

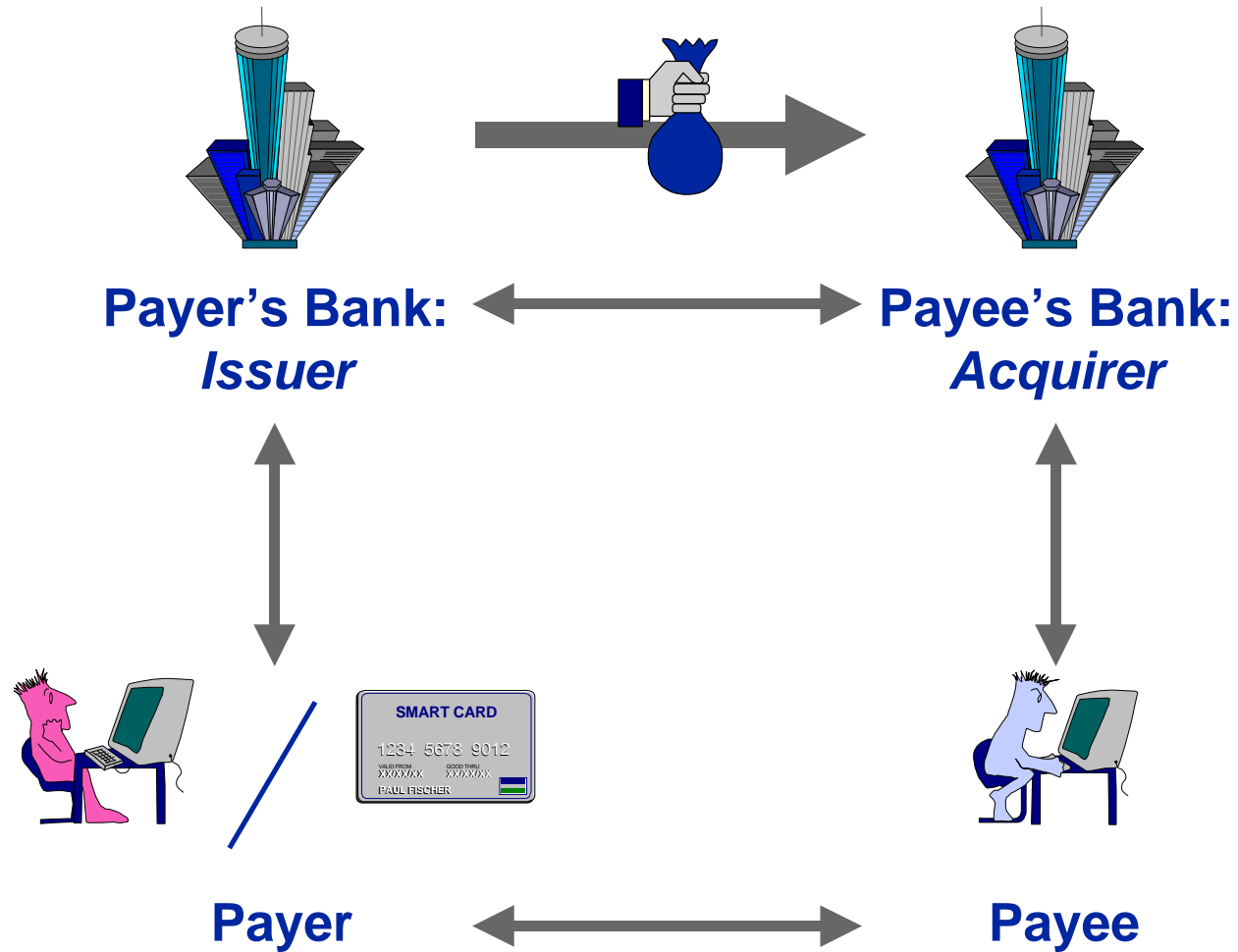
Outline



Payment systems

“Money”

What is a Payment System?



What will be Used in the Digital World?

- u **The same types as in the paper world!**
 - u Cash, for small and anonymous payments
 - u Cheques, credit cards
 - u Money transfer orders (push, pull)
 - u Payment-like systems: vouchers, coupons

- u **Same metaphor, i.e.,**
 - u same “business model,” same “look-and-feel”
 - u at least as cost-effective
 - u at least as secure, privacy protecting
 - u ... but very different implementation

Payment Integrity

- u **Integrity** for *payer, payee, payment system*
 - u **Nothing happens without authorization**
 - u Nobody gives (sometimes also: receives) money without an explicit agreement, stating all necessary payment details
 - u **Nothing happens without generating sufficient pieces of evidence**
 - u If *X* receives money, it can *prove* this fact to “court”
 - u If *X* has *not* given money, nobody can convince a “court” of the contrary
 - u Sometimes: If *X* gives money, it gets a *receipt*
- u **The “rules” and technical procedures for “dispute handling” are part of the system!**

Payment Privacy

- u **Privacy of payer and payee**
 - u **Payment confidentiality:**
 - u Payment details
 - u payer, payee, account numbers, amounts, date and time, payment subject, etc.
 - must not become known to outsiders
 - u **Payment anonymity:**
 - u **Payer anonymity:** Only a pseudonym is known to the payee, no identity (*cash*)
 - u **Payer unlinkability:** Payee cannot link any two payments of the same payer (*cash*)
 - u **Payer untraceability:** Payment system cannot trace payments back to the payer (*coins*)

“Money”

