blockchain.taltech.ee

SECURE AND FLEXIBLE BLOCKCHAIN-BASED NON-GOVERNMENTAL ID-AUTHENTICATION FOR SOCIOTECHNICAL SYSTEMS APPLICATIONS

Alex Norta (Assoc.Prof.PhD.MSc.)
Department of Software Science/ Institute of Information Technology
Tallinn University of Technology

27.03.2019

AGENDA

- My own accidental venture into smart contracts and blockchains
  - Stories from my old PhD days
  - Wild ventures into the ICO space
  - Sociotechnical consequences of blockchain application
- Basic introduction of blockchains and smart contracts
  - Problems that blockchains solve
  - Smart-contract ecosystem overview
- Case presentation of blockchain-based Authcoin securing
  - Authcoin is non-governmental ID-authentication protocol
  - Security risk-oriented patterns stress testing
  - We show the application methodology to secure Authcoin protocol

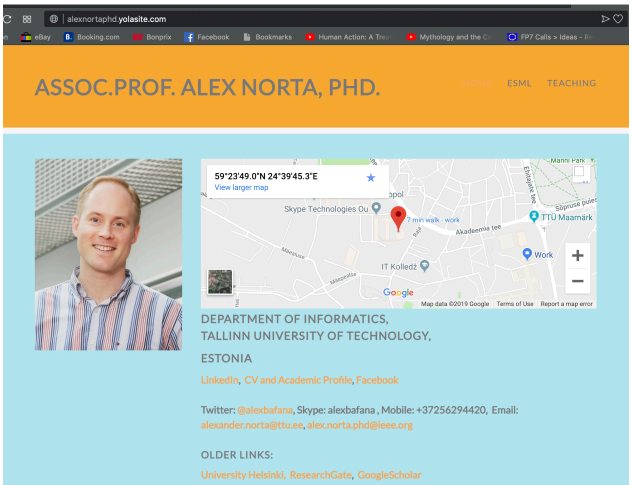
TALLINN UNIVERSITY OF TECHNOLOGY

BLOCKCHAIN TECHNOLOGY GROUP

MY OWN JOURNEY TO SMART CONTRACTS

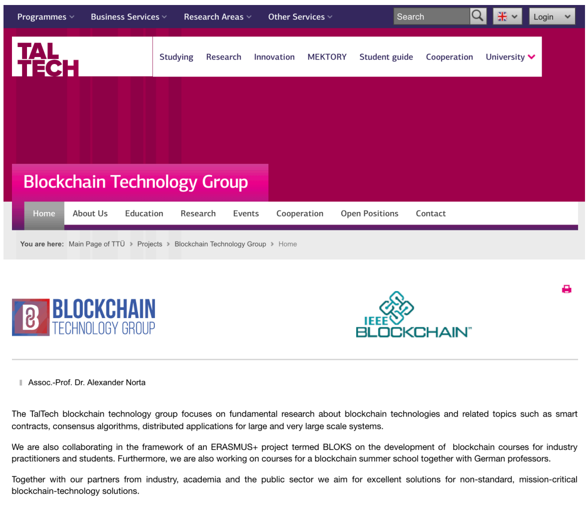
BLOCKCHAIN TECHNOLOGY GROUP

MY OWN JOURNEY TO BLOCKCHAINS (SMART CONTRACTS)



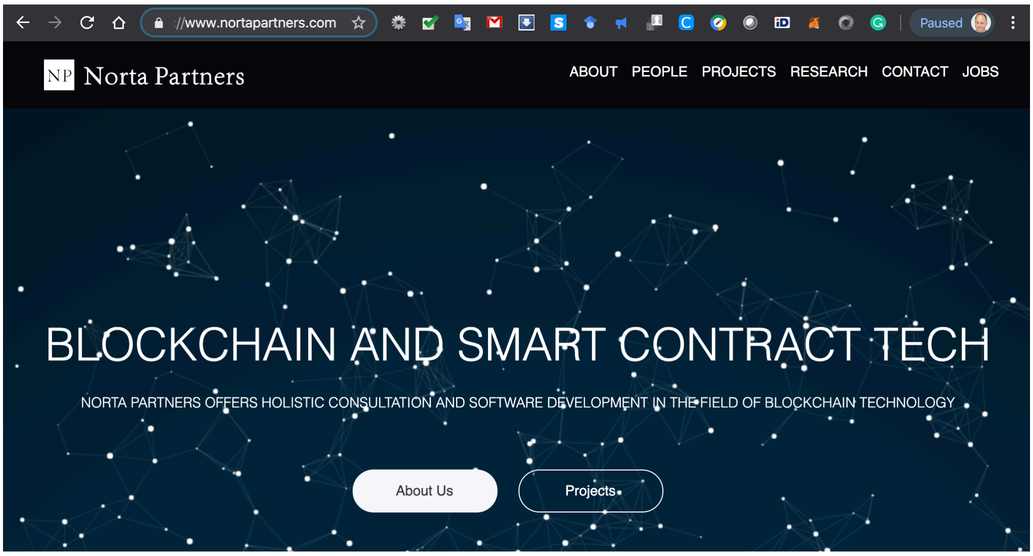
TALTECH TALLINN UNIVERSITY OF TECHNOLOGY

blockchain.taltech.ee



MY OWN JOURNEY TO BLOCKCHAINS (SMART CONTRACTS)

BLOCKCHAIN TECHNOLOGY GROUP

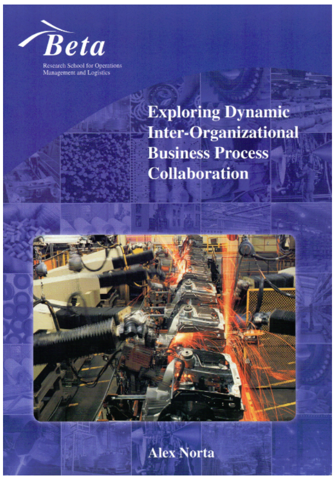


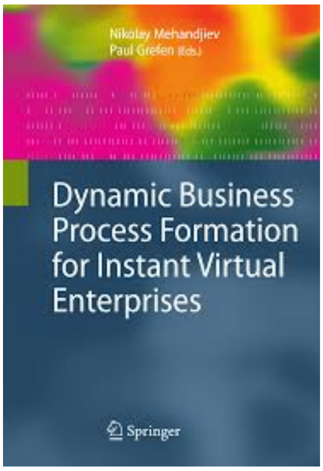
TAL TECH

MY OWN JOURNEY TO BLOCKCHAINS (SMART CONTRACTS)

