by však pozměnil tak, aby se identifikátor shodoval s prvním kusem a dále na něj přenesl i další klíčové prvky (viz v dalším textu), získal by velmi zdařilé falzum. V případě číselného identifikátoru ze spojité řady totiž u dvou po sobě jdoucích čísel stačí pozměnit jedinou (konkrétně koncovou) číslici. Naopak při použití dlouhých alfanumerických identifikátorů 1 z nespojité řady, jak bylo nastíněno výše, by útočník musel pozměnit velmi mnoho znaků, často celý řetězec. Pokud bude identifikátor navíc vyveden jako chráněný prvek, např. přelakováním iridiscentním lakem, vysázením knihtiskem, proveden jako děrování, případně ve formě opticky variabilního prvku, pak bude mít případný útočník pokusy o pozměnění velmi ztížené a nebude tak moci realizovat útok na ceninu metodou pozměnění identifikátoru.

Pole 2 pro doplnění prvního autorizačního faktoru 2A

Na nosiči šifrovacích klíčů pro digitální měnu je umístěno jasně viditelné pole 2 pro doplnění prvního autorizačního faktoru 2A, neboli první části informace, které je potřeba k disponibilitě částkou digitální měny, která je použita ke krytí nosiče. Není podstatné, jakým způsobem je první autorizační faktor 2A připojen: může být na nosič dotištěn, nalepen, ručně dopsán, vyryt, proděrován, vypálen laserem, vybroušen atp.

První autorizační faktor 2A nemusí být chráněn bezpečnostními prvky, pouze musí být zajištěna jeho čitelnost a rozumná míra trvanlivosti a odolnosti pro účely fyzického platebního styku. Pole 2 pro doplnění prvního autorizačního faktoru 2A proto nemusí využívat žádnou speciální technologii.

Prvek je zachycen na obr. 14, 15 a 16.

Pole 3 pro doplnění digitálního podpisu 3A

Na nosič šifrovacích klíčů pro digitální měnu je umístěno jasně viditelné pole 3 pro doplnění digitálního podpisu 3A. Není podstatné, jakým způsobem je digitální podpis 3A připojen: může být na nosič dotištěn, nalepen, ručně dopsán, vyryt, proděrován, vypálen laserem, vybroušen atp.

Digitální podpis 3A nemusí být chráněn bezpečnostními prvky, pouze musí být zajištěna jeho čitelnost a rozumná míra trvanlivosti a odolnosti pro účely fyzického platebního styku. Pole 3 pro doplnění digitálního podpisu 3A proto nemusí využívat žádnou speciální technologii.

Digitálním podpisem 3A se v tomto bodě myslí fyzická reprezentace dat, které vznikly metodou digitálního podpisu. Data mohou být reprezentována v binární, oktalové, desítkové, hexadecimální nebo jiné vhodné soustavě a provedena jako alfanumerický řetězec čitelný pouhým okem, nebo strojově čitelný grafický obrazec (čárový kód, prostorový čárový kód), případně obojí dohromady.

Za určitých okolností může být praktické zkombinovat první autorizační faktor 2A a digitální podpis 3A do jediného pole a zjednodušit tak proces vystavení i proces ověřování nosiče. Tato varianta nosiče šifrovacích klíčů má tedy pouze jedno pole pro doplnění obou informací najednou. Znázorněno na obr. 14a 16.

Druhý autorizační faktor 5A

Druhá část informace chránící krytí digitální měnou je poskytnuta výrobcem nosiče, označujeme ji jako druhý autorizační faktor 5A. V závislosti na tom, zda je druhý autorizační faktor 5A integrován do nosiče, se nabízejí dvě odlišné varianty provedení celého řešení.

a) Výhodné je druhý autorizační faktor 5A začlenit do nosiče ve formě pole chráněného v tamper–evident režimu, neboli tak, aby byla spolehlivě zajištěna detekce průniku, přičemž v tomto případě se průnikem myslí pouhé přečtení druhého autorizačního faktoru. Cílem tedy je, aby druhý autorizační faktor 5A byl na nosiči vyveden tak, že při jeho přečtení dojde k současné viditelné (evidentní) změně příslušného prvku, nebo celého nosiče tak, aby se na první pohled jevil jako znehodnocený. Příkladem může být stírací pole známé z výherních losů, nebo destruktivní nálepka, kterou používají bankovní společnosti pro zaslání PINu k platebním kartám poštou. Případně lze zapouzdřit druhý autorizační faktor 5A uvnitř v těle platebního prostředku tak, aby k jeho přečtení bylo nutné rozebrání/rozdělení prostředku na dvě části. Tento přístup používá (lit. 7). Důležité je, aby proces pozměnění byl nevratný a aby byl spolehlivý, tzn., nebylo možné jej obejít a informaci získat bez současného evidentního pozměnění/znehodnocení, a to ani sofistikovanými fyzikálními nebo chemickými metodami.

Pokud nosič šifrovacích klíčů pro digitální měnu obsahuje druhý autorizační faktor 5A ve formě pole v tamper–evident režimu, není pro zpětnou změnu reprezentace měny z fyzické na elektronickou potřeba žádný prostředník a poslední držitel může prostředky použité ke krytí nosiče vyvést, postačí k tomu "chytrý" mobilní telefon nebo tablet s příslušným SW vybavením a připojení k Internetu. Zároveň je tato varianta řešení pro výrobce nosiče jak technicky, tak finančně náročnější.

b) Výrobně jednodušší a zároveň levnější může být varianta řešení, která počítá s tím, že druhý autorizační faktor zůstává po celou dobu znám pouze vydavateli nosiče šifrovacích klíčů a není do nosiče integrován. Zároveň se však v této variantě provedení vydavatel stává jediným subjektem, který je schopen z fyzické reprezentace digitální měny ve formě nosiče šifrovacích klíčů udělat zpět elektronickou reprezentaci, neboli vyvést krytí. V praxi to znamená, že pokud se aktuální držitel řádně vystaveného (krytého) nosiče rozhodne změnit reprezentaci měny z fyzické zpět na elektronickou, musí nosič doručit zpět vydavateli a od něj pak obdrží příslušné prostředky. Zároveň vydavatel musí garantovat, že při zpětvzetí nosiče dojde i k jeho definitivnímu zničení.

Nutnost návratu nosiče k vydavateli za účelem zrušení krytí činí tento model logisticky i procesně náročnější a činí z vydavatele centrální bod pro potenciální útoky padělatelů, odpadají však náklady na tamper–evident technologie, což může výrobu fyzického nosiče šifrovacích klíčů výrazně zlevnit.

Nominální hodnota

Nosič šifrovacích klíčů pro digitální měnu v krytém stavu by měl vždy obsahovat jasně čitelnou informaci 4 o nominální hodnotě a jednotkách měny, případně název měny samotné.

Nosič může být s touto informací již vyroben a dodán na trh v několika různých nominálních hodnotách, nebo lze nechat volbu nominální hodnoty na výstavci (podobně, jako je tomu u šeků). V takovém případě musí nosič disponovat adekvátním polem pro doplnění této informace (obr. 16).

Rozmístění prvků

Prvky jsou v rámci nosiče šifrovacích klíčů pro digitální měnu rozmístěny v souladu s ergonomií použití, přičemž je zohledněn především postup pro ověřování nosiče jakožto předpokládaná nejčastější činnost, která je s nosičem prováděna. Sekundárně jsou vzaty do úvahy i postupy vystavení a znehodnocení. Teoreticky však na konkrétním rozmístění prvků nezáleží a podstatu předloženého technického řešení to nijak neovlivní. Papírová forma (obr. 15) by tak např. nemusela mít všechny prvky na lícové straně, ale obě pole pro dotisk by bylo možno přesunout na rubovou stranu. Úprav se nabízí celá řada.