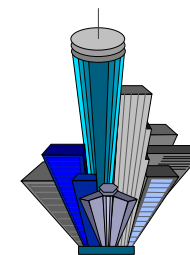
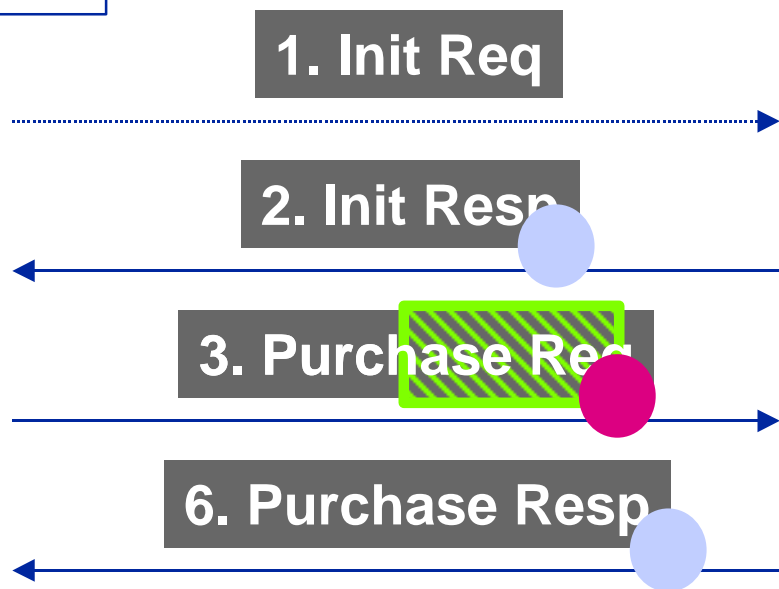


Basic Approach: Simulate Paper World

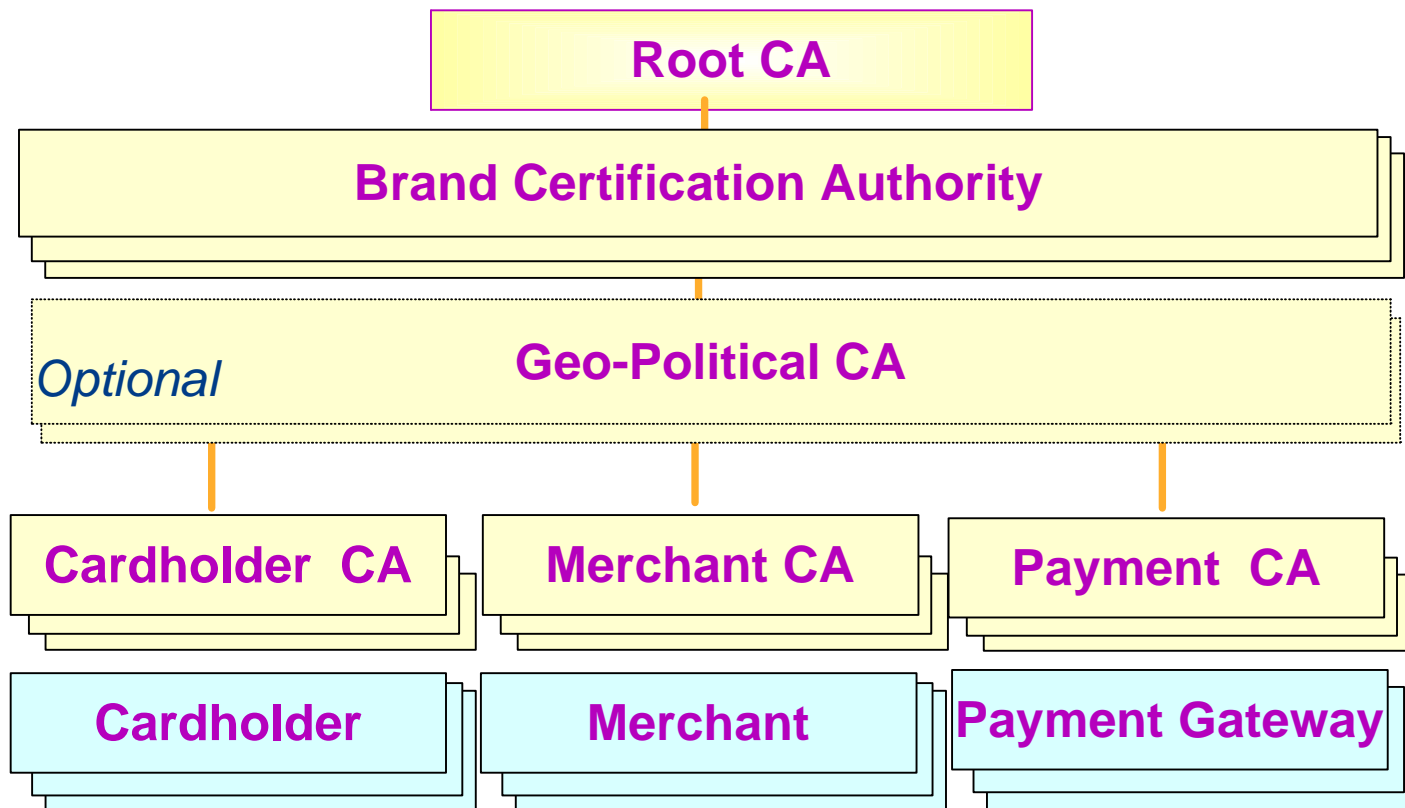
u Online Creditcards / SET

Variants:

- 3KP ● ● ●
- 2KP ● ●



SET CA Hierarchy



SET Status and Extensions

- u **Schedule SET 1.0**
 - u **Final specs: 5/97**
 - u **Product general availability: 9/97**

- u **SET Debit Card Applications**
 - u **IBM / Fuji Bank: private extensions for PINs**

- u **SET with Smartcards**
 - u **... for security and mobility**
 - u **France (EPI/MCI C-SET, VISA E-Comm),
Japan**



SET



- u **Accepted and well-known payment model**
- u **Agreed standard**
- u **Signature based**
 - u Potential for dispute handling
- u **Exploits existing banking infrastructure**



- u **Online service**
 - u Gateway potential bottleneck
- u **Too large for current smartcards**
- u **Costly**
 - u Relatively expensive crypto

Existing Systems and Proposals

	Online Payments	Offline Payments
Traceable	<ul style="list-style-type: none"> ♦ Crypto-less systems: just-do-it, <i>FirstVirtual</i> ♦ Encrypted CC: just-do-it, e.g., <i>SSL</i> ♦ Secure CC: <i>CyberCash, iKP/IPay, SET, Smartcard-based SET</i> ♦ Secure cheques: <i>FSTC e-check</i> ♦ Billing server for micro payments: <i>NetBill, NetCash</i> ♦ Micro payments: <i>CAFE, Phoneticks, Micro-iKP, Millicent, MicroMint, MiniPay</i> 	<ul style="list-style-type: none"> ♦ Smartcard-based electronic purses <ul style="list-style-type: none"> ♦ MAC-based: <i>Danmont, Proton, ZKA, Chipper, ...</i> ♦ Signature-based: <i>CLIP, Mondex, ...</i>
Untraceable	<ul style="list-style-type: none"> ♦ Anonymous “exchangers”: <i>Anonymous Credit Cards, NetCash</i> ♦ Blind signatures: <i>ecash</i> 	<ul style="list-style-type: none"> ♦ Smartcard-based or electronic wallets + blind signatures: <i>CAFE</i>