BLOCKCHAIN TECHNOLOGY GROUP

- Serendipity has brought me here





TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

MY OWN JOURNEY TO BLOCKCHAINS (SMART CONTRACTS)

BLOCKCHAIN TECHNOLOGY GROUP

- Some of my earlier papers

Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations

Alex Norta

Department of Informatics, Tallinn University of Technology, Akademia tee 15A, 12816, Tallinn, Estonia
alex.norta.phd@ieee.org

Norta et al. Journal of Internet Services and Applications (2015) 6:8
DOI 10.1186/s13174-015-0023-7

Journal of Internet Services and Applications
a SpringerOpen Journal

RESEARCH Open Access

eContractual choreography-language properties towards cross-organizational business collaboration

Alex Norta[1*], Lixin Ma[1,3], Yucong Duan[2], Addi Rull[1], Merit Kõlvart[1] and Kuldar Taveter[1]

Establishing Distributed Governance Infrastructures for Enacting Cross-Organization Collaborations

Alex Norta

Department of Informatics, Tallinn University of Technology, Akademia tee 15A, 12816, Tallinn, Estonia
alex.norta.phd@ieee.org

SOCA (2016) 10:233–251
DOI 10.1007/s11761-015-0183-0

CrossMark

ORIGINAL RESEARCH PAPER

Sound conflict management and resolution for virtual-enterprise collaborations

Nanjangud C. Narendra[1] · Alex Norta[2] · Msury Mahunnah[2] · Lixin Ma[4] · Fabrizio Maria Maggi[3]

Conflict-Resolution Lifecycles for Governed Decentralized Autonomous Organization Collaboration

Alex Norta, Anis Ben Othman, Kuldar Taveter
Tallinn University of Technology, 12618 Akadeemia tee 15A, Tallinn, Estonia
alex.norta.phd@ieee.org, anis.ben@gmail.com, kuldar.taveter@ttu.ee

Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations

Alex Norta

Department of Informatics, Tallinn University of Technology, Akademia tee 15A, 12816, Tallinn, Estonia
alex.norta.phd@ieee.org

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

DISTRIBUTED APPLICATIONS (DAPPS)

BLOCKCHAIN TECHNOLOGY GROUP

- Some whitepapers for DAPPS

Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform

Patrick Dai[1], Neil Mahi[1], Jordan Earls[1], Alex Norta[2]

[1] Qtum Foundation, Singapore
foundation@qtum.org
[2] Large-Scale Systems Group, Tallinn University of Technology, Akademia tee 15A, 12816 Tallinn, Estonia
alex.norta.phd@ieee.org

Self-Aware Agent-Supported Contract Management on Blockchains for Legal Accountability

Alex Norta[1,2], Anton Vedeshin[1], Hando Rand[1], Simon Tobies[2], Addi Rull[1,2], Margus Poola[1,2], Teddi Rull[1]

[1] Agrello OÜ
Pärnu mnt. 548-15, 10916 Tallinn, Estonia
hando@agrello.org, addi@agrello.org
[2] Large-Scale Systems Group, Tallinn University of Technology, Akademia tee 15A, 12816 Tallinn, Estonia
alex.norta.phd@ieee.org

Lowering Financial Inclusion Barriers With a Blockchain-Based Capital Transfer System

Whitepaper

Alexi Lane[1], Benjamin Leiding[2], and Alex Norta[3]

[1] Everex, Singapore
alexi@everex.io
[2] Chaindrium, Göttingen, Germany
mail@chaindrium.com
[3] Large-Scale Systems Group, Tallinn University of Technology, Tallinn, Estonia
alex.norta.phd@ieee.org

CEDEX
A Certified Blockchain Based Diamond Exchange
WHITE PAPER
TRANSFORMING DIAMONDS INTO A NEW ASSET CLASS

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

BLOCKCHAIN TECHNOLOGY GROUP

DISTRIBUTED APPLICATIONS (DAPPS)

- Some whitepapers for DAPPS

A Data-Ownership Assuring Blockchain Wallet For Privacy-Protected Data Exchange
Version 1.0

Daniel Hawthorne[1], Serafin L. Engel[1], Alex Norta[2]

[1] Pnyks Inc.
55E 3rd Ave San Mateo, CA 94401 USA
[2] Large-Scale Systems Group, Tallinn University of Technology,
Akadeemia tee 15A, 12616 Tallinn, Estonia

Tokenizing Commercial Property With Smart Contracts

Chad Fernandez[1], Sergey Petkevic[1], and Alex Norta[3]

[1] Blockgemini.com, UAB
chad@blockgemini.com, sergey@blockgemini.com
[2] Large-Scale Systems Group, Tallinn University of Technology, Estonia
alex.norta.phd@ieee.org

- Research paper examples

Mapping Requirements Specifications into a Formalized Blockchain-Enabled Authentication Protocol for Secured Personal Identity Assurance

Benjamin Leiding[1] and Alex Norta[2]

[1] University of Göttingen, Institute of Computer Science, Göttingen, Germany
benjamin.leiding@cs.uni-goettingen.de
[2] Department of Software Science, Tallinn University of Technology, Tallinn, Estonia
alex.norta.phd@ieee.org

Safeguarding a Formalized Blockchain-Enabled Identity-Authentication Protocol by Applying Security Risk-Oriented Patterns

Alex Norta
Large-Scale-Systems Group
Tallinn University of Technology,
12618 Akadeemia tee 15A,
Tallinn, Estonia
Email: alex.norta.phd@ieee.org

Raimundas Matulevičius
Institute of Computer Science,
University of Tartu, J. Liivi 2, 50409,
Tartu, Estonia
Email:rma@ut.ee

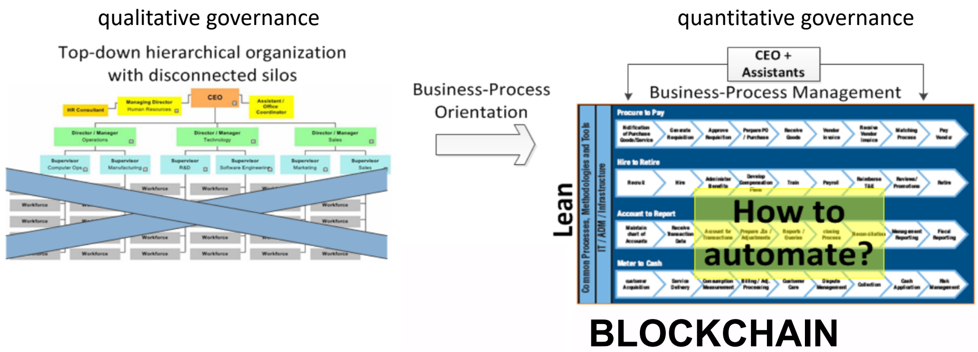
Benjamin Leiding
University of Göttingen,
Institute of Computer Science,
Göttingen, Germany
Email: benjamin.leiding@cs.uni-goettingen.de

