

Digital Money. Russia 2001



Dr.Victor Dostov, PayCash

www.paycash.ru

www.cyphermint.com

Report purposes

- What happens in Russian digital money
- How market and technologies evolve in last years
- Digital cash in 2001
- PayCash project

- In Russia, digital cash internet payment appeared almost simultaneously with credit card internet processing. This situation gives a chance to compare different payment systems in more "fair" environment



Russian Internet

6-10 mln. of persons with Internet access, 1-3 mln. active users

Compare: UK

dozens of “large” WWW-sites: 20,000+ visitors per day

Large mail and search portals (with 500K-1M of users.)



Successful e-commerce projects www.ozon.ru

Bookstore:

- books
- video
- ratings
- abstracts
- delivery
- payment options

~3500 visits per day

~300 purchases

~4% purchase/visits

Reality: e-retail – dozens of mln USD per year.

Problems

- low income
- legal (general)
- accounting
- taxes
- no inexpensive delivery system (almost no Quelle, in fact!)

- **No good payment system**

Payment methods in Russian e-commerce

Cash on delivery	80-85%
Cards	3-10%
Digital money	3-10%

Given

- e-payment systems needed badly
 - high math and software specialists' level
 - low credit card penetration rate
 - high credit card fraud rate (aggressive environment)
-

Yield

Fast progress in home-made e-payment systems

Segments

- Credit card processing
- Internet-banking
- smart cards
- scratch cards
- digital currency and alike

Internet banking

Mostly B2B. Reason – low penetration of private banking accounts.

Market (B2C, P2P) share: low

Smart cards

Practically dead till 2000. In 2000 – huge project by government-associated Sberbank. To April 2001 still no internet payments.

Scratch cards

- Standalone systems starting at beginning of 2001:
ePort, CreditPilot
- Embedded systems (Webmoney, Paycash)

Credit card processing

Dominating and very competitive segment appeared 2-3 years ago. About 50-80% (volume) of B2C online payments in different segments.

Major operators, **Cyberplat.com**, Menatep SPb, Assist, are consolidated with largest Russian banks.

Cyberplat.com			
	Local trans. per year	Intl. transactions per year	Shops
Dec 99	25,000	20,000	44
Dec 00	50,000	200,000	115

Digital cash and alike

Digital bearer certificates, bank accounts with digital signatures etc.

DBC #1234678988 Value: \$123.25

Underwritten: Tavrishesky Bank Date:12.1.98 11:01

U/W Digital Signature: 12345467575643434556563452678999


Main players: Paycash, Webmoney

Market share: 3-10%, but

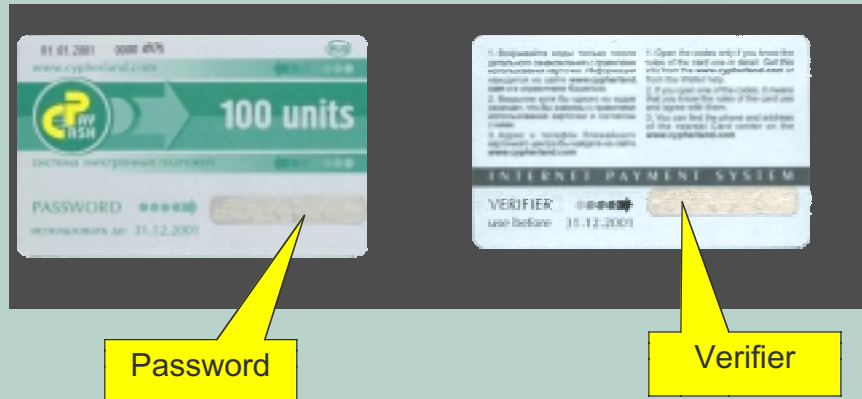
- large amount of [micro] transactions
- large amount of shops, including minishops (one program, etc)

PayCash (started 1997, running since 1999)

From Chaum's eCash toward

- less "external" trust needed ("untrustworthy" Bank)
- Multicurrency and multybanking
- Slow "used coins" database growth
- Contracts, embedded into payments
- New type scratch card support embedded 

Cypherland project New two-stage scratch card protocol



Patent: Method for a cardholder to request fulfilment of an obligation associated with the card and for the issuer to acknowledge this obligation

Beyond Chaum's patent umbrella

Patents:

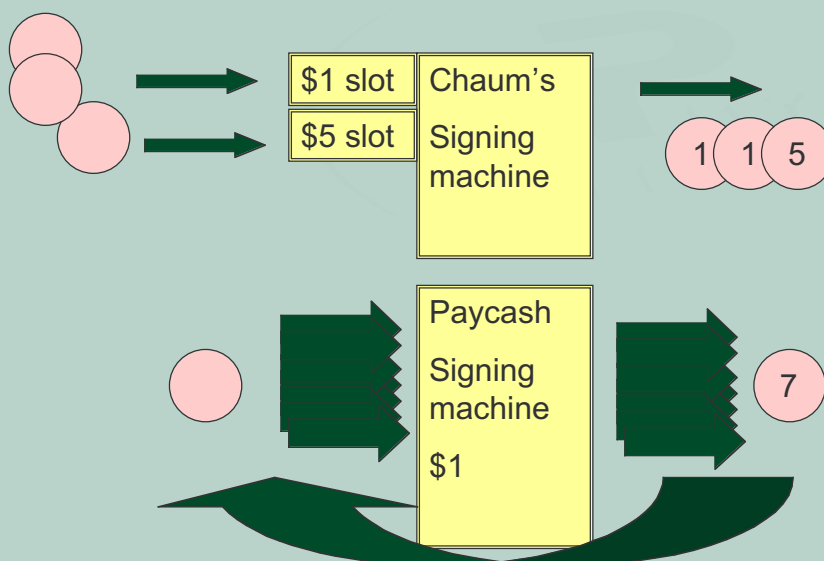
- 1) METHOD FOR MAKING A BLIND RSA-SIGNATURE AND APPARATUS THEREFOR
- 2) METHOD FOR EFFECTING PAYMENTS AND APPARATUS THEREFOR

Main ideas

One *paybook* instead of multitude of coins
Used coin databases almost does not grow vs. time

Contracts associated with payments
Payment purposes and conditions can be fixed for future investigations (court, e.g.)

Digital coins vs. paybooks



Some math

$$\text{Chaum's Coin}(i, X) = \{i, X, g_i^{-1}(f(X))\},$$

where X is the random serial number of a coin, chosen by a customer, X belongs to a large set $M' \subset M = (\mathbb{Z}/m\mathbb{Z})^*$, m is a composite number whose factorization is known only to the bank, $f: M' \rightarrow M$ is an easy-to-calculate mapping publicly known and hard-to-invert for all parties of the payment system except, possibly, for the bank

$$\text{PayBook}(N, P) = \{N, P, g^N(f(P))\},$$

where P is User's random public key, f , and g have the same meaning as above, and $g^N(X) = g(g^{-1}(\dots g^{-1}(X)\dots))$. A nonnegative integer N (the disposition of the book) determines paying capacity of the book.



PayCash industrial version started 2001

Positive:

1. System works stable and is attractive for shops
2. Testing group: 20,000 users, 100+ shops
3. Main shops: games/casinos, internet access, books/CD, software portals
4. Minishops: software, services, etc.
5. Branding and loyalty programs
6. Productivity/scalability: 2 PII 550 MHz
20 payments per second – 1.5 mln. per day

Problems:

Small market share comparing to cash-on-delivery

Paypal
0.15 mln. ppd
6 mln. users

**Paycash in exCIS:
Latvia (Netmaks)
Ukraine (Paycash Ukraine).**

- Relatively small Internet auditorium and e-commerce penetration
- Very high motivation
- Trans-border payments
- Virtual banks with real e\$ are due to May

Paycash in USA: Cyphermint Inc.

- Company start-up in March 00
- Established in NY, office in Boston
- January 01 – first contract with bidz.com
- Virtual bank with real e\$ due to May

Bottleneck is to put money into the system

Compare: eGold

Cash in offices	Inconvenient
Bank (wire) transfers	Low amount of private accounts, fees. Requires special software
Credit cards	Fraud rate up to 90%
Scratch cards (proprietary protocol)	Dealer Commissions, taxes

Market concepts evolution

INCREASED	DECREASED
Corporate systems (portals, large shops, casinos, FOREX, etc.)	Full (Chaum's) privacy role
Branding and loyalty programs	Positions of cards in retails look strong
	Micropayments

Competitors 2001

Scratch cards	Simple system with easy money input	High cost of distribution -> limited segment. One way payments
Virtual (disposable) credit (debit) cards like 7-11/AMEX.	Ready infrastructure	More or less traditional, although improved. Productivity.

www.paycash.ru
vd@mailbox.alkor.ru