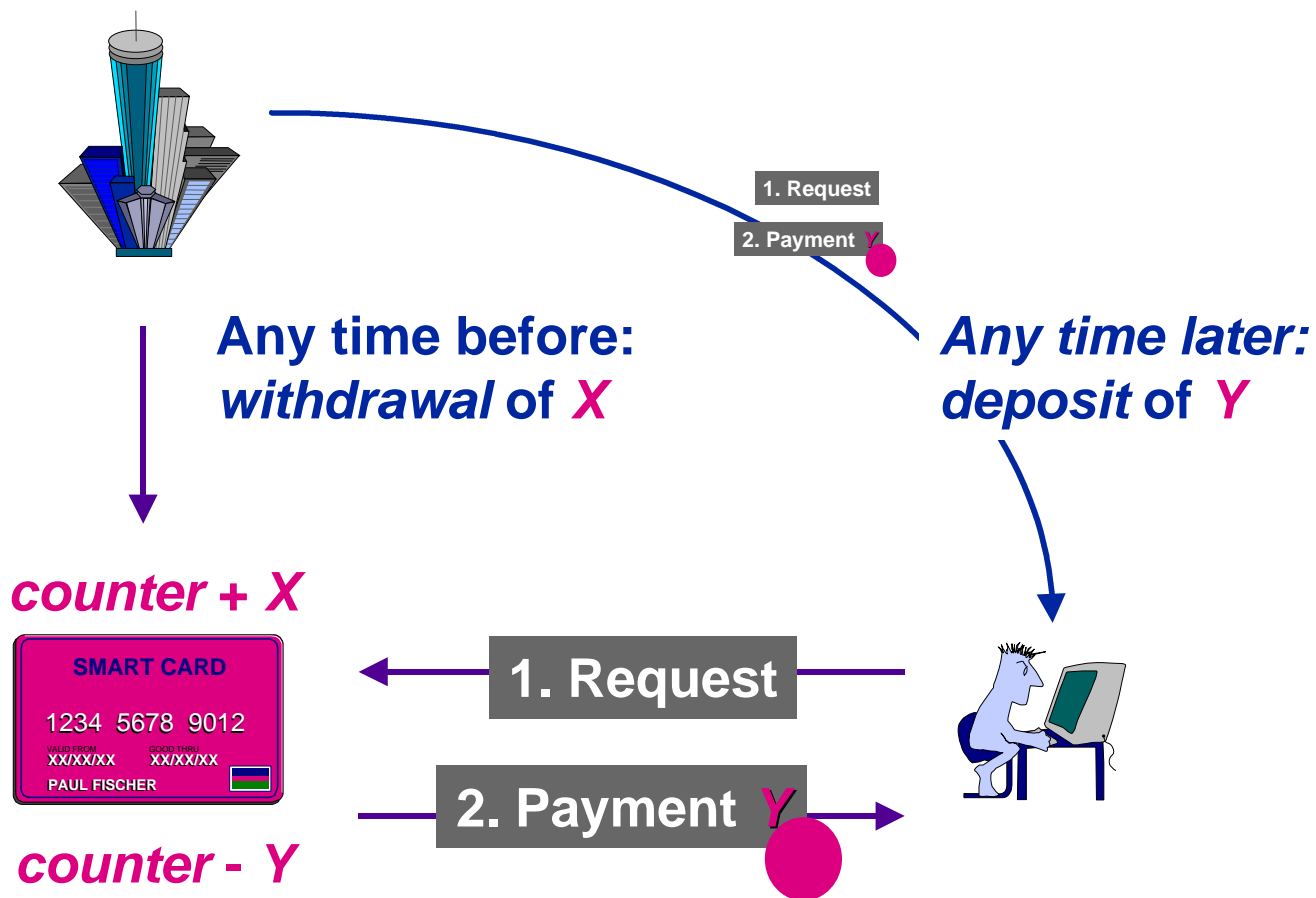
+ many other proposals and projects ...

“Money”



