Neuro - Taxable Electronic Payments with Customer-Anonymity

Florian Dold, Benedikt Müller

Department for Computer Science
Technische Universität München

June 12, 2014

Motivation

What we want.

Motivation

Where we want it.

Motivation

What we have.

Naming

Neuro

- borrowed from Euro and new/network or possibly gNu
- other awesome suggestions are welcome

Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macro- and micropayments

Requirements

- **Customer anonymity**
  It should not be possible to trace the spending behavior of a customer.
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macro- and micropayments

Requirements

- Customer anonymity
- **Unlinkability**
  It should be infeasible to link a set of transactions (even aborted ones) to the same customer.
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macro- and micropayments

Requirements

- Customer anonymity
- Unlinkability
- **Taxability**
  As it is the responsibility of the merchant to deduct taxes, he should be fully auditable and non-anonymous.
  Additionally it must not be possible to transfer cash illicitly (i.e. evading audit).
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macro- and micropayments

Requirements

- Customer anonymity
- Unlinkability
- Taxability
- **Verifiability**
  The trust necessary between the participants of the system should be minimized.
  Signatures over contractual information should be available in order to resolve disputes.
- Ease of deployment
- Green / low resource consumption
- Macro- and micropayments

Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- **Ease of deployment**
  Low entry-barrier by providing a gateway to the existing financial system (i.e. Internet-banking protocols such as HBCI/FinTS), a free software reference implementation and a open protocol standard.
- Green / low resource consumption
- Macro- and micropayments

Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- **Green / low resource consumption**
  Avoid reliance on expensive and especially ”wasteful” computations such as proof-of-work.
- Macro- and micropayments

Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- **Macro- and micropayments**
  The system should be able to provide a solution for macro as well as micropayments.

Related Work

- **Chaum style electronic cash[Cha83]**
- Opencoin
- Peppercoin
- Bitcoin
- Zerocoin
- Brands

Chaum style electronic cash

Key ideas proposed by Chaum:

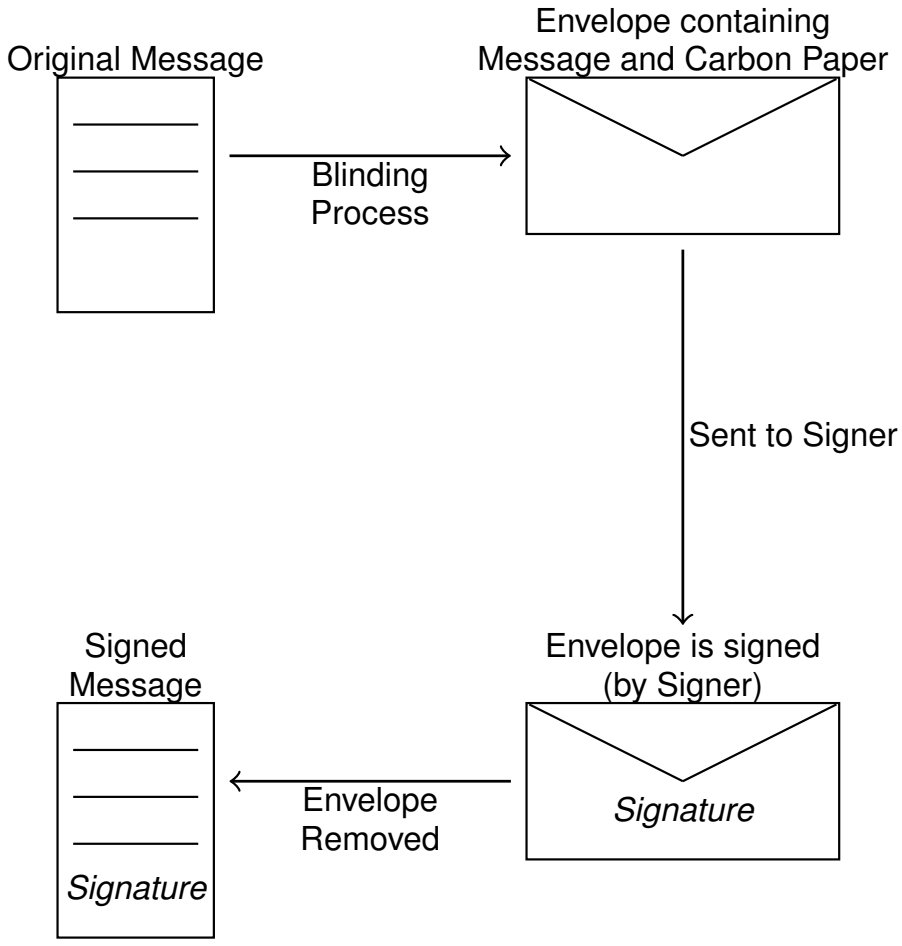
- Anonymity of customer
- Verifiability of payment
- Blind signatures as a means of providing anonymity of customer
- Possibility to utilize post-hoc detection of double-spending