Vlastnosti fyzického nosiče šifrovacích klíčů a způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací – shrnutí inovace

Navržený nosič šifrovacích klíčů pro digitální měnu má následující klíčové vlastnosti:

1. Jedná se o velmi obtížně padělatelnou fyzickou reprezentaci digitální měny.

2. Aktuální držitel je výhradním disponentem digitální měny použité na krytí daného kusu nosiče. Jinými slovy má jistotu, že nikdo z předchozích držitelů, ani subjekt vydavatele nemá možnost krytí zpronevěřit.

3. Pokrýt (vystavit) jej může kdokoli za pomocí běžně dostupné kancelářské a výpočetní techniky a připojení k internetu.

4. Ověřit jej může kdokoli za pomocí běžné dostupné mobilní výpočetní techniky a předem nainstalovaného softwaru, a to i bez připojení k internetu.

5. Ve variantě řešení využívající druhý autorizační faktor 5A vyvedený v tamper–evident režimu může zrušit krytí a vyvést finanční prostředky kdokoli za pomocí běžně dostupné (mobilní) výpočetní techniky a přístupu k internetu, ovšem pouze za současného znehodnocení/evidentního poničení nosiče.

Oproti existující fyzickým produktům zaměřeným na uchování zůstatku digitálních měn představuje předložené technické řešení zásadní kvalitativní posun vpřed, a to především díky bodům 2 a 4 této kapitoly.

Při srovnání s běžně dostupnými platebními prostředky, které jsou produktem bank a/nebo států (bankovky, mince, šeky) přináší předložené technické řešení rovněž zásadní inovaci. Běžné dostupné platební prostředky jsou přímo založeny na důvěře (viz obr. 5) a pokud se vytratí důvěra ve vydavatele, platební prostředek okamžitě ztrácí svoji funkci i hodnotu. Držitel není přímým (faktickým) disponentem příslušného krytí daného platebního prostředku. Jeho postavení vůči vydavateli není rovné a v případě úpadku vydavatele nebo např. měnové reformy zpravidla držitel o hodnotu reprezentovanou těmito substituty zcela přichází.

Naproti tomu předkládané technické řešení popisuje platební prostředek, který uchovává hodnotu bez ohledu na ekonomický stav vydavatele. Ve variantě, kdy fyzický nosič obsahuje i druhý autorizační faktor 5A vyvedený v tamper–evident režimu, dokonce ani úpadek a případná likvidace subjektu vydavatele nemají žádný vliv na hodnotu vystavených nosičů šifrovacích klíčů pro digitální měnu jakožto platebních prostředků. Ty i nadále plní svoji funkci uchovatele hodnoty a facilitátora platebního styku.

Tento nosič šifrovacích klíčů pro digitální měnu má na rozdíl od zmíněných peněžních substitutů svoji vnitřní hodnotu ekvivalentní zůstatku v digitální měně. Vnitřní hodnota ho připodobňuje např. situaci, kdy je jako platidlo používán přímo drahý kov (zlato, stříbro). Takovéto platidlo, zpravidla mince, má také svoji vnitřní hodnotu, která je nezávislá na subjektu vydavatele.

Řešení nosiče šifrovacích klíčů pro digitální měnu jako platebního prostředku si ponechává výhody shodné s běžnými moderními fyzickými platebními prostředky – nízkou váhu a malou velikost. Bankovky byly zavedeny mj. proto, že manipulace s větším množstvím fyzického zlata se jevila nepraktická. Stejně tak vynalezený nosič šifrovacích klíčů představuje nástroj pro usnadnění platebního styku osobám, pro něž je manipulace s digitální měnou ve své nativní elektronické podobě nepraktická. Zároveň si však zachovává svoji vnitřní hodnotu, takže se nejedná o substitut, ale spíše o fyzickou "obálku" pro elektronickou měnu.

Na navržené řešení se lze dívat jako na nástroj pro metamorfózu digitální měny z elektronického prostředí do fyzického prostředí a zpět (obr. 11). Přičemž je důležitý ten fakt, že v momentě, kdy měna přejde do fyzického světa, nadále neexistuje nikdo, kdo by s ní mohl disponovat v původním elektronickém světě. Takto je možné jinak popsat zmíněný princip výhradní disponibility aktuálního držitele. Doposud existující fyzické produkty týkající se digitálních měn totiž používají schéma z obr. 6, kdy v momentě vystavení prostředku existují dva disponenti, a to vydavatel a držitel a může tak kdykoli v budoucnosti dojít k situaci znázorněné na obr. 10, tedy že "elektronický disponent" s finančními prostředky dále nakládá a "fyzický disponent" při pokusu o znehodnocení předmětu a vyvedení krytí zpět do elektronického prostředí zjistí, že již skutečným disponentem není a že byl okraden.

Metamorfózu mezi elektronickou a fyzickou reprezentací peněz běžně provádíme, když neseme do banky/bankomatu hotovost a vložíme ji na účet, nebo naopak když v bance/bankomatu uskutečníme výběr z účtu a odneseme si hotovost.

Předložené řešení umožňuje tuto metamorfózu provádět v pohodlí domova a bez prostředníka (banky). Stačí mít potřebné množství nekrytých kusů popsaného nosiče šifrovacích klíčů pro digitální měnu a za pomocí běžné kancelářské a výpočetní techniky a připojení k internetu můžeme změnit elektronickou reprezentaci měny na fyzickou. Ve variantě řešení, kdy fyzický nosič obsahuje i druhý autorizační faktor 5A vyvedený v tamper–evident režimu, je možná i opačná změna a postačí k ní připojení k Internetu a chytrý mobilní telefon nebo tablet.

Předložené řešení zároveň nepostrádá sekundární funkci bezpečného offline úložiště digitální měny, čili jím lze nahradit i papírové peněženky a jiné formy zálohy privátních klíčů. I v případě, že není použit k platebnímu styku, tedy zůstává jeho funkce uchovatele hodnoty.

Varianty řešení

(1) Řešení fyzického nosiče šifrovacích klíčů pro digitální měnu má smysl i bez části s digitálním podpisem 3A, a to v situaci, kdy pouze příjemce platebního prostředku je vybaven internetovým připojením a plátce nikoli. Touto situací může být např. nákup v kamenném obchodě. Příjemce může vlastnit terminál připojený k Internetu a pomocí něj ověřovat krytí jednotlivých kusů platebního prostředku přímo online.

(2) Za určitých okolností může být výhodné ponechat druhý autorizační faktor 5A u vydavatele, ale na ceninu přesto v tamper–evident režimu integrovat jisté tajné "heslo", které ve fázi rušení krytí prokáže na dálku, že komunikující strana je skutečným držitelem platebního prostředku. Takto upravený model tedy vyžaduje spolupráci vydavatele i pro zrušení krytí, ale může se odehrát na dálku bez fyzického kontaktu vydavatele s platebním prostředkem. Motivací pro realizaci této úpravy může být více, jednou z nich je redukce velikosti informace chráněné v tamper–evident režimu. Např. pokud výrobní cena a/nebo zranitelnost roste s rozsahem chráněné informace a celý kryptograficky silný druhý autorizační faktor 5A by bylo obtížné takto integrovat.

(3) Krytí vystavovaného prostředku může teoreticky poskytnout i třetí strana. Výstavce ji musí v průběhu vystavení informovat, na jakou adresu prostředky deponovat a poté získat identifikátor příslušné transakce. Krytí může také poskytnout sám vydavatel, neboť to v určitých případech může zrychlit proces vystavení, resp. proces vystavení digitálního podpisu 3A. U této modifikace modelu se vychází z předpokladu, že výstavce dříve deponoval u vydavatele určitý finanční obnos a následně z něho při vystavování jednotlivých kusů platebního prostředku čerpá, jde tedy o jistou formu úschovy finančních prostředků.