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

BLOCKCHAIN TECHNOLOGY GROUP

MY OWN JOURNEY TO BLOCKCHAINS (SMART CONTRACTS)

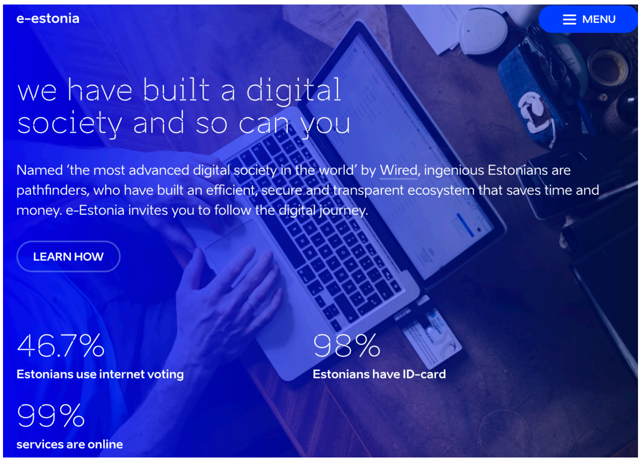
- My lesson learned:
- Inefficient and coercive pyramids rule society
  - governments, banks, corporations, NGOs, etc.
- Shift from master/slave to Peer-to-Peer (P2P)
  - qualitative governance with humans & fraud, crime, corruption, nepotism etc.
  - quantitative governance based on mathematics using blockchain technology



TAL TECH

BLOCKCHAIN TECHNOLOGY GROUP

ESTONIA HAS GREAT E-GOVERNANCE MODELS



- https://e-resident.gov.ee
- https://e-estonia.com/solutions/interoperability-services/x-road/
- https://www.techrepublic.com/article/how-estonia-became-an-e-government-powerhouse/
- https://www.youtube.com/watch?v=sh7W3kudseq&t=001s
- https://www.youtube.com/watch?v=9bYpk75JnZU&t=01s
- https://www.youtube.com/watch?v=EjYmpVwAjKU&t=01s
- https://www.youtube.com/watch?v=9IWpM9xtcyk
- HOWEVER!!! There is no blockchain in X-Road!

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

BLOCKCHAIN TECHNOLOGY GROUP

BASICS OF BLOCKCHAINS AND SMART CONTRACTS

BLOCKCHAIN TECHNOLOGY GROUP

ALT-COINS RISINFG

- Whitepaper of Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

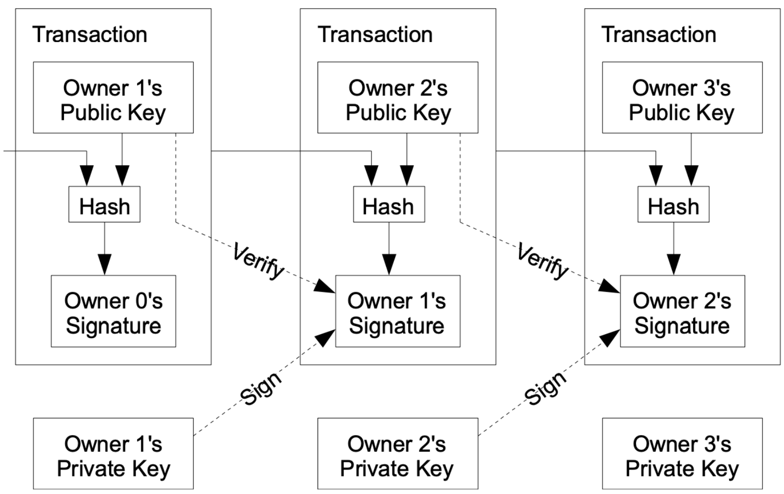
bitcoin

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

BLOCKCHAIN TECHNOLOGY GROUP

FIRST BLOCKCHAIN USECASE

- Whitepaper of Satoshi Nakamoto

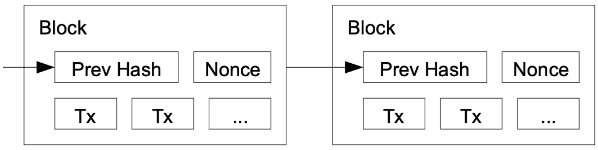


TAL TECH

FIRST BLOCKCHAIN USECASE

- Whitepaper of Satoshi Nakamoto

Proof-of-Work



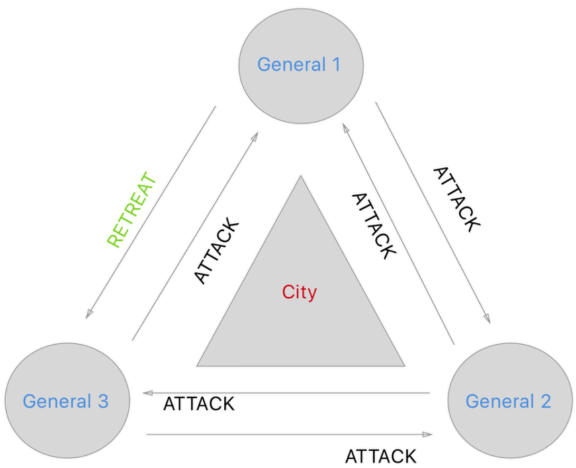
5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

BITCOIN AS FIRST BLOCKCHAIN USECASE

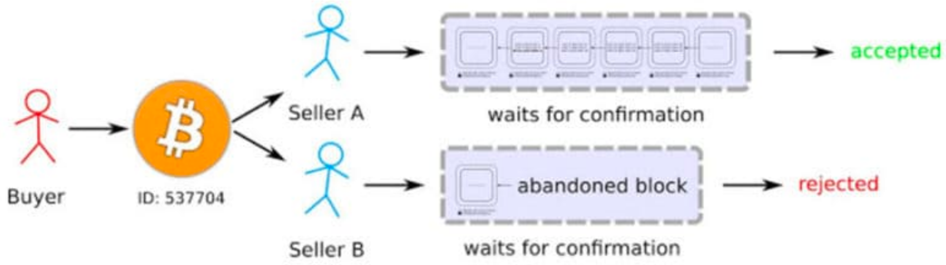
- What problems has the blockchain solved?
  – Byzantine general's problem