Chaum style electronic cash

Requirements by Chaum:

- Public/private key digital signatures
- Blind signatures (as proposed by Chaum)
- Conservation of signatures (i.e. from one blindly signed value only one unblinded signed value can be derived)

Blind signatures



Chaum style electronic cash

Requirements for blind signatures by Chaum:

- Public key crypto such that $D_{pub}(E_{priv}(x)) = x$ where E_{priv} is the private encryption function and E_{pub} the public decryption function.
- A commuting function c and its inverse c' both only known to the customer with $c'(E_{pub}(c(x))) = E(x)$.

Chaum style electronic cash

Basic protocol for blind signatures:

1. Customer chooses x at random, computes and provides $c(x)$ to mint
2. Mint signs $c(x)$ with E_{priv} and returns $E_{priv}(c(x))$ to customer
3. Customer strips signed matter by application of c'. $c'(E_{priv}(c(x))) = E_{priv}(x)$

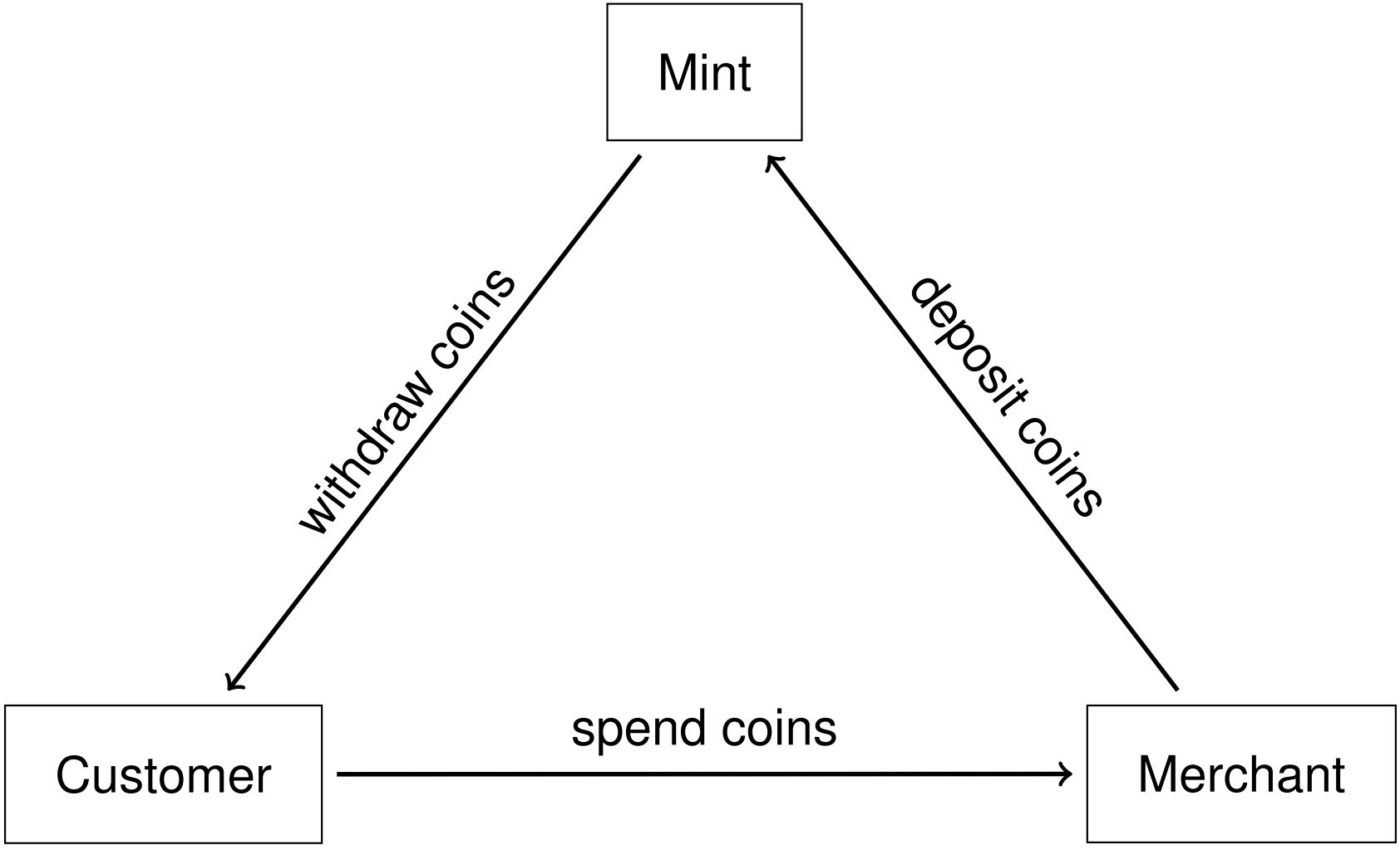
Example RSA blind signature scheme

- Generate RSA key pair
- Choose a random value r that is relatively prime to N
- Blinding factor $B = r^e mod N$

1. Customer $\rightarrow$ Mint: $m' \equiv mr^e \pmod{N}$
2. Customer $\leftarrow$ Mint: $s' \equiv (m')^d \pmod{N}$
3. Customer removes the blinding factor to reveal s, the valid RSA siganture of m: $s \equiv s' \cdot r^{-1} \pmod{N}$

- RSA keys satisfy $r^{ed} \equiv r \pmod{N}$ an thus $s \equiv s' \cdot r^{-1} \equiv (m')^d r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod{N}$

Architecture of Chaum style currencies



Payment scheme by Chaum

1. Customer chooses random coin identifier, blinds and send it to mint.
2. Mint signs blinded value, giving the coin its value as note of currency and sends it back to customer
3. Customer unblinds the value. The coin is now spendable
4. Coin is sitting in customer's wallet for some time
5. Customer provides signed value to merchant as means of payment
6. Merchant forwards the signed value to the mint
7.
   - Mint adds the value to the list of spent coins and informs merchant of acceptance
   - Mint recognizes double spending and reconstructs identity of customer
8. Mint credits account of merchant