Double-spending Prevention

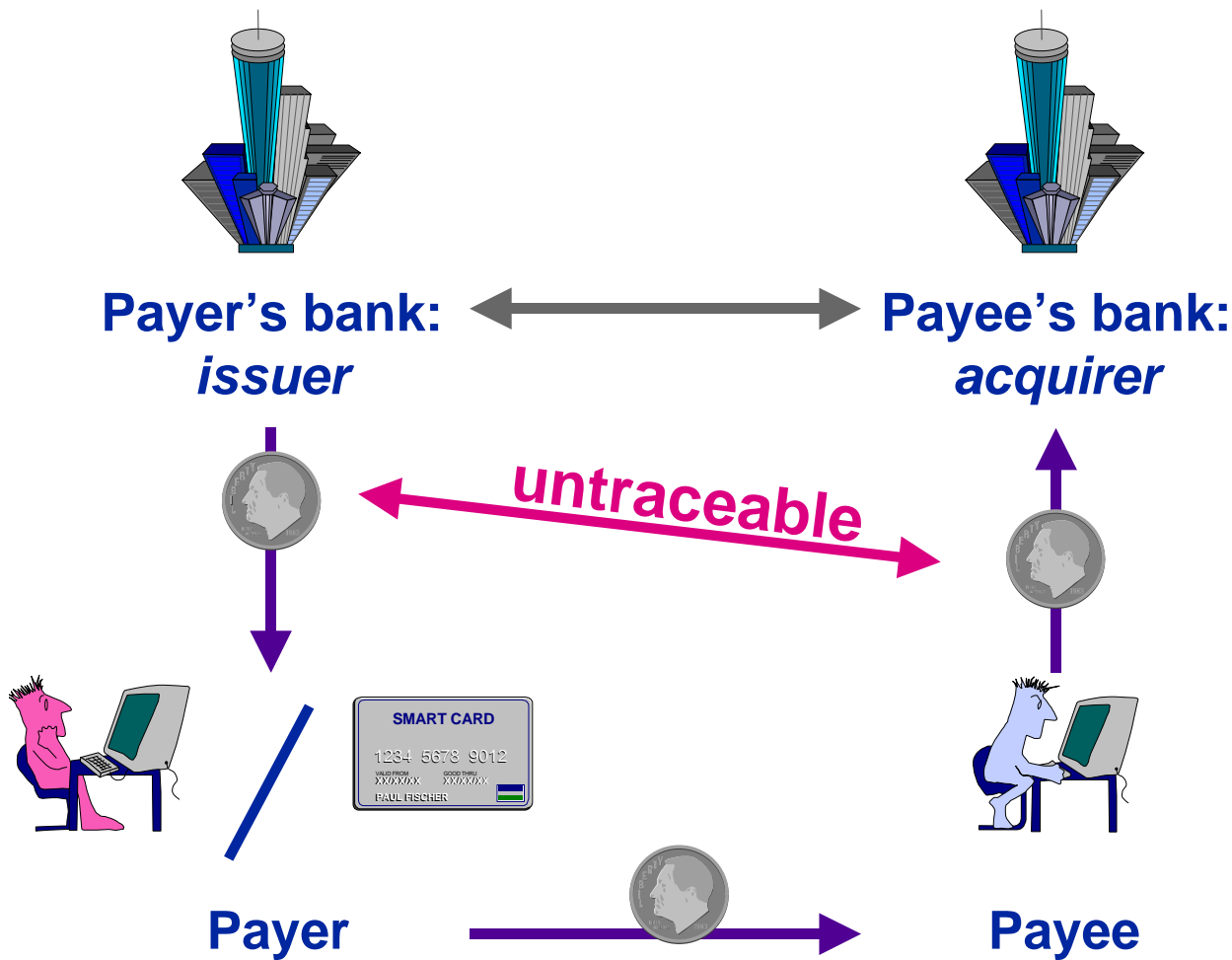
u Signature-based offline purse (e.g., CLIP)