BLOCKCHAIN TECHNOLOGY GROUP

BITCOIN AS FIRST BLOCKCHAIN USECASE

- What problems has the blockchain solved?
  - Double spend problem

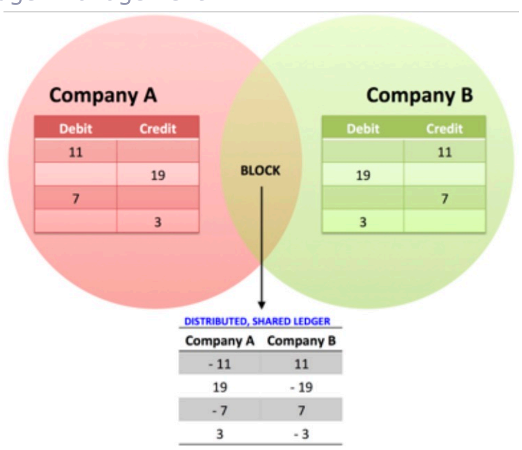


TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

BLOCKCHAIN TECHNOLOGY GROUP

BITCOIN AS FIRST BLOCKCHAIN USECASE

- What problems has the blockchain solved?
  - Triple entry ledger management



TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

BITCOIN AS FIRST BLOCKCHAIN USECASE

- Problems with bitcoins
  – long transaction times
  – block size is too small -> scalability problem
  – core developers have been usurped
  – high electricity consumption for PoW confirmation
  – high price volatility
- Lightning network tries to address long transaction time
  – "Layer 2" payment protocol that relies on the blockchain
  – bidirectional payment channels established between two participants
  – Lightning network for payment path establishment across network
  – blockchain as arbiter with unlimited off-blockchain transactions
  – >low cost, scalable, instant payments that are cross-blockchain atomic swaps

TALLINN UNIVERSITY OF TECHNOLOGY

SMART CONTRACT BASICS

- Ethereum as first smart-contract system

A Next-Generation Smart Contract and Decentralized Application Platform

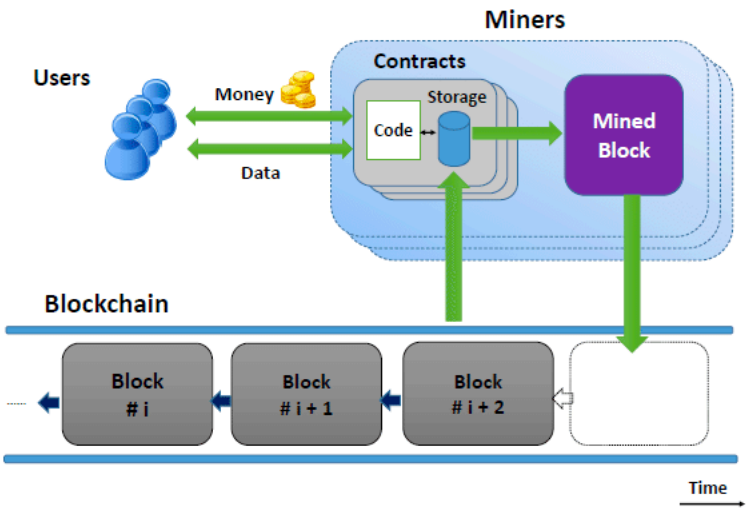
gitter Docs chat

> An introductory paper to Ethereum, introduced before launch, which is maintained.

Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or intrinsic value and no centralized issuer or controller. However, another - arguably more important - part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments (colored coins), the ownership of an underlying physical device (smart property), non-fungible assets such as domain names (Namecoin), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules (smart contracts) or even blockchain-based decentralized autonomous organizations (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

Contents

SMART CONTRACT BASICS



TAL TECH

SMART CONTRACT LANGUAGES (SCL)

SCL	Blockchain Plateforms	Pros	Cons
Solidity	Ethereum [96], Quorum [73] ,Wanchain [91] Rootstock [49], Cardano [43], Qtum [2] Dfinity [104], Soil, Monax, Ubiq	1.Turing Complete 2. Enjoys probably the biggest community of developers. 3. Most supported smart contract platform	1. Uses solidity, that is not as powerful as compared to today's languages such as C++, C, python, go etc 2. Can prove to be costly if the contract is not written efficiently.
Sophia	Aeternity [33]	1. Introduced new smart contract language and VMs for faster and safer code execution. 2. Using State channels and efficient ways to execute contracts keep the transaction prices low. 3. By providing a version of the EVM it is easy to migrate EVM contracts to Æternity	Keeping track of an implicit stack is generally error-prone and arguably not suitable for a high-level developer-facing language.
Serpent	Counterparty [33]	Real-time garbage collection: Squeak has a pretty fast generational scavenging collector, but Serpent does even better with a parallel mark-sweep garbage collector.	Being a low-level language, Serpent is not useful for building applications unless you have a hands-on experience.
F*	Zen [89]	As the smart contract language is "Dependently Typed", thus it is less prone to errors and is expressive enough to use it for 'FormalVerification'	Multiple transactions involving the same smart contract may not be easily parallelised, and may have to be executed in series.

TAL TECH

SMART CONTRACT LANGUAGES (SCL)

SCL	Blockchain Plateforms	Pros	Cons
RHOLang	RChain [95]	1. Turing Complete 2. Smart contracts enjoy a number of industry-leading functions such as: Meta-programming , Reactive Data Streams, Pattern Matching. As a result, RChain contracts have programmability	Rholang falls short in not adopting any syntax provisions for integrating business rules and policies.
RIDEON	Waves [11]	1. Rideon is a non Turing-complete smart contracts that covers the majority of the common use cases. 2. It has functionality of muli-signature.	1. Halting Problem 2. Termination at cost-calculation stage
GoLang	HyperLedger [6] Fabric	Highly modular platform that allows you to have high control over its performance, scalability and security.	As the contracts are deployed on peers (nodes) rather than on network, one has to deploy the contract code on every node(endorsers) on the network
Plutus	Cardano [43]	Heavily focused on making it easier to provide guarantees that a smart contract behaves as designed without hidden vulnerabilities.	Like Ethereum, IELE will use gas to limit resource usage and prevent DoS attacks. This presents some challenges to formal verification that are considered " tricky.
Michelson	Tezos [29]	Unlike Solidity, Michelson is not compiled to anything; it is a low level, stack-based, Turing-complete programming language that is directly interpreted by the Tezos virtual machine	It has a restricted type instructions. Michelson is not suitable to express contractual business business sementics because it has lack of vocabulary.