Related work

- Chaum style electronic cash
- **Opencoin**
- Peppercoin
- Bitcoin
- Zerocoin
- Brands

Opencoin

- Attempt to implement Chaum style digital cash
- Free software implementation (GPL)
- Uses post-hoc double spending
- Project status: abandoned
- See opencoin.org

Related work

- Chaum style electronic cash
- Opencoin
- **Peppercoin[Riv04]**
- Bitcoin
- Zerocoin
- Brands

Peppercoin

- Based on probabilistic selection
- Proposed as extension to current payment systems (such as credit card)
- Addresses problem of expensive transactions
- $1\text{ct} \approx 0.1\% \cdot 10€$

Peppercoin - aggregation models

- Session level aggregation
- Aggregation by intermediation
- Universal aggregation

Peppercoin - aggregation models

- **Session level aggregation**
  - Consumer repeatedly makes small purchases with same vendor
  - Limited scope, not applicable in general
- Aggregation by intermediation
- Universal aggregation

Peppercoin - aggregation models

- Session level aggregation
- **Aggregation by intermediation**
  - Intermediary has to emulates financial system
  - Increases complexity and processing instead of minimizing it
  - Intermediary still needs to handle each payment
- Universal aggregation

Peppercoin - aggregation models

- Session level aggregation
- Aggregation by intermediation
- **Universal aggregation**
  - Merchant processes micropayments
  - Only “upgraded” micropayments - macropayments are relayed to the mint
  - mint buffers upgraded payments in case the cumulative value of spent micropayments is lower than the upgraded payment
  - Upgrade selection not random but based on deterministic values

Peppercoin - Downsides

- No exact payments possible
- No customer anonymity
- Customer and merchant can conspire against mint

Related work

- Chaum style electronic cash
- Opencoin
- Peppercoin
- **Bitcoin[Nak08]**
- Zerocoin
- Brands

Bitcoin

Why Bitcoin will NOT be the payment system of the future:

- No taxability
- No unlinkability $\rightarrow$ limited anonymity
- No fast and cheap transactions
- No stable value
- Waste of resources (transaction-chain, proof-of-work, bandwidth)

