**Fizetési módszerek**

Termékek, szolgáltatások vásárlása kapcsán számos módszerrel történhet a fizetés.

A szereplők a vásárló, a kereskedő és a bank.

A módszerek egy részében kétszereplős a művelet (vásárló-kereskedő), de lehet háromszereplős is (online tranzakciók).

- **készpénzes**
- **banki átutalás**
- **POS** (Point Of Sale) **terminál**
- **Internetes vásárlás** (hitelkártyaszám)
- ***elektronikus készpénzt tároló intelligens chipkártya***

**A fizetési módszer ideális, ha**

**korlátlan térben és időben**: minden fizetési helyen (utca, benzinkút, étterem, áruház stb.) a nap 24 órájában használható,  a kifizethető összeg ne legyen korlátozva (természetesen a fedezet, hitelkeret erejéig).

**biztonságos**: nyújtson megfelelő védelmet a lopás, hamisítás ellen.

**anonim**: fizetéseink összegei, irányai ne lehessenek követhetők.

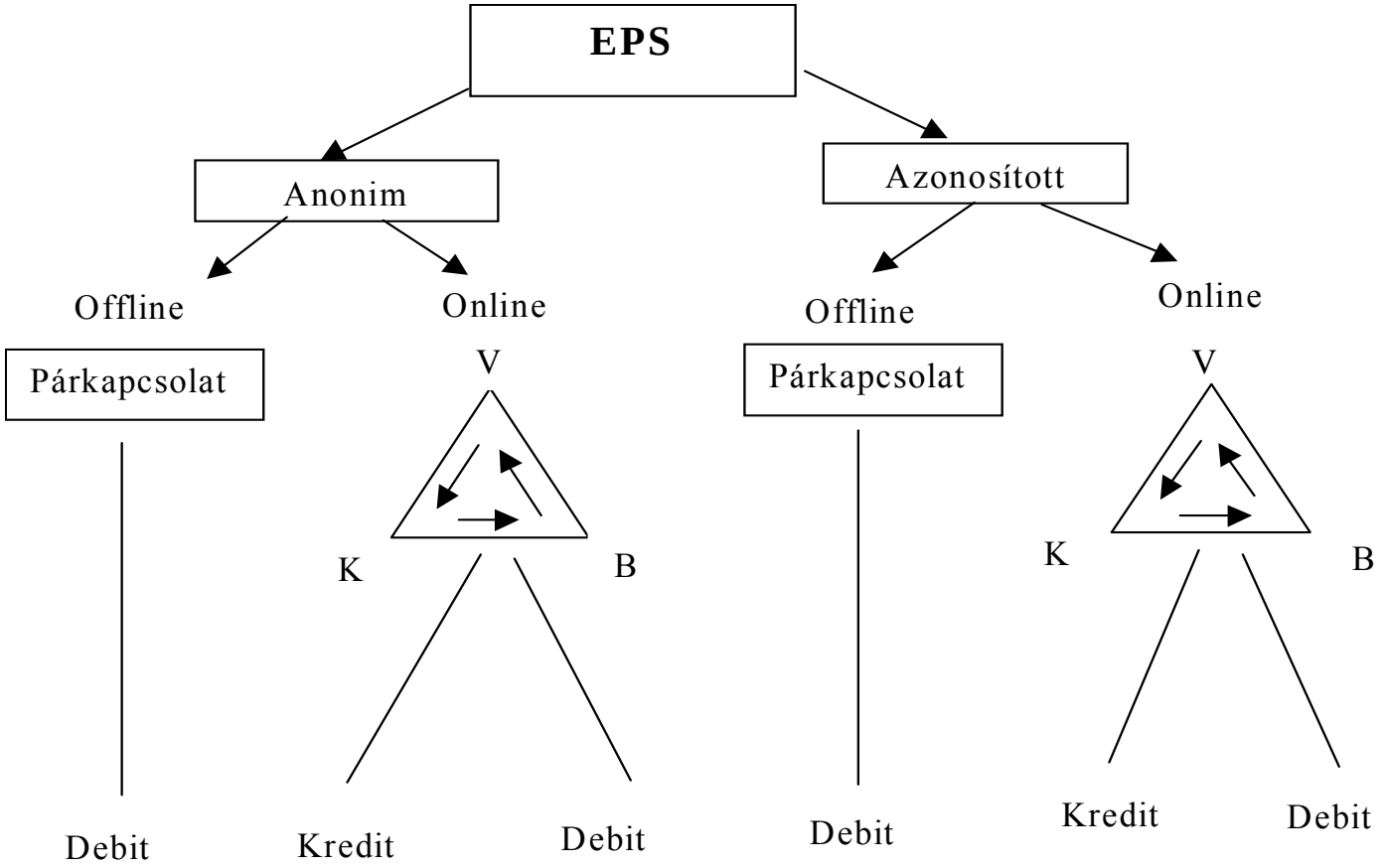
**Készpénz:**

•korlátlan mennyiségben, bárhol, bármikor fizethetünk készpénzzel.
•a kifizetett pénz útja nem követhető (a boltban nem írják rá a bankjegyre, hogy ki fizetett vele).
•egyszerűen átadva átruházható.

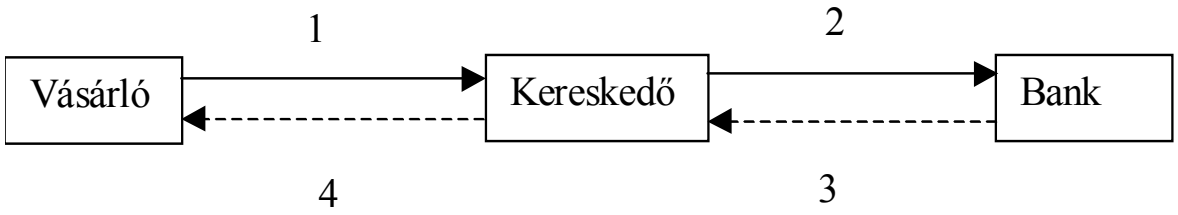
ugyanakkor nem biztonságos, mivel

•ellopható.
•hamisíthatósága a fizikai kiviteltől függő.

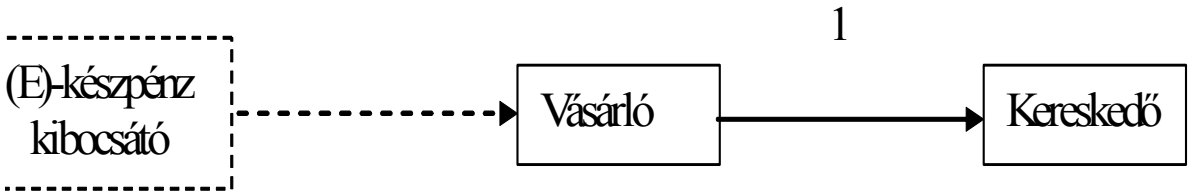
A fizetési rendszerek osztályozása történhet az alábbi fõ szempontok szerint:
*kredit vagy debit*
*azonosított vagy anonim*
*online vagy offline*




EPS rendszerek csoportosítása