SECURING IDENTITY AUTHENTICATION

THE PAPER

Computers & Security
Volume 86, September 2019, Pages 253-269

Safeguarding a formalized Blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns

Alex Norta [a], Raimundas Matulevičius [b], Benjamin Leiding [c]

[a] Blockchain Technology Group, Tallinn University of Technology, 12618 Akadeemia tee 15A, Tallinn, Estonia
[b] Institute of Computer Science, University of Tartu, Tartu, J. Liivi 2, 50409, Estonia
[c] Institute of Computer Science, University of Göttingen, Göttingen, Goldschmidtstr. 7, 37077, Germany

Received 23 March 2018, Revised 15 April 2019, Accepted 24 May 2019, Available online

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

Abstract

Designing government independent and secure identification- and authentication protocols is a challenging task. Design flaws and missing specifications as well as security- and privacy issues of such protocols pose considerable user risks. Formal methods, such as Colored Petri Nets (CPN), are utilised for the design, development and analysis of such new protocols in order to detect flaws and mitigate identified security risks before deployment. This paper fills the gap, by applying in a novel way a set of security risk-oriented patterns (SRP) to the so-called Authcoin protocol that we formalise using CPN. The initial formal model of Authcoin facilitates the detection and elimination of design flaws, missing specifications as well as security- and privacy issues. The additional risk- and threat analysis based on the Information Systems Security Risk Management (ISSRM) domain model we perform on the formal CPN models of the protocol. The identified risks are mitigated by applying SRPs to the formal model of the Authcoin protocol. SRPs are a means to mitigate common security- and privacy risks in a business-process context by applying thoroughly tested and proven best-practice solutions. The goal of this work is to test the utility of SRPs outside of the the usual application domain, to reduce the risks and vulnerabilities of the Authcoin protocol.

EARLIER PAPER WITH BASIC AUTHCOIN PROTOCOL

Mapping Requirements Specifications into a Formalized Blockchain-Enabled Authentication Protocol for Secured Personal Identity Assurance

Benjamin Leiding[1] and Alex Norta[2]

[1] University of Göttingen, Institute of Computer Science, Göttingen, Germany
benjamin.leiding@cs.uni-goettingen.de
[2] Tallinn University of Technology, Department of Software Systems, Tallinn, Estonia
alex.norta.phd@ieee.org

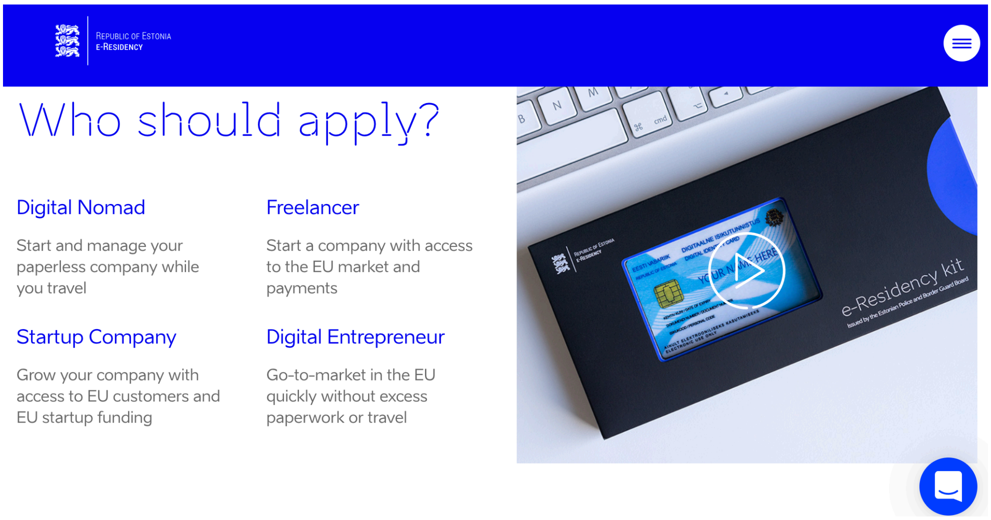
Abstract. The design and development of novel security and authentication protocols is a challenging task. Design flaws, security and privacy issues as well as incomplete specifications pose risks for its users. Authcoin is a blockchain-based validation and authentication protocol for secure identity assurance. Formal methods, such as Colored Petri Nets (CPNs), are suitable to design, develop and analyze such new protocols in order to detect flaws and mitigate identified security risks. In this work, the Authcoin protocol is formalized using Colored Petri Nets resulting in a verifiable CPN model. An Agent-Oriented Modeling (AOM) methodology is used to create goal models and corresponding behavior models. Next, these models are used to derive the Authcoin CPN models. The modeling strategy as well as the required protocol semantics are explained in detail. Furthermore, we conduct a state-space analysis on the resulting CPN model and derive specific model properties. The result is a complete and correct formal specification that is used to guide future implementations of Authcoin.

Keywords: authcoin, colored petri net, authentication, security, trust, privacy, access control, identity, blockchain, smart contract, formal verification

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

INTRODUCTION

- Government ID-systems are dangerous
  - Citizens can be switched off, e.g., Chinese social-credit score



TAL TECH

INTRODUCTION

- Blockchain-based private ID-systems
  - Do not consider authentication

TAL TECH
TALLINN UNIVERSITY OF TECHNOLOGY

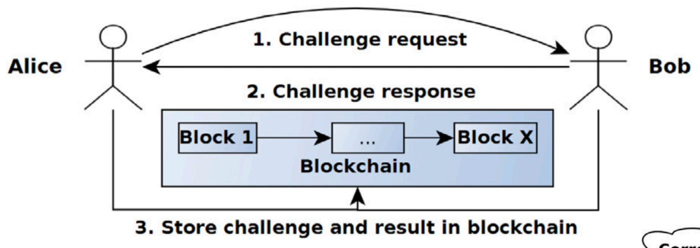
INTRODUCTION

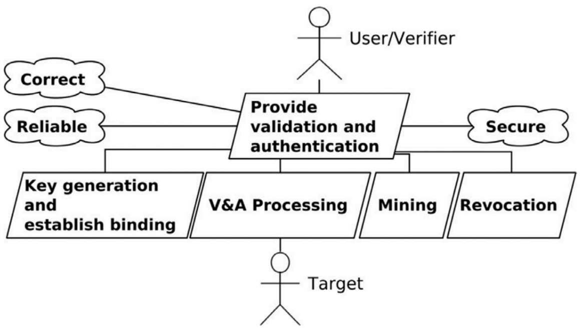
- Securing such a non-governmental ID-Auth protocol is a challenge
  - Beyond technical means of securing
  - Requires a unique socio-technical approach
  - Security risk-oriented patterns (SRP) for BPM fortification
- Research questions
  - Main RQ: How to analyse security threats of the identity authenticating Authcoin protocol (running case) by applying in a novel way SRPs?
  - Sub RQ1: What assets and data object in the Authcoin protocol are under risk threats?
  - Sub RQ2: What existing security risk-oriented patterns are applicable for generating an improved Authcoin protocol model?
  - Sub RQ3: What modification of the existing Authcoin models are required to implement the chosen security risk-oriented patterns?
- Thus, we "stress test" SRPs outside of the typical BPM application domain.