Related work

- Chaum style electronic cash
- Opencoin
- Peppercoin
- Bitcoin
- **Zerocoin[MGGR13]**
- Brands

Zerocoin

- Extension to Bitcoin
- Removes linkability by conversion (BC $\rightarrow$ ZC $\rightarrow$ BC)
- No trusted third parties necessary
- Uses massive crypto (zero-knowledge proofs, cryptographic accumulators, commitment schemes, etc)
- $\rightarrow$ secure money laundering

Related Work

- Chaum Style Electronic Cash
- Opencoin
- Peppercoin
- Bitcoin
- Zerocoin
- **Brands[Bra93]**

Brands

- Based on Chaums architecture
- Realizes divisibility by k-show signatures
- Post-hoc double spending detection
- Proposes the integration of a ”secure” observer into customers wallet :(
- Mainly theoretical, has never been implemented

Neuro

Assumptions

- Existence of anonymous channel (customer $\rightarrow$ mint, customer $\rightarrow$ merchant)
- **Curve25519 elliptic curve cryptography**
- Blind signatures over elliptic curves
- Hash functions :)
- but: no global/state PKI

Curve25519

- Elliptic curve cryptography curve by Daniel J. Bernstein
- Used by wide variety of software (e.g. GNUnet)
- Optimized for and fast on 64-bit x86 processors
- No magic constants by NIST/NSA
- EdDSA: small signature (64 byte) and private/public key (32 byte)