(V: vásárló, K: kereskedő, B: bank)




Online séma




Offline séma

**Online:**
A vásárló összeállít egy üzenetet, amelynek tartalmazza a vásárolt termék/szolgáltatás megjelölését, a vásárló és kereskedő nevét, a pénzösszeget, a vásárló bankszámlaszámát, a vásárlás időpontját, majd ezen üzenetre elhelyezi digitális aláírását, s elküldi a kereskedőnek. A kereskedő azonnal továbbítja a Bank felé jóváhagyás végett. A visszajelzés után a kereskedő elfogadja a vásárlás üzenetet, s rendbenhagyólag visszajelez a vásárlónak.

**Offline** vásárlás során a tranzakció a vásárló és a kereskedő között jön létre harmadik fél közbeiktatása nélkül, azaz a pénzt továbbítja a vásárló a kereskedőnek, aki maga meg tud győződni annak hitelességéről.

Az azonosított EPS során követhetők a vásárló korábbi tranzakciói.

Például bankkártyás vásárlás során egy papír dokumentum is készül a kereskedő boltjában, aki a “kártyalehúzós” termináljáról telefonon keresztül ellenőrzi a vásárló jelenlétében a hitelképességet, s egy papír dokumentumon pl. megjelenik a kártyaszám 4 digitje, esetleg a vásárló aláírását is meg kell hogy adja, jelezve hogy valóban megtörtént a vásárlás, továbbá a kártyán a kereskedő mindig láthatja a nevet. (Ideálisan anoním EPS esetén a vásárló adatai titokban maradnak, s nem követhetők a vásárlásai.)

**Azonosított online** EPS esetén mind a kereskedő, mind a Bank azonosítja a vásárlót, s a kereskedő a Banktól visszaigazolást vár.