(4) Ochranu proti padělání nosiče šifrovacích klíčů pro digitální měnu by bylo teoreticky možné výrazně vylepšit použitím technologie označované jako Physical Unclonable Function (PUF), což je v současnosti používaný souhrnný název pro způsoby, jak vyrobit fyzický objekt, který nelze zkopírovat, duplikovat, nebo funkčně napodobit (lit. 10, 11, 12, 13), a to ani s použitím nejpokročilejších fyzikálních a chemických metod. Unikátních vlastností se dosahuje výrobou elektronického zařízení s jedinečnými elektromagnetickými vlastnostmi, které pramení z uspořádání molekul a atomů a je proto technicky nemožné vyrobit identickou kopii. V praxi by to znamenalo vybavit nosič šifrovacích klíčů pro digitální měnu elektronickým čipem s implementací PUF a nahradit jím jedinečný alfanumerický identifikátor 1 popsaný v předchozím textu. V této variantě by se zároveň nabízelo realizovat připojení prvního autorizačního faktoru 2A a digitálního podpisu 3A výstavcem rovněž v elektronické formě, zabudovaný čip by mohl disponovat přepisovatelnou pamětí. Vyšší ochrana prostředku proti padělání by byla vykoupena vyššími nároky na vybavení ověřitele, neboť ten by musel disponovat pokročilejším zařízením pro komunikaci s elektronikou zabudovanou do nosiče šifrovacích klíčů pro digitální měnu. Výsledný produkt proto nebyl tak univerzálně použitelný. Zároveň by vyvstala celá řada dalších otázek a problémů souvisejících s implementací, neboť z oblasti kontaktních a bezkontaktních platebních karet vybavených čipem je známo, že množství potenciálních útoků a zranitelností je velké.

Průmyslová využitelnost

Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací a fyzický nosič šifrovacích klíčů pro digitální měnu k provádění tohoto způsobu má uplatnění v oblasti uchování a transferu hodnoty při platebním styku.

V textu použitá literatura či jiné zdroje informací

Lit. 1. Bitaddress. [Online] https://www.bitaddress.org.

Lit. 2. BitcoinPaperwallet.com. [Online] https://bitcoinpaperwallet.com/.

Lit. 3. Wallet Generator. [Online] https://walletgenerator.net.

Lit. 4. BIP 38: Passphrase–protected priváte key. [Online]
https://github.com/bitcoin/bips/blob/master/bip-0038.mediawiki.

Lit. 5. OVD Kinegram AG. [Online] http://www.kinegram.com/.

Lit. 6. **Soheil Hamedani, Gregor Innitzer**. Coin having integrated rfid identification device and method for the production thereof. US 20120055996 3 8, 2012.

Lit. 7. Swiss Bitcoin Certificates. [Online]
https://www.bitcoinsuisse.ch/en/about-certificates/.

Lit. 8. **Shamir, Adi.** How to share a secret. Communications of the ACM.
1979, Sv. 22.

Lit. 9. BIP 16: Pay to Script Hash. [Online]
https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

Lit. 10. **Christoph, Böhm a Maximilian, Hofer.** Physical Unclonable
Functions in Theory and Practice. místo neznámé : Springer, 2012.

Lit. 11. **Pappu, R., a další.** Physical one–way functions. Science. 2002, 297.

Lit. 12. **Naccache David, Frémanteau Patrice.** Unforgeable identification
device, identification device reader and method of identification. EP0583709 1992.

Lit. 13. **Roel, Maes.** Physically Unclonable Functions: Constructions, Properties and Applications, místo neznámé : Arenberg Doctoral School of Science, Engineering & Technology, 2012.

Lit. 14. **Feigelson, Douglas.** Creating and using digital currency. US 2013/0 166 455 6 27, 2013.

PATENTOVÉ NÁROKY

1. Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací, **vyznačující se tím**, že na trhu distribuovaný nosič v prázdném stavu, k němuž náleží druhý autorizační faktor (5A) bezpečně uložený u výrobce nebo integrovaný do nosiče ve formě pole v tamper–evident režimu, je výstavcem pomocí SW aplikace pro vystavení nosiče načten a na základě výstavcem vygenerovaného prvního autorizačního faktoru (2A) a identifikátoru nosiče je odvozena a sdělena výstavci adresa pro zaslání zůstatku digitální měny o odpovídající výši shodné s nominální hodnotou nosiče, načež prostřednictvím online služby pro vydávání digitálního podpisu (3A) je na požádání při splnění všech požadovaných náležitostí o autentičnosti kusu nosiče a výši zaslaného zůstatku digitální měny odpovídající nominální hodnotě nosiče, udělen digitální podpis (3A), který SW aplikace pro vystavení nosiče zkombinuje s prvním autorizačním faktorem (2A) a tato data jsou výstavcem doplněna potisknutím, popsáním nebo polepením, čímž je nosič uveden do aktivního stavu a může být předán dalšímu držiteli, a to i opakovaně, přičemž příjemce provede

vizuální kontrolu a ověří nosič za použití SW aplikace pro ověření nosiče, ověří výši zůstatku digitální měny, poté je touto SW aplikací ověřena po načtení prvního autorizačního faktoru (2A) a digitálního podpisu (3A) pravost digitálního podpisu (3A), provede se validace prvního autorizačního faktoru (2A) a příjemce porovná digitálně podepsané údaje s údaji viditelnými na nosiči, načež jsou z tohoto nového řádně vystaveného fyzického nosiče v aktivním stavu příjemcem pomocí SW aplikace pro vyvedení prostředků digitální měny načteny všechny na nosiči dostupné autorizační faktory (2A a/nebo 5A) a sestavena a autorizována elektronická transakce v síti dané digitální měny pro vyvedení prostředků v elektronické podobě na soukromou adresu příjemce, přičemž výsledkem je přenos šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s vícefaktorovou autorizací a tedy uskutečnění platebního styku digitální měnou mezi výstavcem a posledním příjemcem a součástí výsledku je dále nosič ve viditelně znehodnoceném stavu.

2. Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s odpovídajícím zůstatkem digitální měny s vícefaktorovou autorizací podle nároku 1, **vyznačující se tím**, že posledním příjemcem, který provede vyvedení prostředků digitální měny a znehodnocení nosiče je jeho původní výrobce nebo vydavatel, přičemž k sestavení a autorizaci transakce v digitální měně využije další autorizační faktory, které nejsou na nosiči uvedeny a jsou známy pouze jemu.

3. Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s odpovídajícím zůstatkem digitální měny s vícefaktorovou autorizací podle nároku 1, **vyznačující se tím**, že SW aplikace pro vystavení nosiče, SW aplikace pro ověření nosiče a SW aplikace pro vyvedení prostředků digitální měny jsou aplikace ve formě open–source veřejně přístupné na internetové síti.

4. Způsob přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče s odpovídajícím zůstatkem digitální měny s vícefaktorovou autorizací podle nároku 1 nebo 2, **vyznačující se tím**, že SW aplikace pro vystavení nosiče, SW aplikace pro ověření nosiče a SW aplikace pro vyvedení prostředků digitální měny tvoří jednu SW aplikaci.

5. Fyzický nosič šifrovacích klíčů pro digitální měnu pro realizaci způsobu přenosu šifrovacích klíčů digitální měny na základě postupu vystavování, ověřování a znehodnocování fyzického nosiče uvedeného v nároku 1, **vyznačující se tím**, že je tvořen základovým tělesem ve formě plochého rovinného objektu libovolného tvaru vytvořeným z kompaktního materiálu, přičemž jedna z jeho hlavních rovinných ploch je označena unikátním alfanumerickým identifikátorem (1), přičemž fyzický nosič je podle konkrétního provedení opatřen aplikacemi ochranných prvků proti padělání, přičemž na jedné nebo na obou hlavních rovinných plochách jsou dále pole (2) pro umístění prvního autorizačního faktoru (2A) a dále pole (3) pro doplnění digitálního podpisu (3A).

6. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že základová tělesa ve formě plochého rovinného objektu jsou ve tvaru geometrického obrazce.

7. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 6, **vyznačující se tím**, že základové těleso ve formě plochého rovinného objektu ve tvaru geometrického obrazce je ve tvaru čtverce, obdélníku nebo kruhu.

8. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5 nebo 6, **vyznačující se tím**, že je ve tvaru standardizovaných platebních karet, mincí nebo bankovek.

9. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že na jedné zobou stran je opatřen informací (4) o nominální hodnotě a jednotce měny.

10. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že aplikace ochranných prvků proti padělání v případě listinného provedení jsou bezpečnostní papír s vodoznakem nebo metalickými proužky, opticky variabilní prvky, velmi jemné grafické prvky, tzv. giloše, irisové barevné přechody, barvy s UV nebo IR luminiscencí nebo chemicky reagentní barvy.

11. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že aplikací ochranných prvků proti padělání v případě provedení ve formě plastových karet jsou hologramy.

12. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že aplikací ochranných prvků proti padělání v případě provedení ve formě kovových mincí je difrakční bezpečností prvek kinegram nebo elektronický RFID čip.

13. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že unikátní alfanumerický identifikátor (1) je proveden ve formě chráněného prvku, jako je přelakování iridiscentním lakem nebo děrování nebo jako opticky variabilní prvek.

14. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že pole (2) pro umístění prvního autorizačního faktoru (2A) a pole (3) pro doplnění digitálního podpisu (3A) tvoří jedno společné pole.

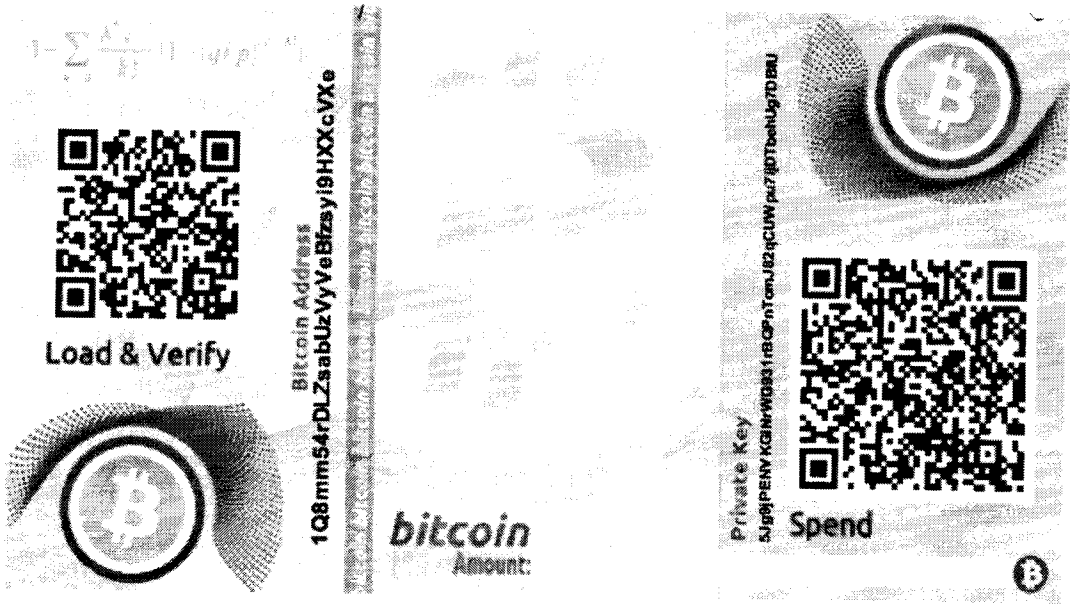
15. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že na jedné nebo na druhé hlavní rovinné ploše je dále pole (5) pro druhý autorizační faktor (5A) vyvedený v tamper–evident režimu.

16. Fyzický nosič šifrovacích klíčů pro digitální měnu podle nároku 5, **vyznačující se tím**, že kompaktní materiál pro zhotovení fyzického nosiče šifrovacích klíčů je plast a/nebo papír a/nebo kov a/nebo slitiny kovů.

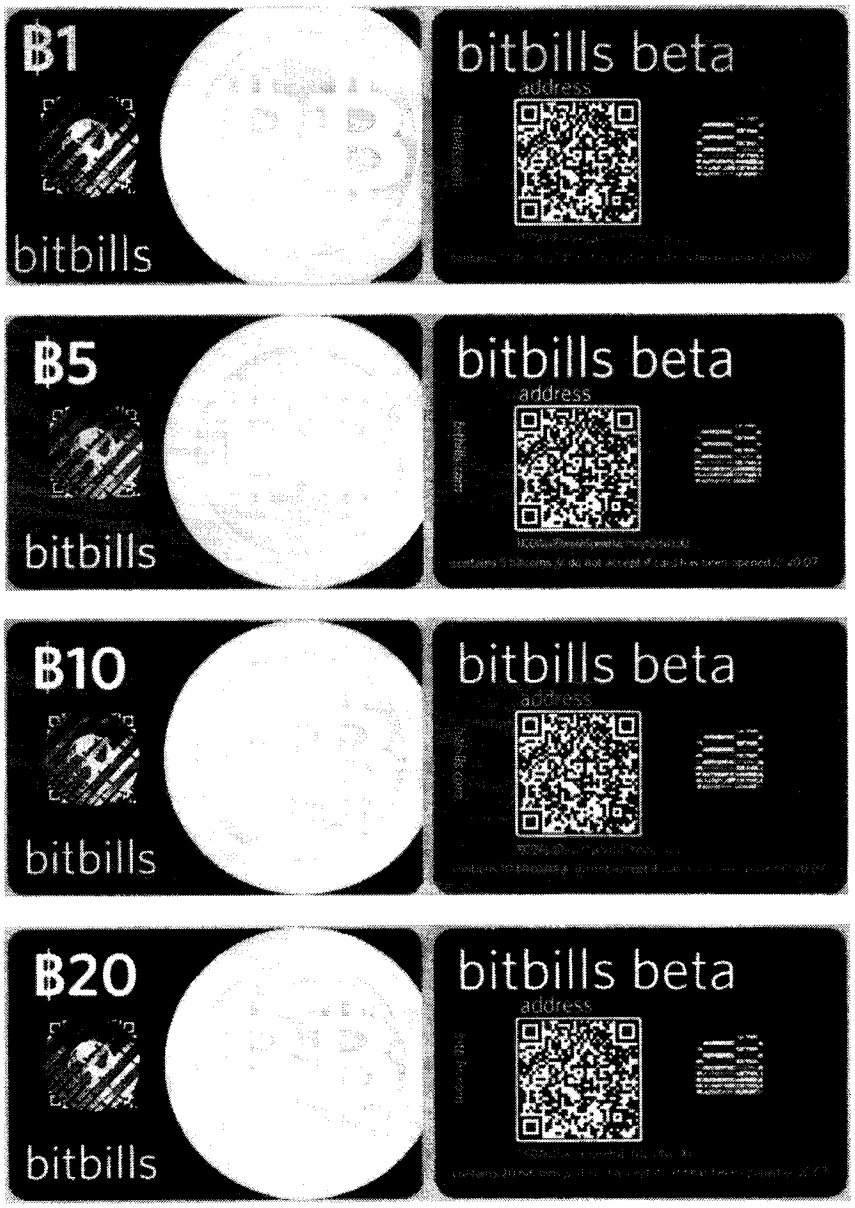
14 výkresů

Seznam vztahových značek:

1 Alfanumerický identifikátor
2 pole pro umístění prvního autorizačního faktoru 2A první autorizační faktor
3 pole pro doplnění digitálního podpisu 3A digitální podpis
4 informace o nominální hodnotě a jednotce měny
5 pole pro umístění druhého autorizačního faktoru 5A druhý autorizační faktor
6 pole pro doplnění nominální hodnoty
7 symbol digitální měny


Load & Verify
Bitcoin Address
1Q8mm54rDLZsabUzVyVeBfzsyi9HXXcVXe
bitcoin
Amount:
Private Key
Spend