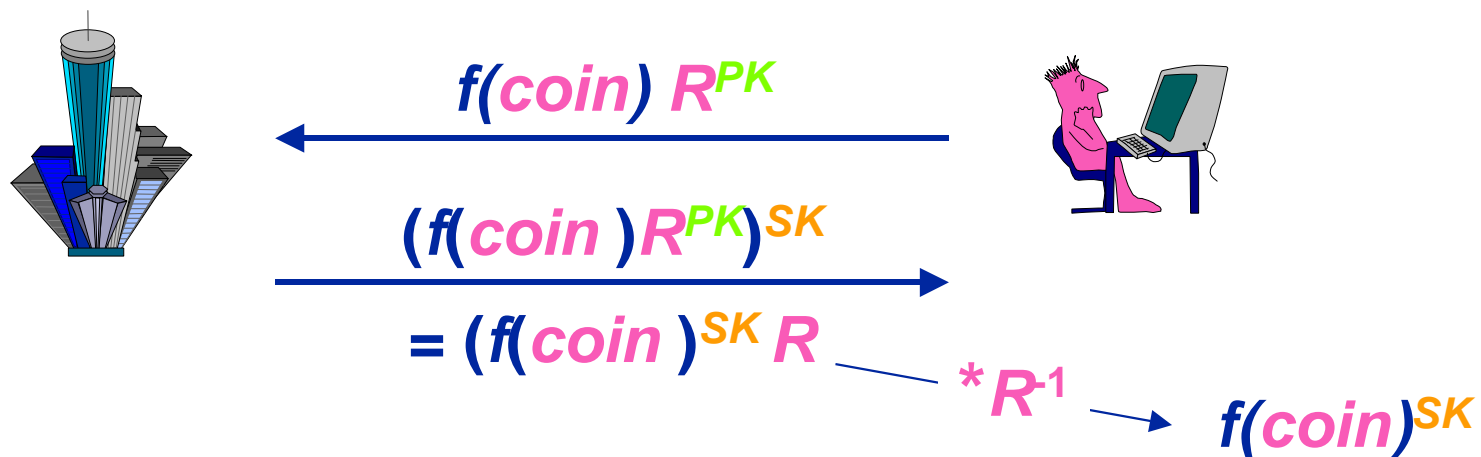
“Blind Signatures” for Unlinkability

u Online: **ecash™**, offline: **CAFE**



ecash™

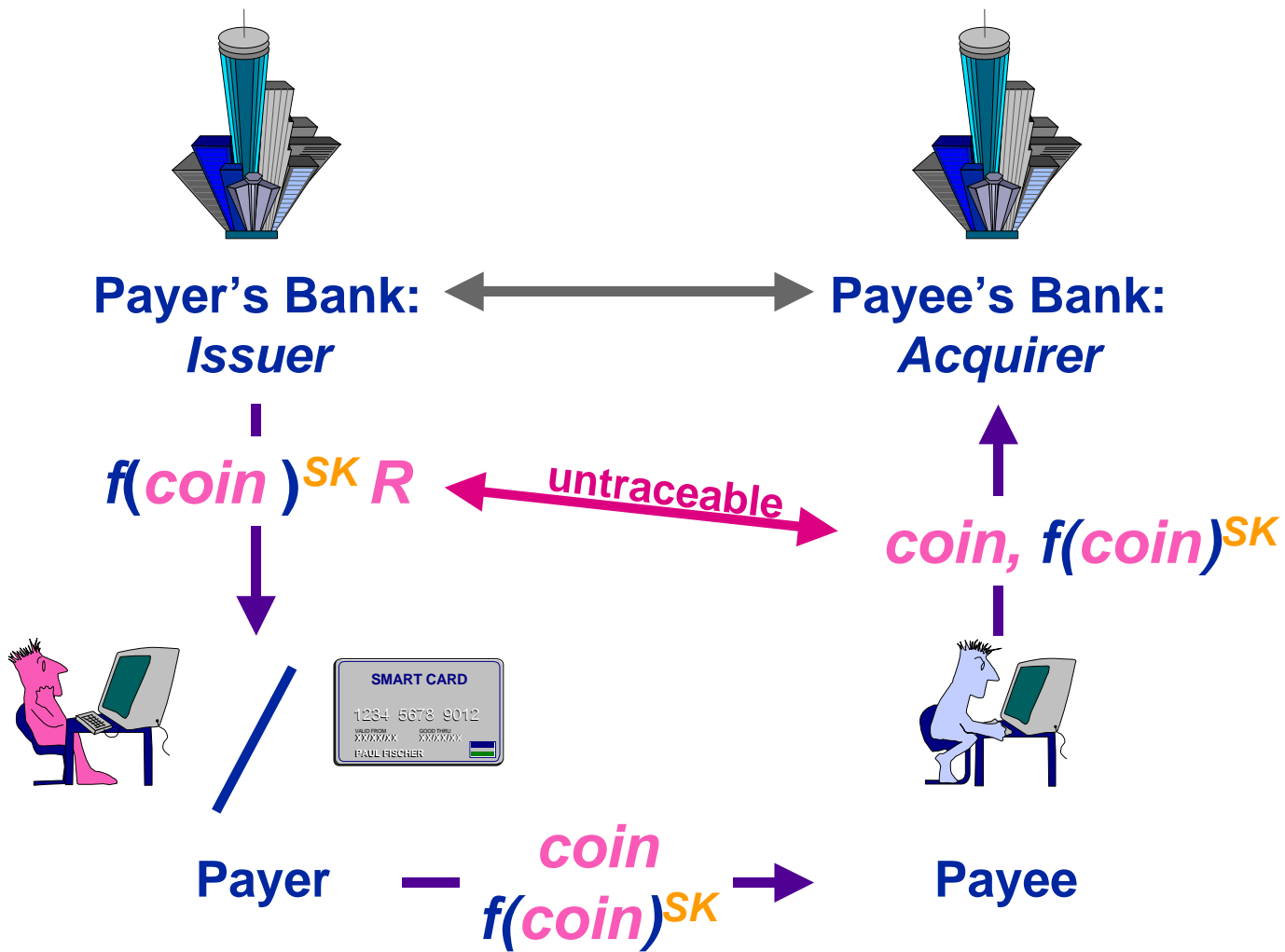
- u **Blinded RSA Signatures**
 - u One-way function f
 - u RSA pair (SK , PK) chosen by **issuer**, defines *one* denomination
- u **Coins:** $(coin, f(coin)^{SK})$
- u **Withdrawal step**



Untraceable Cash



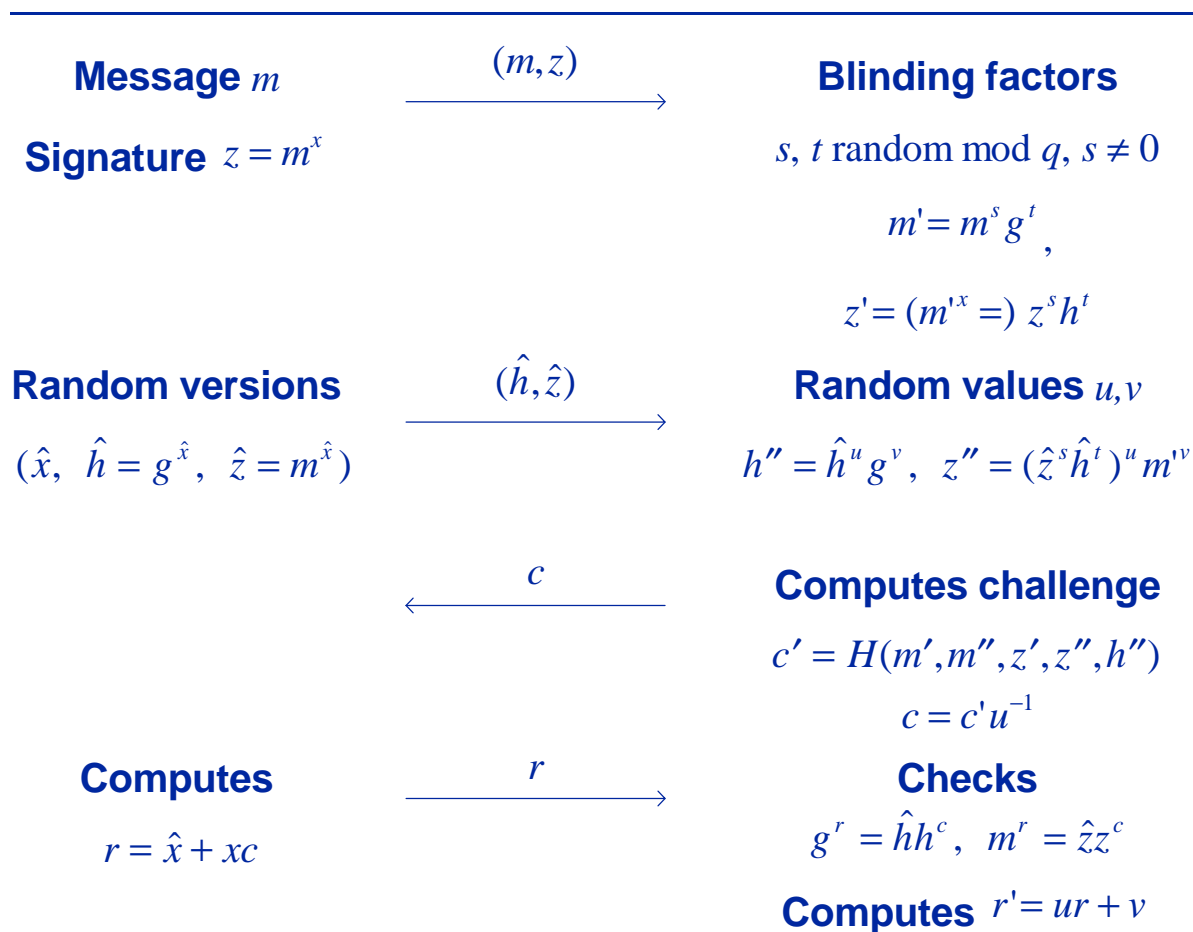
ecash™





Blinded Schnorr Signatures

$$(sk, pk) = (x, h = g^x)$$





Blinded Schnorr Signatures

u **Signature:** $(r', m', m'', z', z'', h'')$

u **Verifier checks**

$$h'' h^{c'} = (\hat{h}^u g^v) h^{cu} = (\hat{h} h^c)^u g^v = g^{ur+v} = g^{r'}$$