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

AUTHCOIN: CONCEPTUAL PRESENTATION

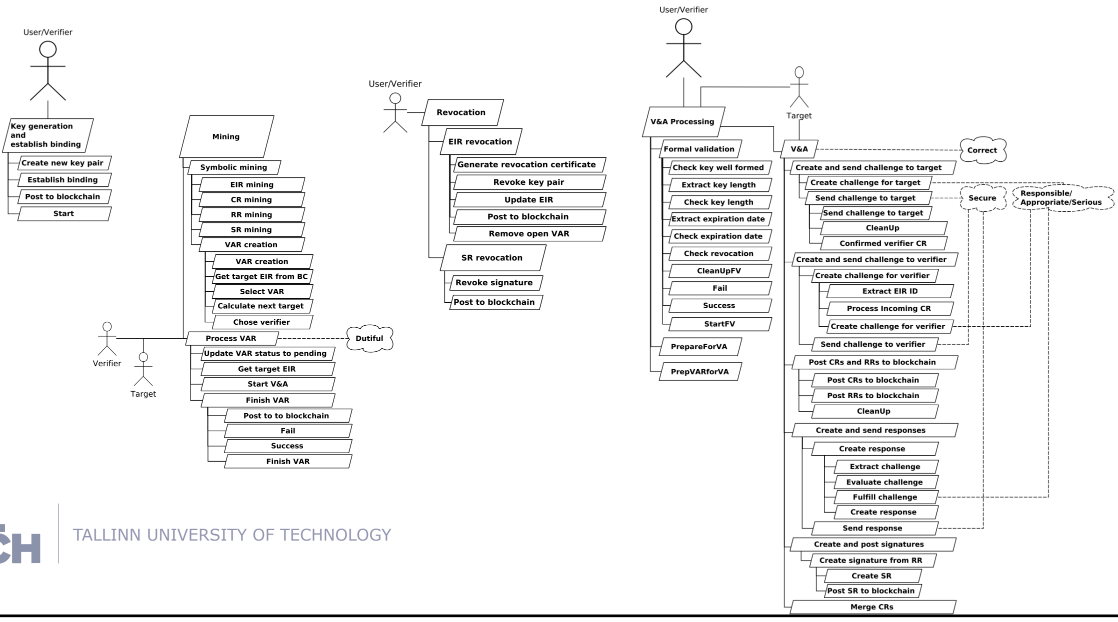
- Authcoin addresses this issue
  - gitHUB: https://github.com/bleidingGOE/Authcoin-Qtum





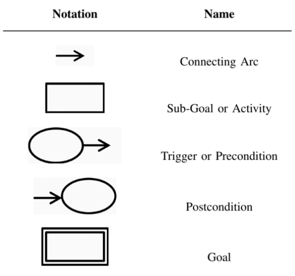
TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

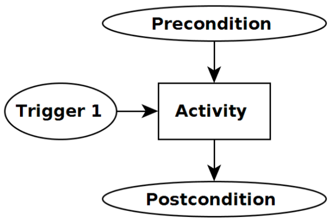
GOAL MODEL REFINEMENTS

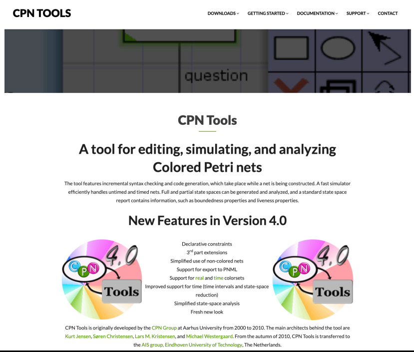


TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

MAPPING FROM GOAL MODELS TO COLORED PETRI NETS (CPN)



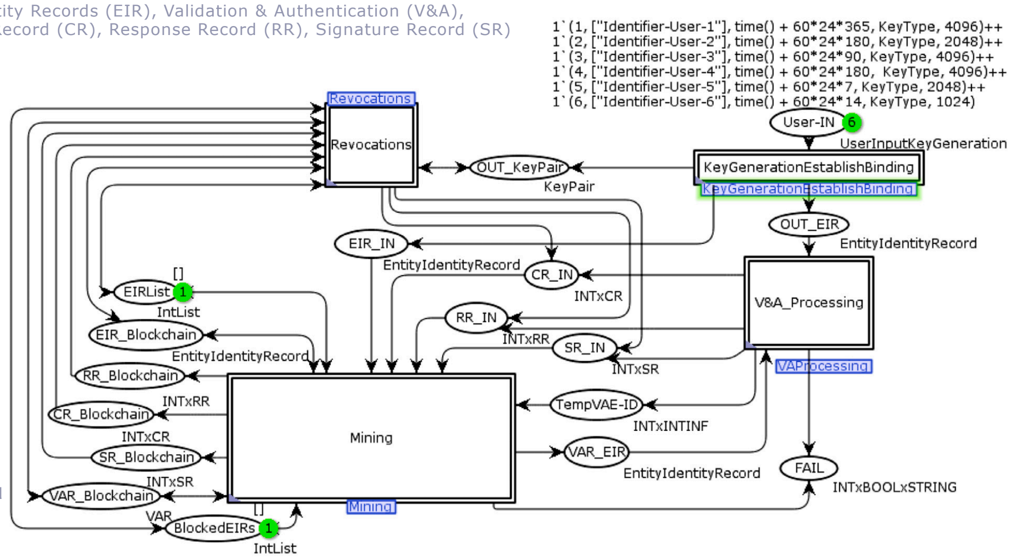




TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

AUTHCOIN: FORMAL PRESENTATION WITH COLORED PETRI NETS

- Top-level Authcoin CPN model
  - Entity Identity Records (EIR), Validation & Authentication (V&A), Challenge Record (CR), Response Record (RR), Signature Record (SR)