Obr. 1

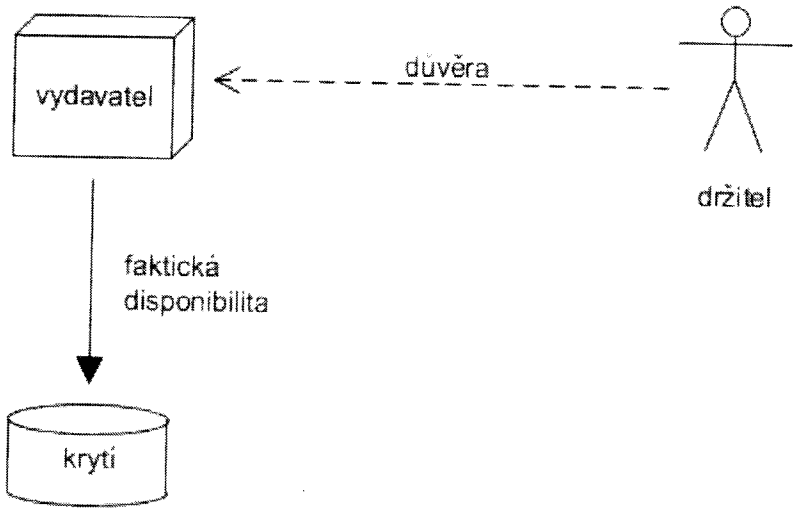

฿1
bitbills
bitbills beta
address
฿5
bitbills
bitbills beta
address
฿10
bitbills
bitbills beta
address
฿20
bitbills
bitbills beta
address

Obr. 2

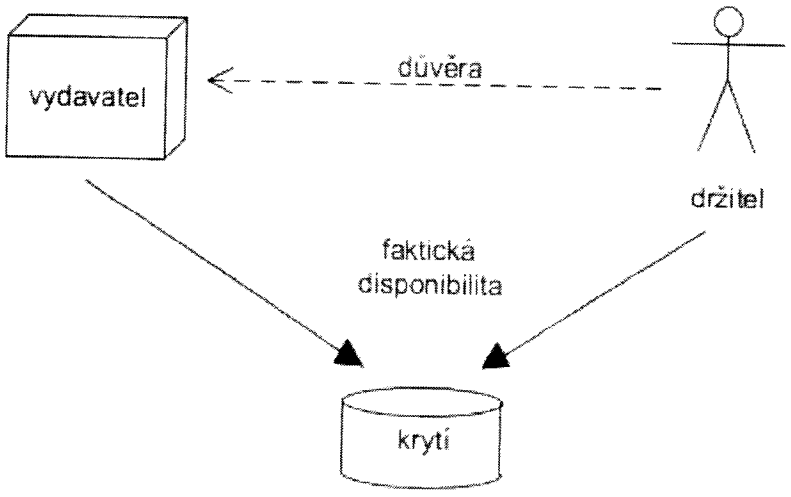
Obr. 3


1Ƀ
1Ƀ
1Ƀ
1Ƀ
© Bitcoin Suisse AG 2013
Bitcoin Suisse AG
ONE BITCOIN
SERIAL
9V6272X76PUSQ
Public key: 12AJDzo64ngWhFW4fWgswF4TweVTKzfHFW
Private Key
Dr. Johannes Schneider
President of the Board
Niklas Nikolajsen
Chief Executive Officer