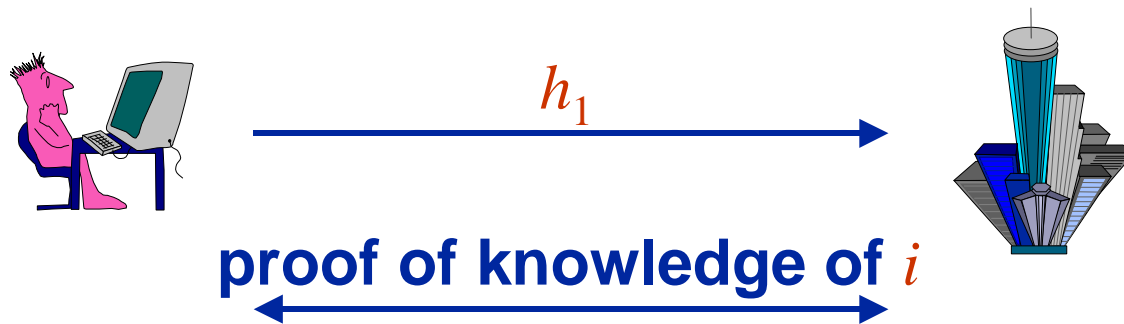
$$z'' z'^{c'} = (\hat{z}^s \hat{h}^t)^u m'^v (z^s h^t)^{cu} = (\hat{z} z^c)^{su} (\hat{h} h^c)^{tu} m'^v =$$

$$m'^{rsu} g^{rtu} m'^v = (m^s g^t)^{ru} m'^v = m'^{ru+v} = m'^{r'}$$



Brands' Restrictive Blinding

- u Let g_1, g_2 two new generators of G
- u Payer chooses index i and sets $h_1 := g_1^i$



- u **Message** $m = h_1 g_2 = g_1^i g_2$
- u In payments, payer has to know $m' = g_1^{x_1} g_2^{x_2}$
therefore blinding is restricted:

$$m' = m^s g^t = g_1^{is} g_2^s g^t \quad \stackrel{?}{\Rightarrow} \quad t = 0$$



Payment Protocol (1)

- u **Withdrawal:**

- u Payer performs blinded signature protocol with

$$m = g_1^i g_2, t = 0, \text{ thus } m' = g_1^{is} g_2^s$$

$$m'' = g_1^{y_1} g_2^{y_2} \text{ for randomly chosen } y_1, y_2$$

- u **Payment:**

- u Payer sends signature (m', m'', z'', h'')

- u Payee checks

- u Payer uses (m', m'') as public key for a fail-stop signature scheme, with secret key (is, s, y_1, y_2) .

- u Payer signs message

$$C = H(\text{all details, including payee's name + date})$$



Payment Protocol (2)

$$u \quad PK_{coin} = (m', m'') = (g_1^{is} g_2^s, g_1^{y_1} g_2^{y_2})$$

$$SK_{coin} = (x_1, x_2, y_1, y_2) = (is, s, y_1, y_2)$$

$$u \quad \text{Signature:} \quad \begin{aligned} s_1 &= x_1 C + y_1 \\ s_2 &= x_2 C + y_2 \end{aligned}$$

$$u \quad \text{Verification:} \quad g_1^{s_1} g_2^{s_2} = g_1^{x_1 C + y_1} g_2^{x_2 C + y_2} = m'^C m''$$

$$u \quad \text{Doublespending with } C, \tilde{C}$$

$$s_1 = x_1 C + y_1 \quad s_2 = x_2 C + y_2$$

$$\tilde{s}_1 = x_1 \tilde{C} + y_1 \quad \tilde{s}_2 = x_2 \tilde{C} + y_2$$



Payment Protocol (3)

u **Doublespending with** C, \tilde{C}

$$s_1 = x_1 C + y_1 \quad s_2 = x_2 C + y_2$$

$$\tilde{s}_1 = x_1 \tilde{C} + y_1 \quad \tilde{s}_2 = x_2 \tilde{C} + y_2$$

$$\Rightarrow \begin{aligned} x_1 &= \frac{s_1 - \tilde{s}_1}{C - \tilde{C}} \\ x_2 &= \frac{s_2 - \tilde{s}_2}{C - \tilde{C}} \end{aligned}$$

$$\Rightarrow i = \frac{x_1}{x_2} = \frac{s_1 - \tilde{s}_1}{s_2 - \tilde{s}_2}$$

**Identity of
Doublespender**



Payment Protocol (4)

- u **Applications**
 - u **Coins (*Brands*):**
 - u Each signature by bank has fixed denomination
 - u Cash represented by these coins
 - u **Cheques with Counter (*Brands, CAFE*):**
 - u Value is determined during payment
 - u Cash represented by tamper-resistant counters
- u **Extensions**
 - u **Loss tolerance / coin & cheque recovery**
 - u **Improved divisibility**
 - u **Improved storage: n -spendable coins / cheques**