AUTHCOIN: FORMAL PRESENTATION WITH COLORED PETRI NETS

- Exemplary Authcoin behavioral interfaces of activities

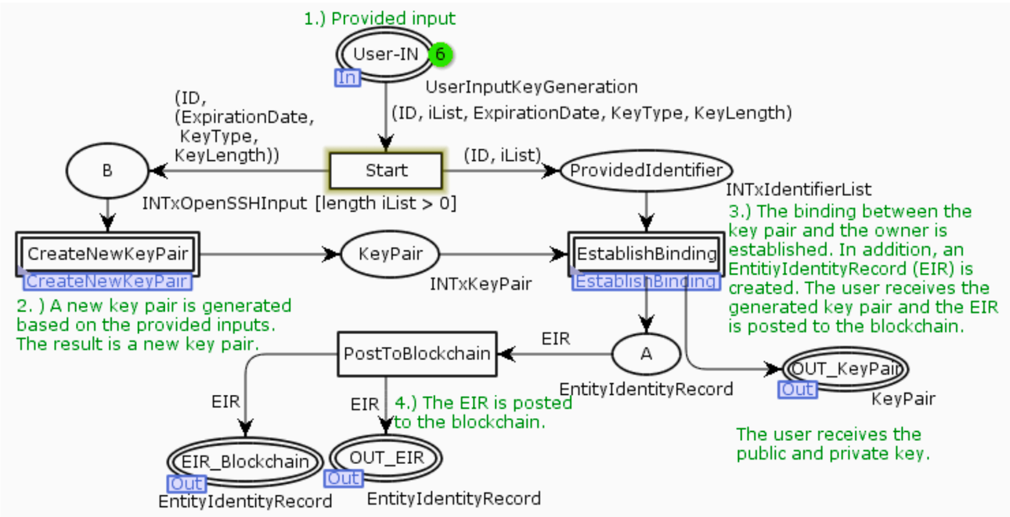
Activity	Trigger	Precondition	Postcondition
Key generation and establish binding	User wants to create a new key pair	identifier list, expiration date, key type, key length	Key pair, EIR on blockchain EIR
V&R Processing	Received EIRs for V&A	Verifier EIR, target EIR	V&A results on blockchain or failure message
Mining	Received input for blockchain	Input transactions	CR, RR and SR on blockchain and VARs or failure message
Revocation	User wants to revoke an EIR or a SR	KeyPair, EIR, SR, CR,RR, VARs	Revoked EIR or SR and updated information on blockchain

- Acronyms, names, descriptions of token colors

Module	Token color	Description	Type
Top Level	PublicKey	Public Key	(Key Finger print, Key, Expiration Date UTC, Key Type,Key Length)
Top Level	PrivateKey	Private Key	String
Top Level	ChallengeRecord	Contains all information of a V&A challenge	(CR_ID,VAE_ID,Time stamp, Challengetype,Challenge, VerifierEIR_ID, Verification TargetEIR_ID)
Top Level	ResponseRecord	Contains all information regarding a V&A response	(RR_ID,VAE_ID, Timestamp, CorrespondCR_ID, Response)

REFINMENTS OF FORMAL CPN MODULES

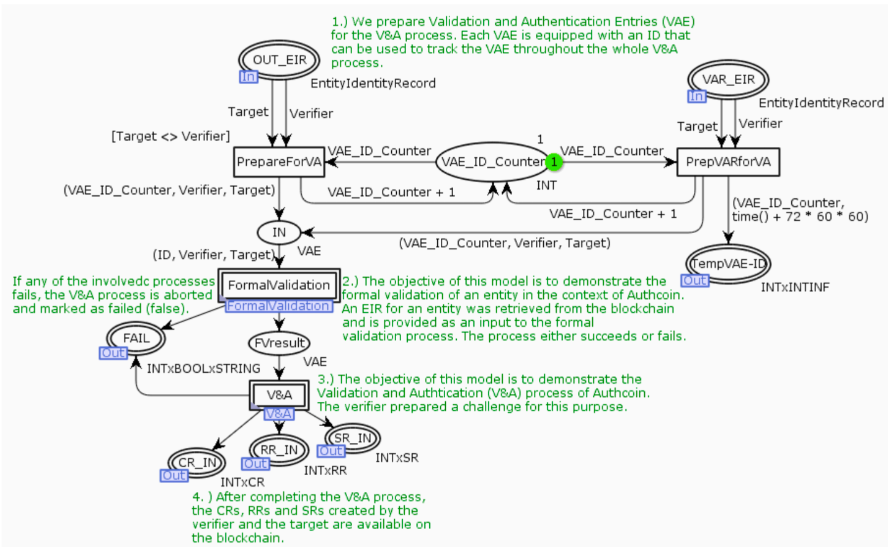
- CPN model of the "KeyGenerationEstablishBinding" module



TAL TECH

REFINMENTS OF FORMAL CPN MODULES

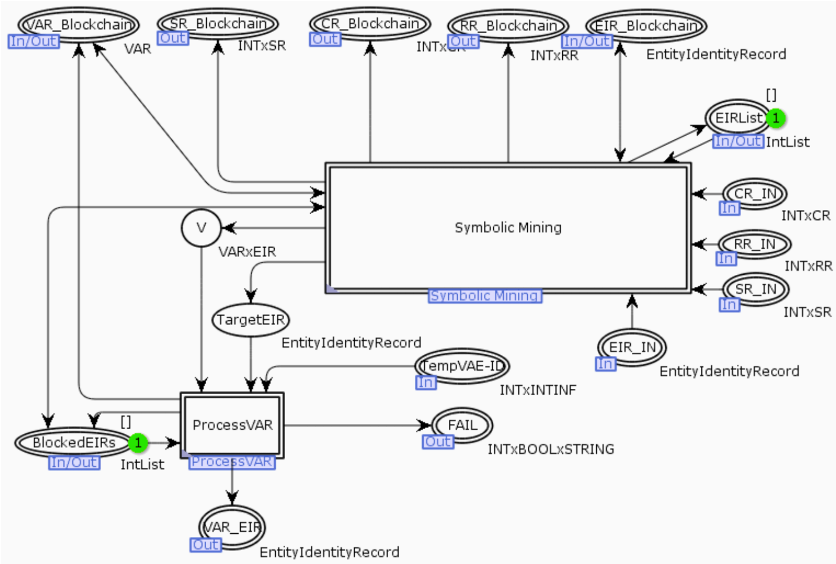
- CPN model of the "V&A-Processing" module