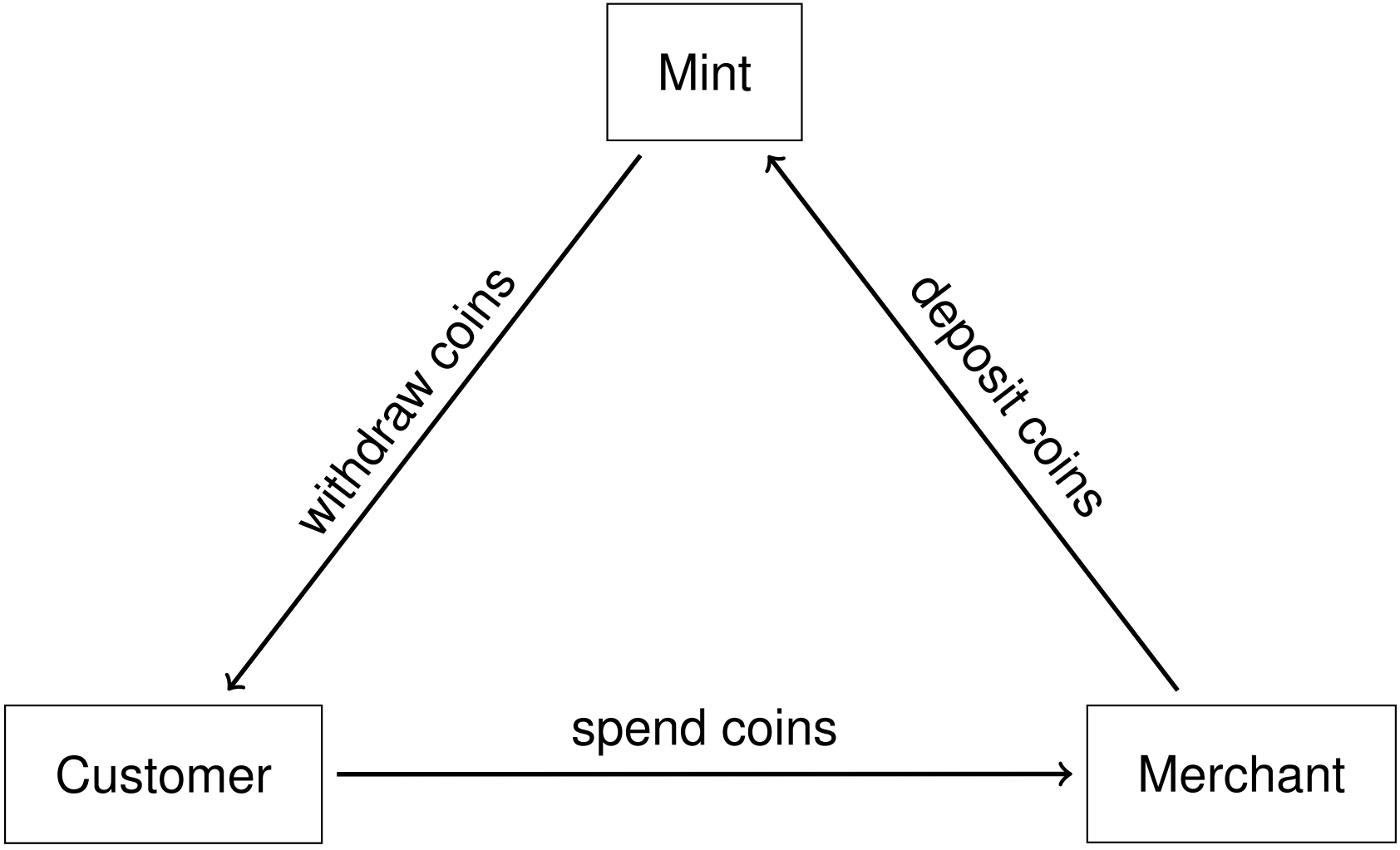
Assumptions

- Existence of anonymous channel
- Curve25519 elliptic curve cryptography
- **Blind signatures over elliptic curves**
- Hash Functions

Blind signatures on elliptic curves

- Multiple new proposals
- Different message order
- Some contain errors or are faulty
- Different but similar
- No final decision on protocol yet

Architecture of Neuro



The Neuro Coin

- Identified by public key
- Only owner knows private key
- Signature of public key by mint denomination key
- Operations are authorized by signature of coin private key
- Expiration date defined by denomination key

The Neuro Mint

- Mints new Neuro coins
- Holds list of all (partially) spent but not expired coins
- Earns money by collecting fees
- Restricted trust necessary, correctness legally enforceable
- It is of economical interest for the mint to operate correctly

Security model: financial security

- Mint is compromised (key lost)
- Mint goes offline
- Hardware failure
- Packet loss/network loss

Security model: adversary

Adversary cannot break crypto primitives $\rightarrow$ privacy guarantee

- Mint can only link customers to coin set
- Customer is not requiered to use his identity

Modes of spending

- Partial Spending
  - Online Payment
  - Lock fraction of a coin
  - Give deposit permission for a fraction
  - Repeat with remaining fraction of the coin
- Incremental spending
  - Online payment
  - Lock maximum amount of coin customer wants to spend
  - Incrementally give deposit permission
- Probabilistic spending (bona fide)
  - Offline payment
  - Gambling for payment ”upgrade”
  - Interaction with mint only when payment gets upgraded
  - Anti-piracy strategies: “Accept and Embrace”, “Detect and Adapt”

Refreshing

Crucial to avoid linkability as merchant knows Coin from

- aborted transactions
- partially spent coins

Illicit transactions

- Transaction after which the private key of a coin is only known by the new owner.
- Transaction that is not registered as a payment by the mint.

Refreshing extended

Avoid possibility to use refreshing for illicit/black market transactions

- Store encrypted private key of new coin with mint
- Make it possible to retrieve the private key of every new coin derived from the old coin with only the private key of the old coin
- Use cut-and-choose to prevent customer from using fake old coin key

SEPA and HBCI Integration

Homebanking Computer Interface (HBCI)

- German standard
- Finalized by Zentraler Kreditausschuss (ZKA)
- Using custom protocol on port 3000 or standard HTTPS
- Supported by most German banks

REST API / JSON

REST API

- using HTTP1.1
- and JSON

Fee Model

A Mint can charge fees for:

- Minting
- Refreshing
- Depositing

The End

Questions?

BRANDS, Stefan A.:

An efficient off-line electronic cash system based on the representation problem.

1993

CHAUM, David:

Blind signatures for untraceable payments.

In: *Advances in cryptology* Springer, 1983, S. 199–203

MIERS, Ian ; GARMAN, Christina ; GREEN, Matthew ; RUBIN, Aviel D.:

Zerocoin: Anonymous distributed e-cash from bitcoin.

In: *Security and Privacy (SP), 2013 IEEE Symposium on* IEEE, 2013, S. 397–411

NAKAMOTO, Satoshi:

Bitcoin: A peer-to-peer electronic cash system.

In: *Consulted* 1 (2008), S. 2012

RIVEST, Ronald L.:

Peppercoin micropayments.

In: *Financial Cryptography* Springer, 2004, S. 2–8