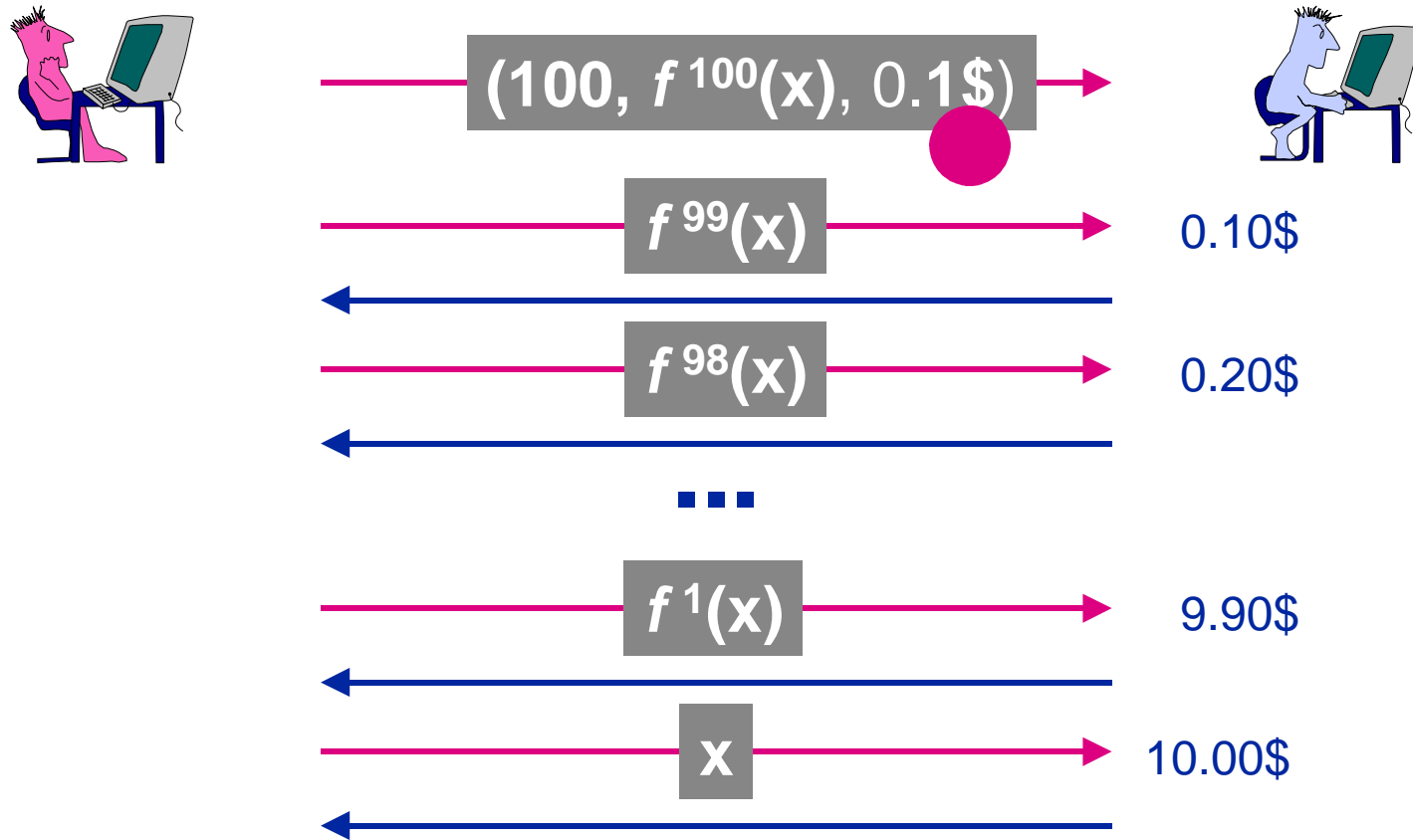
Different Notions of Micropayments

- u **Any combination of small amount (0.01 - 10 CHF)**
 - u with many **payments in short time**, and/or
 - u with payments to **many different payees**
 - u e.g., pay-per-click, metered access
- u **Problems**
 - u policy for implicit user authorization
 - u costs for clearing of small payments
 - u high frequency / constant payee: **CAFE**
 - u high frequency / different payees: **NetBill**
 - u low frequency: **MiniPay**
- u **Not clear yet**
 - u economic need for high frequency / different payees