**Anonim online** EPS esetén a vásárló anonim marad a kereskedő számára.

**Azonosított offline** EPS esetén mind a kereskedő, mind a Bank ismeri a vásárlót.

**Anonim offline** EPS esetén a vásárló anonim marad mind a kereskedő, mind a Bank számára.

**Az ideális EPS tulajdonságai**

***1. Elektronikusan kezelt pénzt ne lehessen ellopni.***

Az én pénzem az enyém, amíg önként át nem adom valakinek egy vásárlás kapcsán.

***2. Elektronikusan kezelt pénzt ne lehessen hamisítani.***

Ne lehessen illegálisan pénzt "gyártani".

***3. Anonim pénzmozgást biztosítson.***

Ne lehessen követni a pénz útját, azaz az elektronikus pénz ne emlékezzen arra, hogy “merre járt korábban”. A szokásos papírpénzről sem tudjuk, hogy milyen kezeken ment át korábban (“pénznek nincsen szaga”). Az elektronikus vásárlói rendszerben vásárolhassunk úgy, hogy az identitásunkat ne kelljen felfedni. (Ezen a ponton már jogi kérdéseket is felvet esetleges pénzmosás kapcsán az anonimitás kritérium.)

***4. Nulla legyen a tranzakciós költség.***

Ideálisan az elektronikus pénzmozgás legyen költségmentes, azaz ne kelljen fizetni az EPS rendszerbe belépéskor, ne legyen havi dijminimum, ne legyen a “pénz” mozgásért fizetendő a tranzakciós költség.

***5. Világméretű legyen elterjedtség***

A világ két különböző pontján levő partnerek (vásárló, kereskedő) tudják használni, ne legyen valutanem probléma, vagy ne kelljen azonos országbeli bankszámlát tartaniuk.

***6. Tetszőleges címleteket tudjon kezelni.***

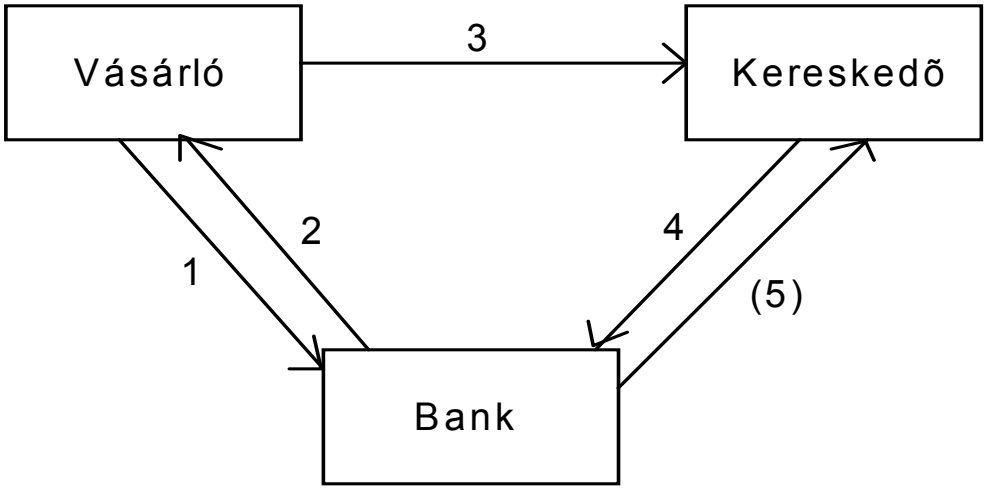
***7. Támogassa mind a kredit mind a debit fizetéseket.***

Támogassa mind a hitelből vásárlást (credit card jelleggel), de a vásárló bankszámláján levő összegből történő vásárlást (debit).

***8. Azonnali pénzmozgást tegyen lehetővé.***

A vásárlótól a kereskedőig (a kereskedő bankszámlájáig) gyakorlatilag azonnal történjen meg a pénzmozgás.

**Digicash**




A résztvevõk a vásárló (V), a kereskedõ (K), valamint az elektronikus bank (B).

**1. V->B:** c, $m=s \cdot r^e \pmod n$

**2. B->V:** $z=m^d \pmod n$

**V:** $w= z/r = s^d$

**3. V->K:** $P=(c,s,s^d)$

**4. K->B:** $P=(c,s,s^d)$

**5. B->K:** P hamis/hiteles

**Kezdeti feltételezés**

1.) A vásárlónak számlája van a bankban, amelyen valamely összeg áll rendelkezésére. (Ezen feltétel megvalósulása az alábbiakban részletezendõ tranzakciós protokolltól független.)

