Authcoin

Validation and Authentication in Decentralized Networks

Benjamin Leiding [1] Clemens H. Cap [2] Thomas Mundt [2]
Samaneh Rashidibajgan [2]

[1]University of Göttingen
benjamin.leiding@cs.uni-goettingen.de

[2]University of Rostock
{*clemens.cap,thomas.mundt,samaneh.rashidibajgan*}*@uni-rostock.de*

September 6, 2016

Overview

Introduction

Motivation

Existing solutions

- Certificate authorities (CAs)
- PGP Web of Trust
- Certcoin

BUT: All of them suffer from several disadvantages.

Certificate Authorities (CAs)

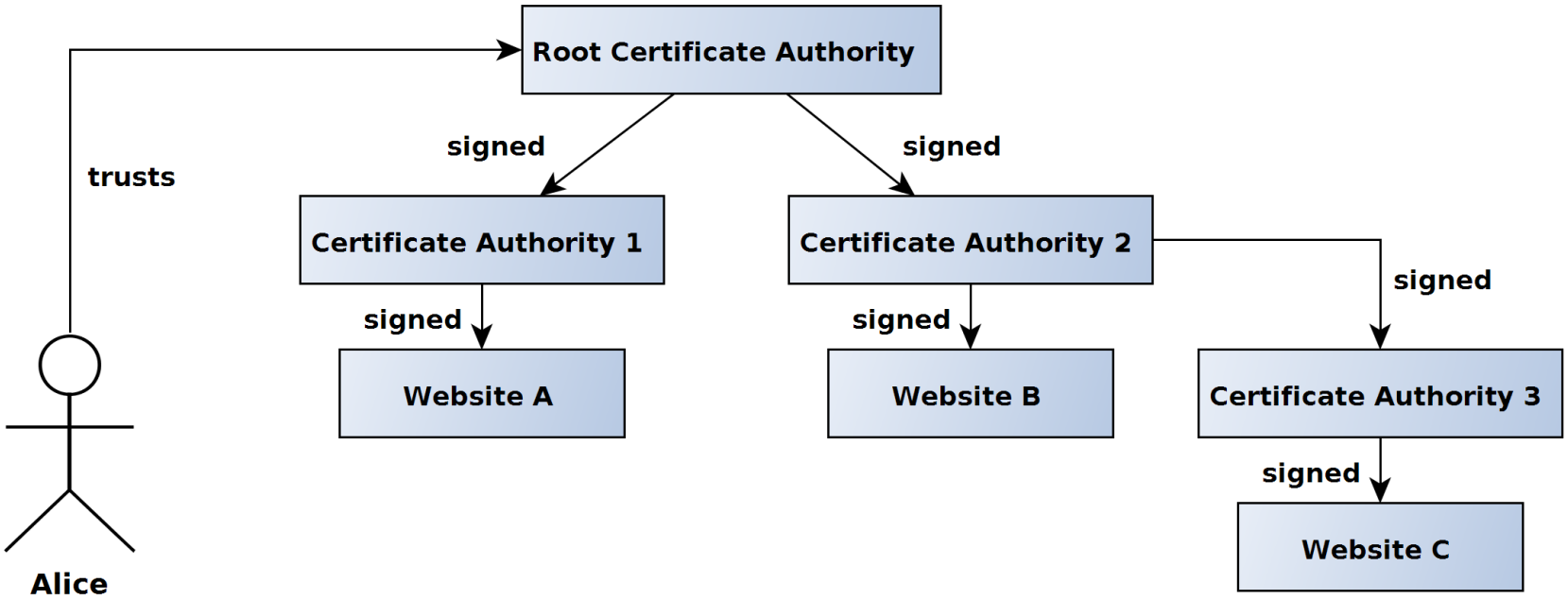


Figure: Hierarchical trust model

PGP Web of Trust

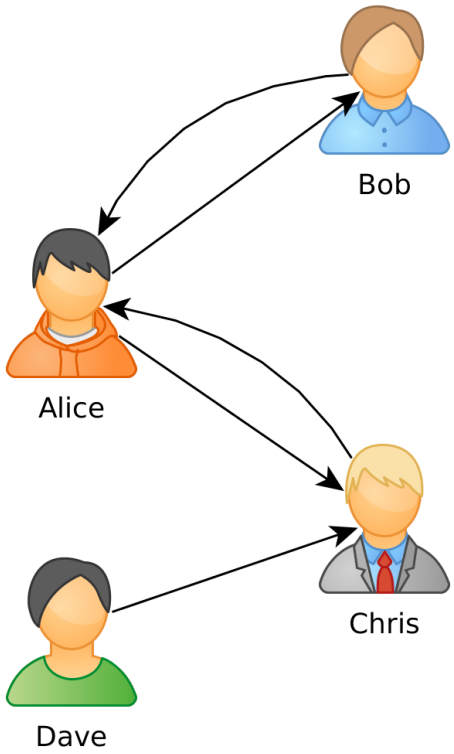


Figure: PGP Web of Trust

- Decentralized trust model for public keys
- Mainly used for encrypted email communication
- Users sign other users' public key using their own private key to certify authenticity
- Interpreting each key as node and each signature as directed edge results in a directed graph $\rightarrow$ The PGP Web of Trust