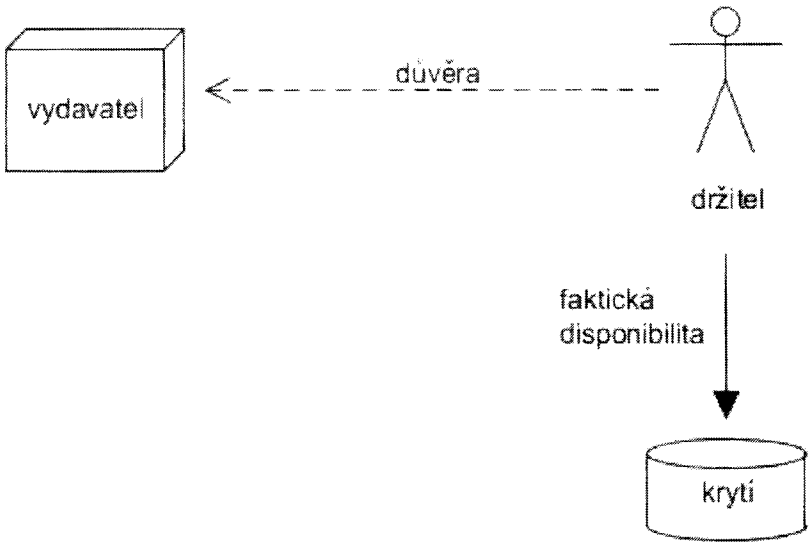
Obr. 4


vydavatel
důvěra
držitel
faktická
disponibilita
krytí

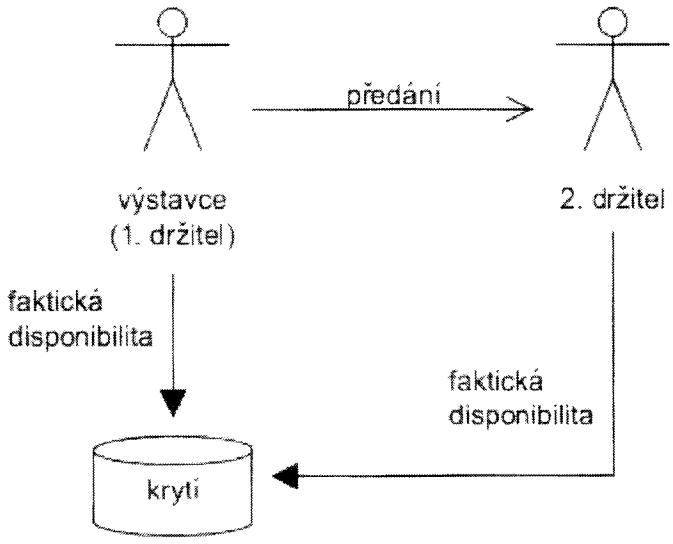
Obr. 5


vydavatel
důvěra
držitel
faktická
disponibilita
krytí

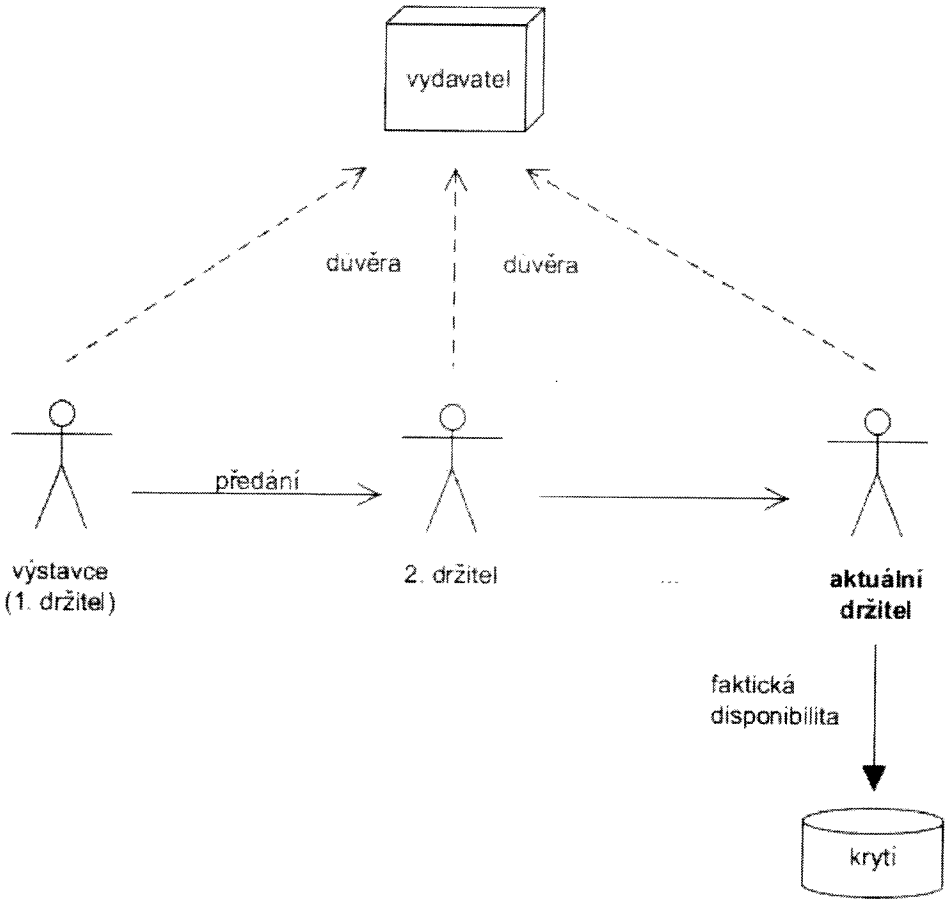
Obr. 6


vydavatel
důvěra
držitel
faktická
disponibilita
krytí

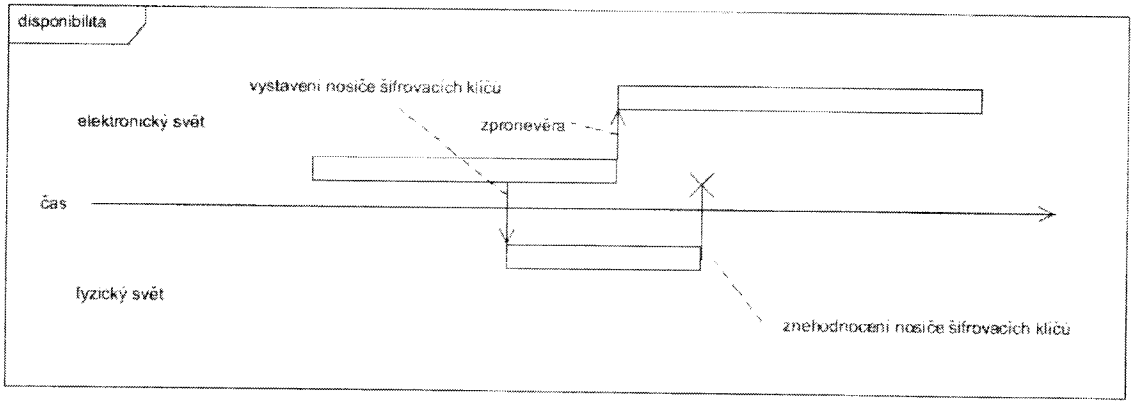
Obr. 7


předání
výstavce
(1. držitel)
2. držitel
faktická
disponibilita
faktická
disponibilita
krytí

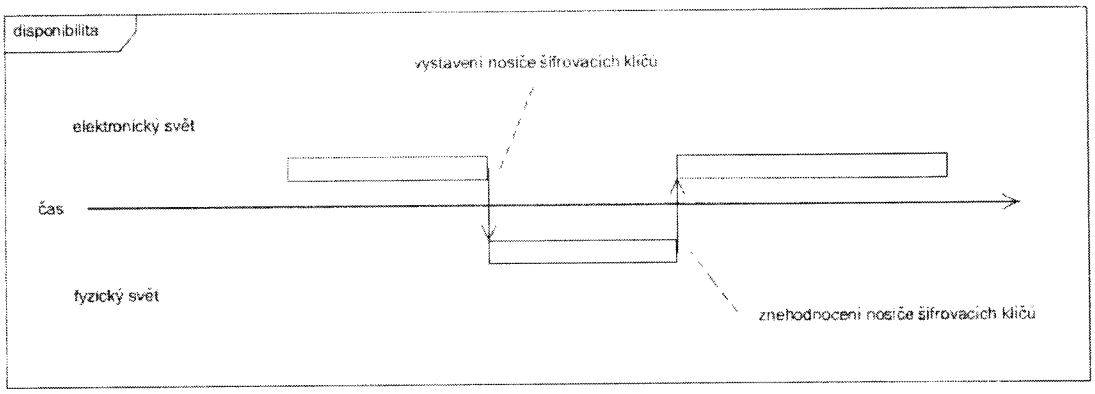
Obr. 8


vydavatel
důvěra
důvěra
předání
výstavce
(1. držitel)
2. držitel
...
aktuální
držitel
faktická
disponibilita
kryti

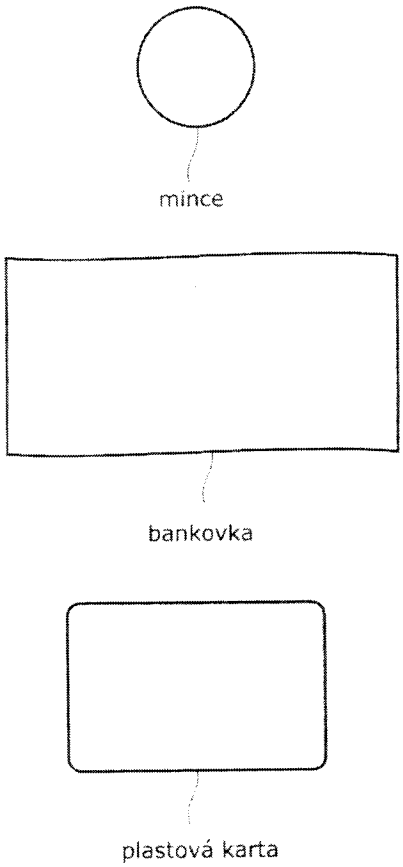
Obr. 9


disponibilita
vystaveni nosiče šifrovacích klíču
elektronický svět
zpronevěra
čas
fyzický svět
znehodnocení nosiče šifrovacích klíču

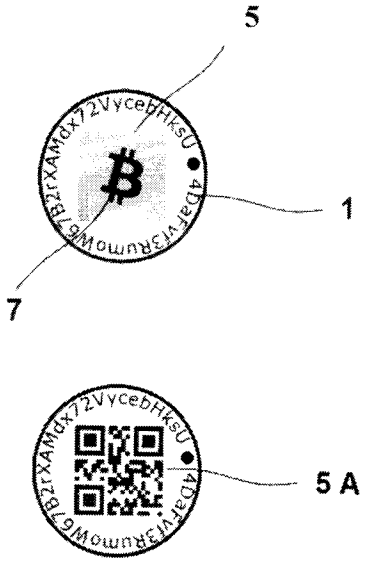
Obr. 10


disponibilita
vystaveni nosiče šifrovacích klíčů
elektronický svět
čas
fyzický svět
znehodnocení nosiče šifrovacích klíčů