2.) Számlanyitáskor a vásárló választ egy $\mathbf{V_e}$, $\mathbf{V_d}$ nyilvános-, titkos RSA kulcspárt, amelyet üzenetei hitelesítésére használ. Ugyanekkor egy **véletlen sorozatszámot** is választ, amely véletlen érték az elektronikus készpénz (e-cash) sorozatszáma generátorának a véletlen magja lesz.

3.) A bank rendelkezik $\mathbf{B_{e\_i}}$, $\mathbf{B_{d\_i}}$, i=1,2,... nyilvános-, titkos RSA kulcspárok sorozatával, ahol az egyes párok a különbözõ (i) pénzcímletekhez tartoznak.

A vásárló jelzi a bank felé pénzkivételi (elektronikus-pénzre konvertálási) szándékát, amit aláírásával hitelesít. Az aláírást ellenõrzi a bank.
(Ezt nem emeltük ki az **alábbi protokollban, ahol csak a pénz gyártására és ellenőrzésére koncentrálunk**. Hasonlóan nem mutatják az alábbi lépések V és K közti biztonságos rendelés és visszaigazolást.)

Sikeres ellenõrzést követõen a vásárló kezdeményezi megfelelõ mennyiségû elektronikus pénz “gyártását”. A e-pénz elõállítása a protokoll 1. és 2. lépése.

**1. V->B:** $c,\ m=s \cdot r^e \pmod n$
**2. B->V:** $z=m^d \pmod n$
**V:** $w= z/r = s^d$

A protokoll 3-5. lépései a vásárlás során kereskedõ felé történõ fizetéshez, s a pénz ellenõrzéséhez tartoznak.

**3. V->K:** $P=(c,s,s^d)$
**4. K->B:** $P=(c,s,s^d)$
**5. B->K:** P hamis/hiteles

A vásárló generálja a következõ **véletlen sorozatszámot** (a véletlen mag felhasználásával), amely azonban rendelkezik azon strukturáltsággal, hogy a baloldali fele egyértelmû determinisztikus kapcsolatban van a jobboldali felével.

Legyen ez a pillanatnyi **sorozatszám s.**

Ha ezen **s** sorozatszámmal szeretne generálni mondjuk i=10$ címletû elektronikus pénzt, akkor a vásárló kiválasztja az ezen **címlet**nek (**c**) megfelelõ

**$e=B_{e\_i}$ banki nyilvános kulcsot,**
**$n=B_{n\_i}$ modulust,**

egy csak általa ismert, **titkos r véletlen számot** (vak-aláíráshoz).

A vásárló az alábbi üzenetet küldi a banknak:

**1. V->B:** c, $m=s \cdot r^e \pmod n$

A bank az 1. lépésben kapott **m** üzenetrészt aláírja az adott címletnek megfelelõ $\mathbf{d=B_{d\_i}}$ titkos kulcsával, s az eredményt visszaküldi a vásárlónak:

**2. B->V:** $z=m^d \pmod n$

A vásárló a $\mathbf{z= (s \cdot r^e)^d = s^d \cdot r \pmod n}$ és **r** mennyiségek ismeretében egy osztással elõállítja a

**V:** $\mathbf{w= z/r = s^d}$

**mennyiséget (z** ellopásával egy támadó nem jut a pénzhez, mivel nem ismeri **r** értékét, azaz nem tudja **w** értéket elõállítani ).

A

$\mathbf{P=(c, s, s^d)}$

**hármas az elektronikus "bankjegy"**. Ennek megfelelõen leolvasható a címlete, az - egyedi - sorozatszáma, valamint hordozza a bank digitális aláírását.

Egyszerûség kedvéért legyen az áru ára egyetlen “bankjegy”, azaz

## 3. V->K: $P=(c,s,s^d)$

(K nyilvános kulcsával rejtjelezetten küldve: a 3. lépés csak a pénz üzenet nyílt szöveget mutatja!)

A kereskedõ a pénzt tárolhatja. Célszerûbb, ha azt elküldi a banknak, egyrészt **ellenõrzés**re, másrészt - hitelesség esetén - egyúttal a pénzt a **bank jóváírja** a kereskedõ számláján, az elektronikus pénz sorozatszámát rögzíti, s az **elektronikus pénz** ettõl kezdve **kivontnak tekintendõ** a forgalomból:

## 4. K->B: $P=(c,s,s^d)$

(B nyilvános kulcsával rejtjelezetten küldve: a 4. lépés csak a pénz üzenet nyílt szöveget mutatja!)