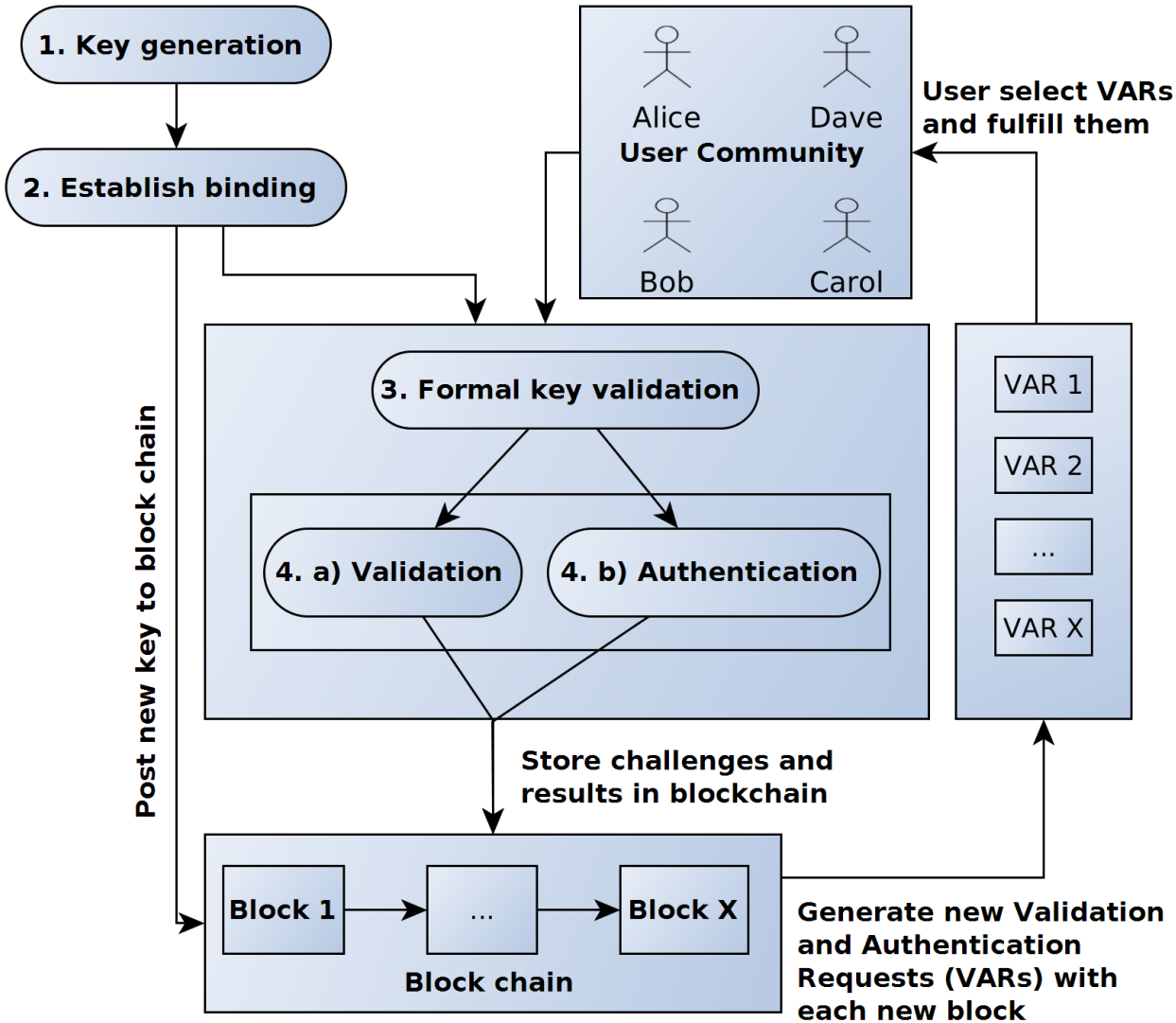
Certcoin

An alternative approach

- PGP Web of Trust + Block chain = Certcoin
- Shares similarities with Authcoin
- Inherited almost all disadvantages of the PGP Web of Trust
- ~~Has not been implemented yet~~