Micropayments




CAFE Phone Ticks





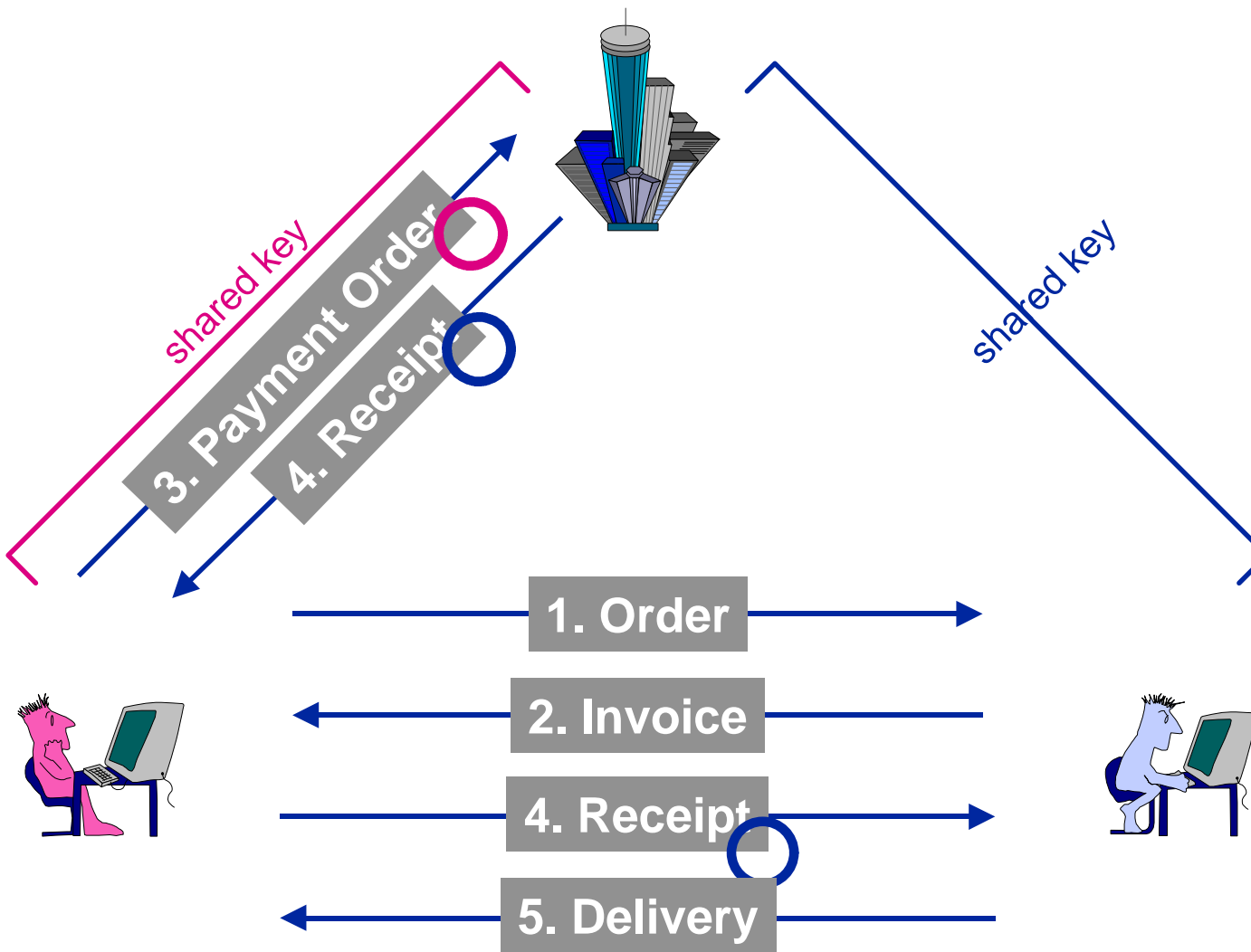
CAFE Phone Ticks

- 
 - u **Efficient**
 - u 1 hash per “tick”
 - u **Approximates fair exchange of tick / value**
 - u **Can be combined with any payment system**
 - 
 - u **Only for high frequency payments to *one* payee**
-
- u **Reinvented by several people afterwards:**
 - u Rivest/Shamir, Anderson, ...

Micropayments



Billing Server





Billing Server



- u **Efficient**
 - u MAC's are sufficient
- u **Billing server can ensure fairness**
 - u Keep money "on hold" until service delivered



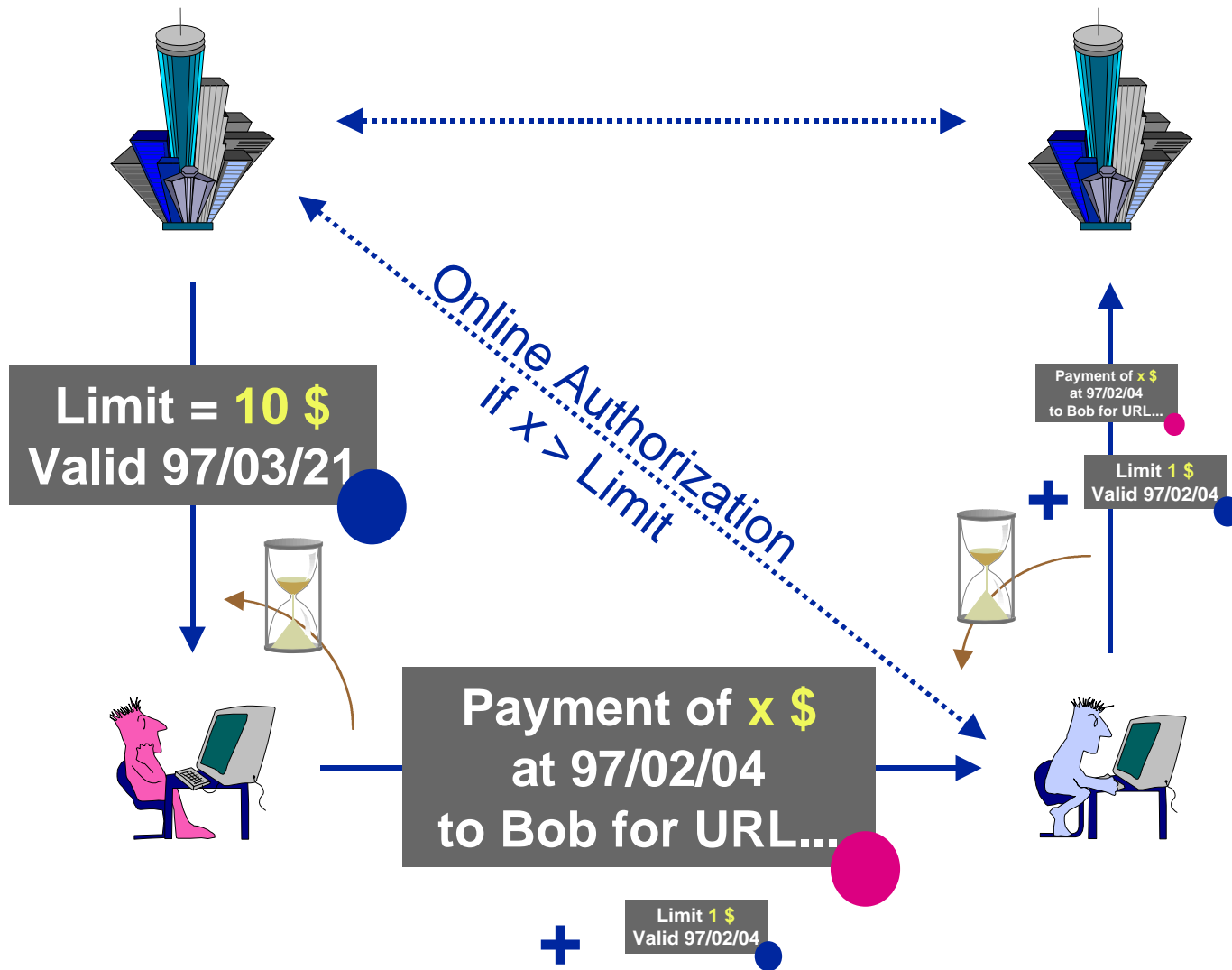
- u **Alice and Bob have to trust 1 billing server**
- u **Online third party**
 - u bottleneck
 - u must be trustworthy



- u **Also called "Payment Server", "Proxy Server"**
- u **Digital signatures instead of MACs for improved scalability and trust management**

Micropayments

IBM MiniPay





IBM MiniPay



- u **Message efficient**
- u **Offline in most cases**
- u **Signature based**
 - u non-repudiation of payment order
- u **Web integration, visibility of policy**



- u **Signature based**
 - u not for high frequency
- u **Fraud not 100% prevented**