**A bank két lépésben ellenõriz:**

**a.)** (**double spending**) az **s** sorszám nem szerepelt-e már egy korábbi ellenõrzésnél, azaz nincs-e szó **pénzduplikálás**ról (ne felejtsük el, hogy most a pénz egy bitsorozat (egy fájlban tárolva), amit másolni standard módon lehet, a klasszikus pénztõl eltérõen). Ha a bank duplikálást észlel, azaz azt egyszer már elköltötték a pénzt, akkor azonnal a tranzakció 5.lépésére tér át, visszajelezve a kereskedõnek azt, hogy az általa ellenõrzésre bemutatott pénz másolat.

Majd ellenõrzi, hogy:

**b.)** az **s** és $\mathbf{s}^{\mathbf{d}}$ összetartozó pár-e, azaz az õ aláírását hordozza-e. Ezt a **c** címlethez tartozó nyilvános kulcsa felhasználásával végzi. Ha ez az ellenõrzés is rendben van, akkor tárolja a sorozatszámot, amivel a pénz forgalomból kivontnak tekinthetõ, továbbá üzen a kereskedõnek:

**5. B->K:** P hamis/hiteles

**Analízis:**

1.) A pénz **nem hamisítható**.

a) Mint láttuk a protokoll lépéseinek magyarázatánál egy másolat (akár a V, akár a K készítené) a banki ellenõrzésen fennakad.

b) Ravaszabb hamisítás próbálkozást, a banki aláírás hamisítását. Ehhez kellene találnia egy **u** értéket, amelyet a cimletnek megfelelõ banki **e** nyilvános kitevõre emelve egy sorszámra jutna. Mivel azonban a sorszámnak - az említett - rögzített struktúrája van, megfelelõ blokkméretek mellett, gyakorlatilag kizárható ezen támadás sikere.

2.) A pénz **anoním:**

Amikor a 2.lépésben B aláírását adja az **m** üzenetre, akkor az **m** felépítése miatt nem tudja megállapítani a V által éppen választott sororozatszámot, hiszen az ismeretlen **r** véletlennel való moduláris szorzás elfedi azt. Tehát úgy ad aláírást az **m** üzenet aláírásra megcélzott **s** részére, hogy nem láthatja annak valódi értékét (ha s értékét látná, tudná kötni a pénzt V-hez). Az ilyen módon történõ aláírást **vak aláírásnak** nevezzük.

Így ez a fizetõeszköz teljesen anoním, azaz a bank sem tudhatja, hogy egy késõbb ellenõrzésre hozzákerülõ elektronikus pénzt ki gyártatta le vele és mikor.

## 4.) Hiányosságok

### Letagadás

A fenti protokoll ebben a formájában még nem teszi lehetõvé **egy V és K közti letagadás vita** feloldását, azaz hogy a kereskedõ ne hazudhassa azt, hogy bank nem fogadta el a pénzt hitelesnek, s így nem került a V által - ténylegesen hitelesen - átküldött pénz a K bankbeli számlájára.  Ez pl. olyan módosítással történhetne, hogy a V és K által is hitelesített - fentiekben részletezett tartalmú - megrendelõ is eljutna a bankhoz a pénzzel együtt, s ott tárolódna, ahol az anonimitást õrizendõ egy hash lenyomat küldése és tárolása történhetne (**commitment**).

### Elvesztés

Ha a K jelezné a V-nek, hogy - a bankba történõ beváltás elõtt - valahogy **elveszett** a 3.lépésben V-tõl megkapott pénz, akkor V-nek jelezni kellene tudnia a bank felé egy letiltást az adott pénzre vonatkozóan, például úgy, hogy megküldi a banknak az eltünt pénz s sorozatszámát, amit a bank feljegyez.

A fentiekben leírt Digicash protokoll az EPS osztálybasorolás szerint tehát

**debit, anonim, on-line**

rendszer. Ugyanakkor a V és B megállapodásától függõen mûködhet kredit rendszerként is, azaz ha a bank engedi hitelben legyártatni nála az elektronikus pénzt.

A rendszer online tulajdonsága azt jelentette, hogy amikor fizetésre került a sor a kereskedõ a 4.lépésben a bankot is bevonta a tranzakcióba, ahhoz hogy megnyugodhasson az elektronikus pénz felõl annak másolatlansága vonatkozásában.