Authcoin

Overview


1. Key generation
2. Establish binding
Alice
Dave
User Community
Bob
Carol
User select VARs and fulfill them
3. Formal key validation
4. a) Validation
4. b) Authentication
VAR 1
VAR 2
...
VAR X
Post new key to block chain
Store challenges and results in blockchain
Block 1
...
Block X
Block chain
Generate new Validation and Authentication Requests (VARs) with each new block

General Validation and Authentication

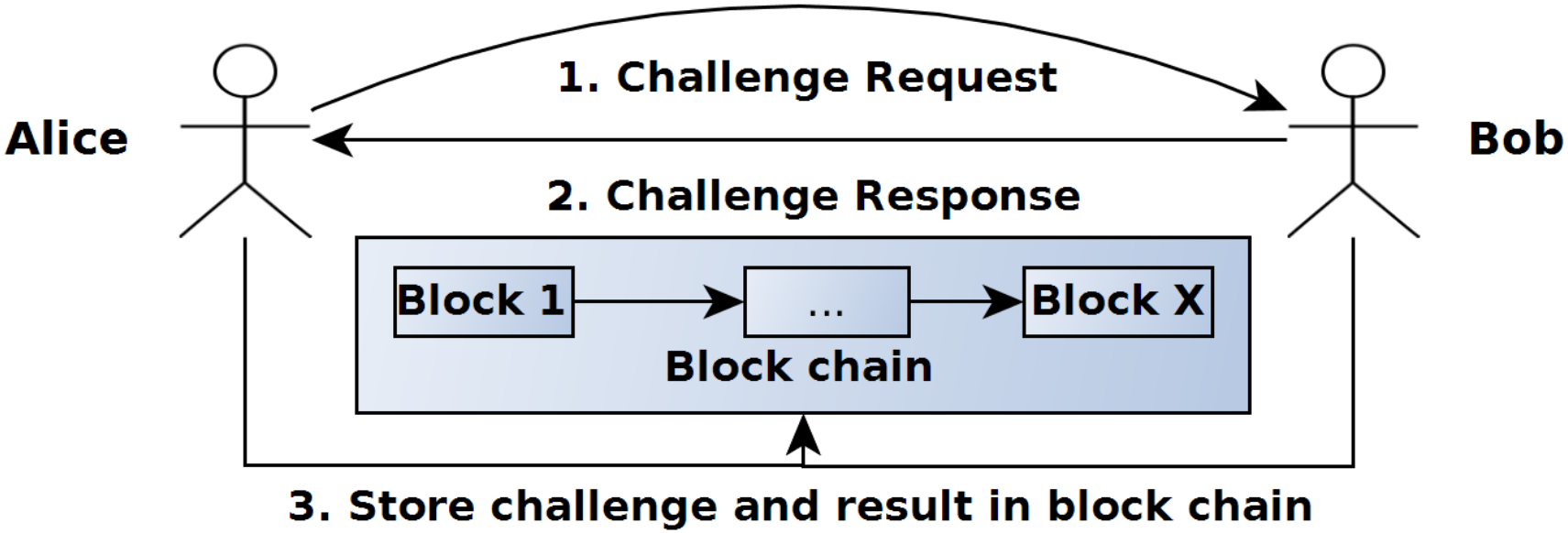


Figure: General V&A procedure

Validation and Authentication

Validation

1. An entity has access to the email account (account validation)
2. Same entity has access to the public and private key (key validation)
3. The key pair corresponds to the tested email account (binding)

Authentication

- Verify the identity of the entity.