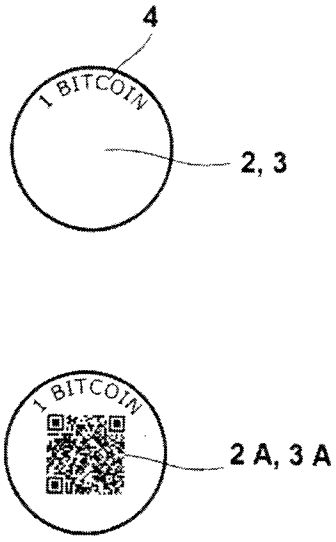
Obr. 11


mince
bankovka
plastová karta

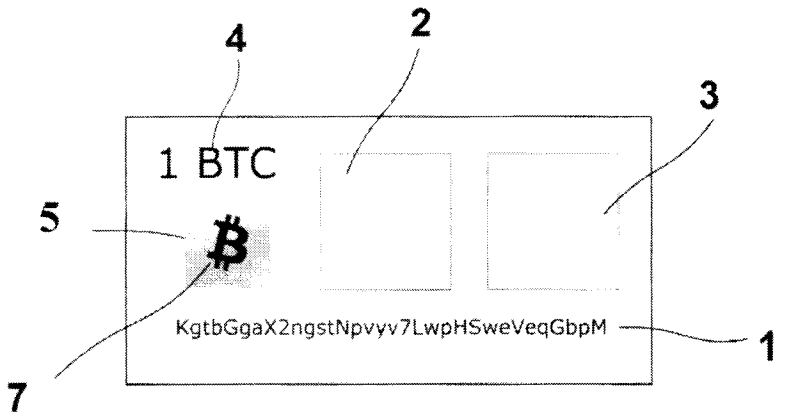
Obr. 12

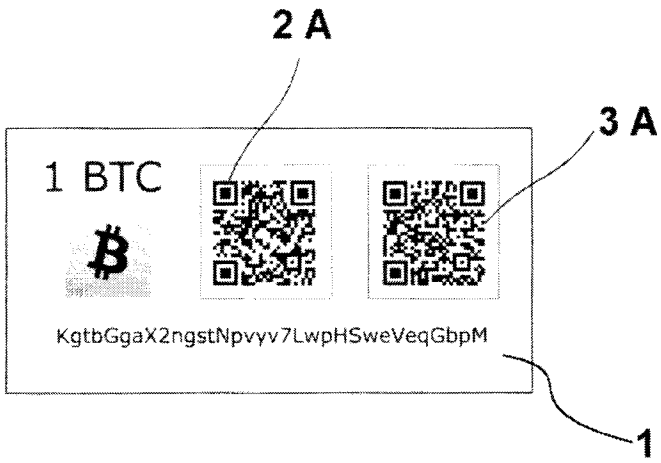


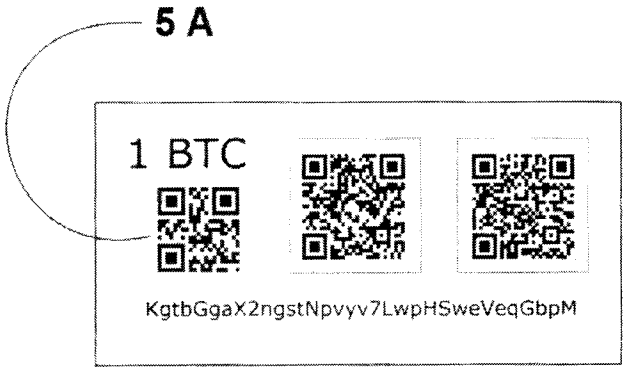
Obr. 13



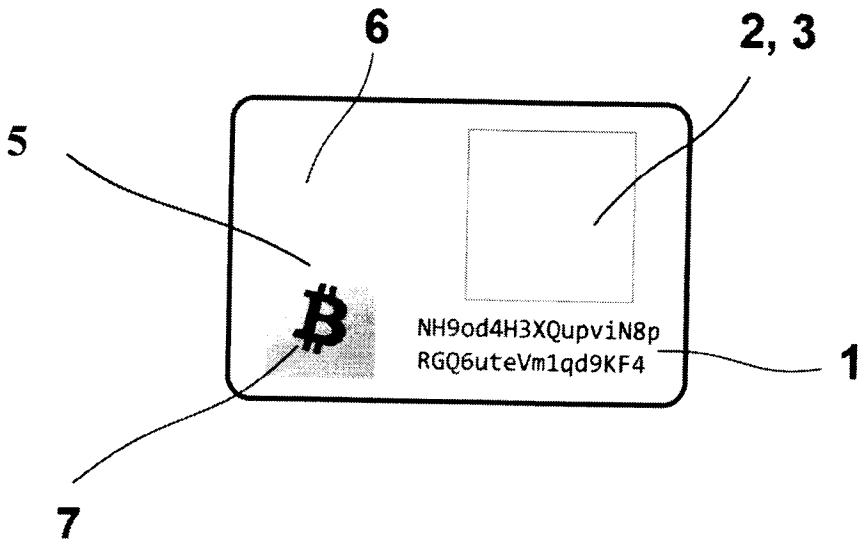
Obr. 14


4
2
3
1 BTC
5
KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM
1
7

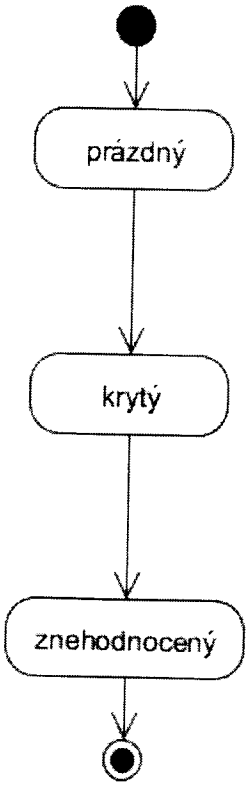

2 A
3 A
1 BTC
KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM
1


5 A
1 BTC
KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM

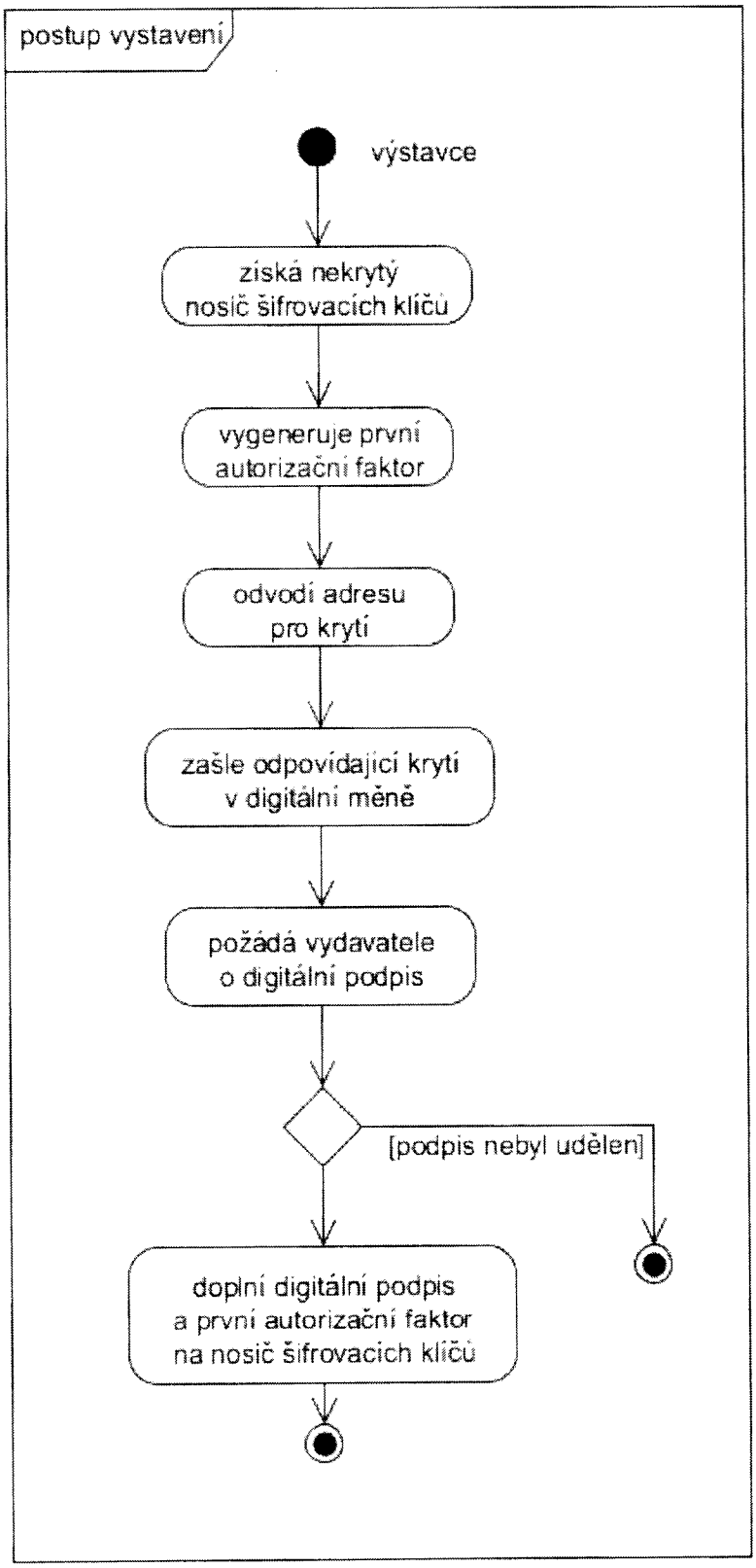
Obr. 15


6
2, 3
5
NH9od4H3XQupviN8p
RGQ6uteVm1qd9KF4
1
7

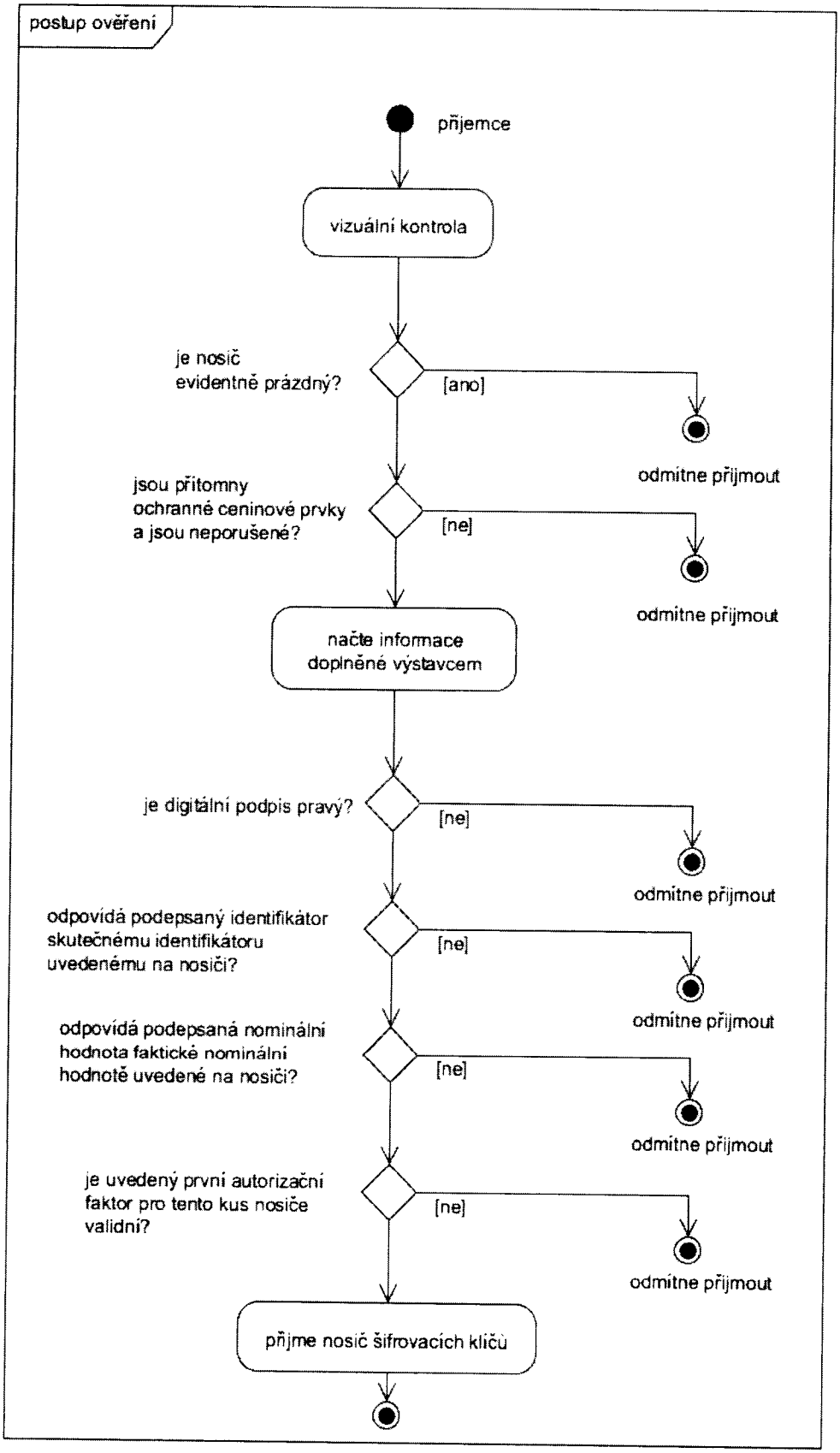
Obr. 16


prázdný
krytý
znehodnocený

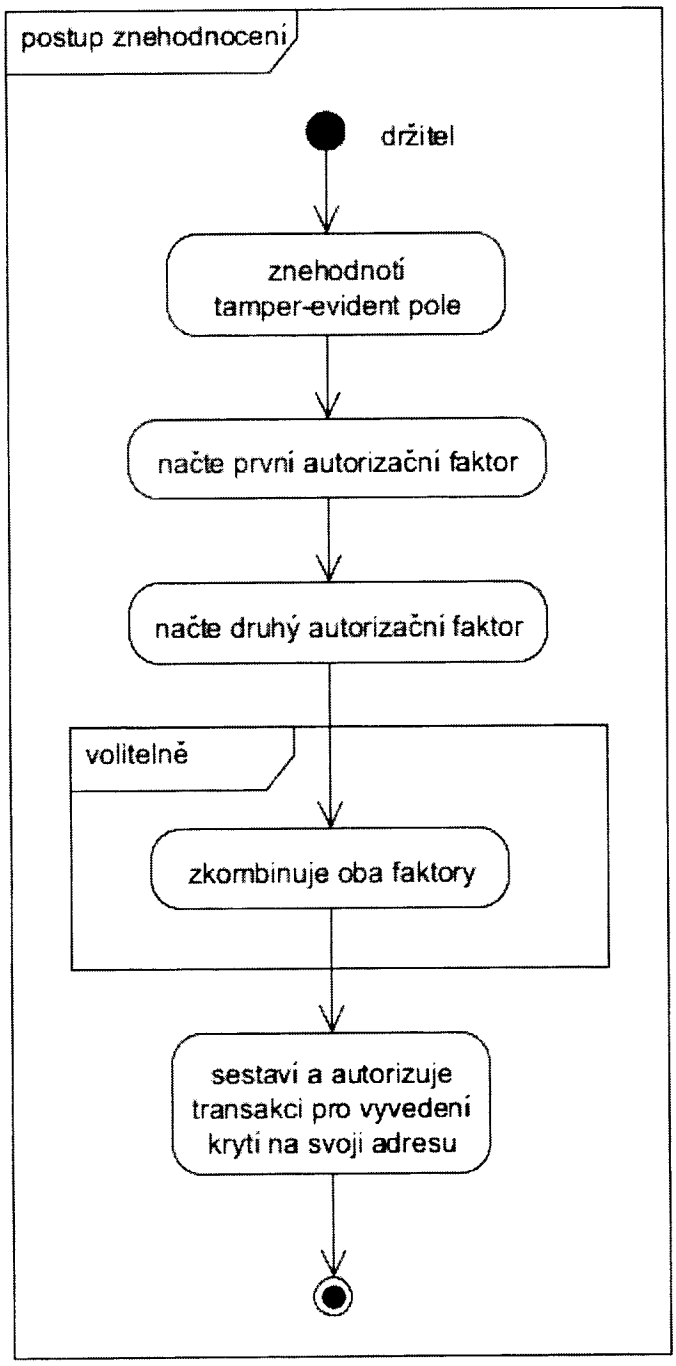
Obr. 17


postup vystavení
výstavce
získá nekrytý nosič šifrovacích klíčů
vygeneruje první autorizační faktor
odvodí adresu pro krytí
zašle odpovídající krytí v digitální měně
požádá vydavatele o digitální podpis
[podpis nebyl udělen]
doplní digitální podpis a první autorizační faktor na nosič šifrovacích klíčů

Obr. 18


postup ověření
příjemce
vizuální kontrola
je nosič evidentně prázdný?
[ano]
odmítne přijmout
jsou přítomny ochranné ceninové prvky a jsou neporušené?
[ne]
odmítne přijmout
načte informace doplněné výstavcem
je digitální podpis pravý?
[ne]
odmítne přijmout
odpovídá podepsaný identifikátor skutečnému identifikátoru uvedenému na nosiči?
[ne]
odmítne přijmout
odpovídá podepsaná nominální hodnota faktické nominální hodnotě uvedené na nosiči?
[ne]
odmítne přijmout
je uvedený první autorizační faktor pro tento kus nosiče validní?
[ne]
odmítne přijmout
přijme nosič šifrovacích klíčů

Obr. 19



Obr. 20

Konec dokumentu