Challenges

Challenges in a Nutshell

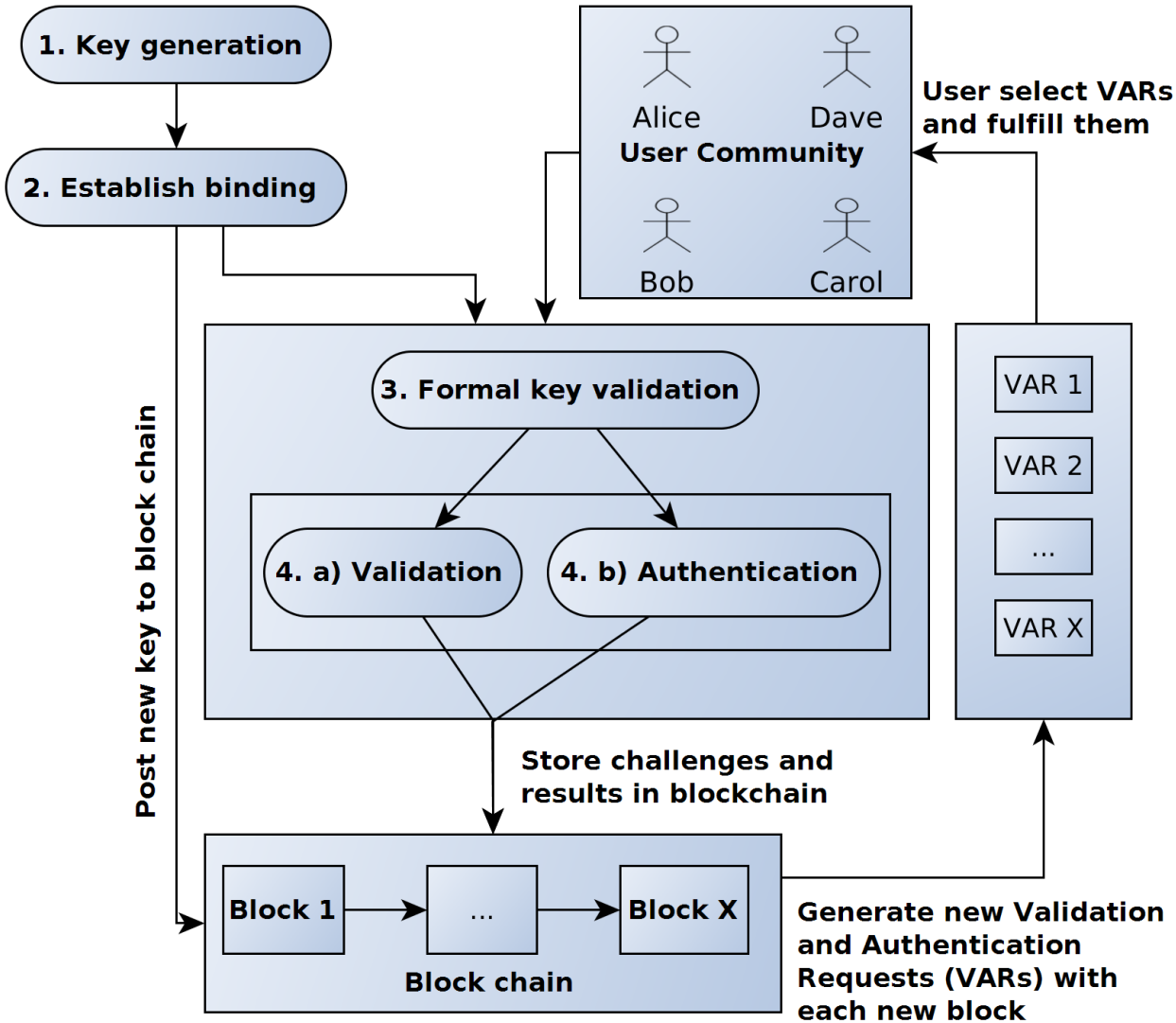
- Security depends on chosen challenges
- Flexible and customizable (use case, threat level, available information)
- Bidirectional validation and authentication
- Varying complexity
- Users have to interpret information

Storing Information

Block chain

- Store keys, signatures, challenges, responses, etc
- Utilize advantages of block chain-based storage: decentralized, distributed, fault tolerant, transparent, difficult to manipulate, etc.
- Either setup own chain or utilize existing one (as Namecoin does)

Overview


1. Key generation
2. Establish binding
Alice
Dave
User Community
Bob
Carol
User select VARs and fulfill them
3. Formal key validation
4. a) Validation
4. b) Authentication
VAR 1
VAR 2
...
VAR X
Post new key to block chain
Store challenges and results in blockchain
Block 1
...
Block X
Block chain
Generate new Validation and Authentication Requests (VARs) with each new block

Automated Validation and Authentication Requests

Validation and Authentication Requests (VARs)

- Automatically and randomly create with each new block
- Number of generated VARs depends on number of valid keys in chain
- Break into sybil collectives "by accident"

Conclusion and Future Work

Conclusion

Conclusion

- Highly flexible Challenge-Response-based V&A
- Bidirectional V&A
- Tamper-proof and transparent information storage (block chain)
- More resilient against sybil node attacks than current solutions
- No single point of failure

Future Work

Future Work

- Implementation
- API-based incentive system
- Abstract from key pair use case
- Biometric identifiers?

Questions?