TAL TECH

REFINMENTS OF FORMAL CPN MODULES

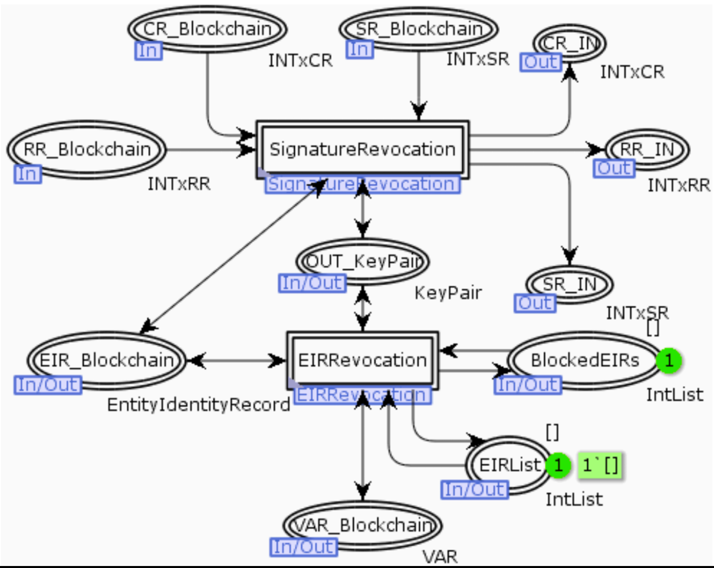
- CPN model of the "Mining" module



TAL TECH

REFINMENTS OF FORMAL CPN MODULES

- CPN model of the "Revocations" module



TAL TECH

STATE-SPACE ANALYSIS

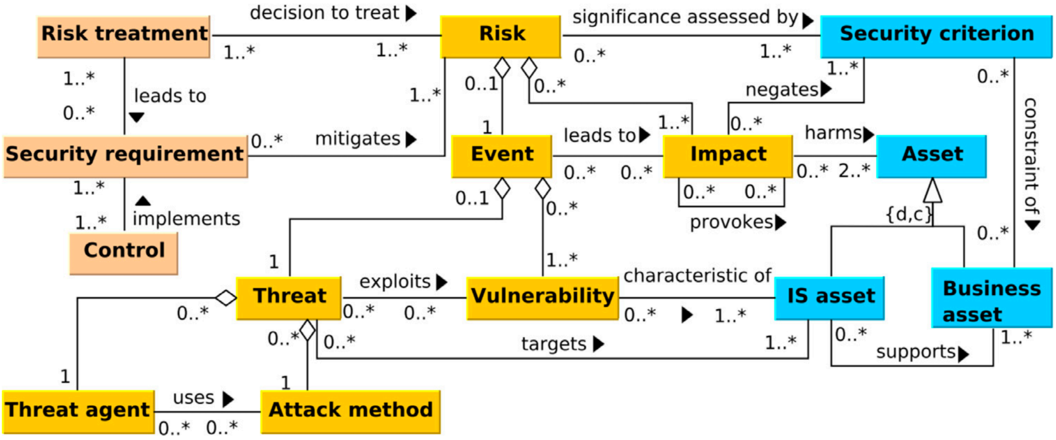
- Partial state-space analysis per module by CPN tools algorithms
- Simulation by token game of entire Authcoin protocol

Module	Loops	Home markings	Dead markings	Dead transitions	Live transitions
Key Generation Establish Binding	No	No	Yes	No	No
Formal Validation	No	No	Yes	Yes	No
Validation & Authentication	No	No	Yes	Yes	No
VAR Creation	No	No	Yes	No	No
Process VAR	No	No	Yes	Yes	No
Revocations	No	No	Yes	Yes	No

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

DOMAIN MODEL FOR SECURITY RISK MANAGEMENT

- Information Systems Security Risk Management (ISSRM) model



TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

SRP: SECURITY RISK-ORIENTED PATTERNS (SORT OF PATTERNS 😊)

- SRP1: secures data from unauthorized access
  - Data confidentiality in business services
  - Risk reduction: access-right checks with sensitivity levels
- SRP2: ensures secure data transmission between business entities
  - Data confidentiality and integrity
  - Interception by attacker during data transmission possible
- SRP3: ensures secure business activity after data submission
  - Availability and integrity of business activities
  - Filtering of incoming data
- SRP4: secures business services against distributed denial of service (DDoS) attacks
  - Availability of data essential
  - Detection of abnormal requests
- SRP5: secures storage of data and data retrieval from storage
  - Confidentiality of data storage due to malicious insider threat
  - Data invisibility, storage monitoring and -controlling

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

RISK 1 AND THREAT ANALYSIS FOR POSTING EIRS, CRS, RRS, SRS AND UPDATED VARS TO THE BLOCKCHAIN

	Risk 1	
	Man-in-the-middle (MITM) outside attacker	
	Motivation:	Undermine trustworthiness and reliability of the protocol
Threat Agent	Resources:	Intercept information posted from genuine user to the blockchain
	Expertise:	Intercept and manipulate transmitted data records
Attack Method	1	Outside attacker intercepts data records (EIR, CR, RR, SR, or VAR) that have been created and posted to the by a genuine user. blockchain or VAR) that have been created and posted to the blockchain
	2	Outside attacker manipulates data records.
	3	Outside attacker forwards manipulated data records to intended receiver (blockchain miners).
Threat	Outside attacker manipulates data records.	
Vulnerability	Data records transmitted during the process of posting information to the blockchain can be manipulated.	
Event	Outside attacker manipulates transmitted data records and forwards the false records to be posted to the blockchain due to a lack of integrity checks of transmitted data records.	
Impact	1	Data records with false information available on the blockchain.
	2	Loss of integrity of transmitted data records.
Risk	Outside attacker manipulates transmitted data records and forwards the false records to be posted to the blockchain due to a lack of integrity checks of transmitted data records.	

TAL TECH

RISK 2 AND THREAT ANALYSIS FOR SENDING AND RECEIVING CRS AND RRS

	Risk 2	
Threat Agent	MITM outside attacker Motivation: Resources: Expertise:	 Undermine trustworthiness and reliability of the protocol Intercept user traffic Intercept and manipulate transmitted data records
Attack Method	1	Outside attacker intercepts data records (EIR, CR, RR, SR, or VAR) that have been created and posted to the by a genuine user. blockchain or VAR) that have been created and posted to the blockchain
	2	Outside attacker manipulates data records.
	3	Outside attacker forwards manipulated data records to intended receiver (blockchain miners).
Threat	Outside attacker manipulates data records.	
Vulnerability	Data records transmitted during the process of posting information to the blockchain can be manipulated.	
Event	Outside attacker manipulates transmitted data records and forwards the false records to be posted to the blockchain due to a lack of integrity checks of transmitted data records.	
Impact	1	Data records with false information available on the blockchain.
	2	Loss of integrity of transmitted data records.
Risk	Outside attacker manipulates transmitted data records and forwards the false records to be posted to the blockchain due to a lack of integrity checks of transmitted data records.	

RISK 3 AND THREAT ANALYSIS OF A DDOS ATTACK

	Risk 3	
Threat Agent	Outside attacker Motivation: Resources: Expertise:	 Disrupt Authcoin services DDoS network with sufficient power Running DDoS attacks
Attack Method	1	Outside attacker performs a DDoS attack on network infrastructures relevant for user communication - either for a specific local user or on a global scale.
	2	Users are no longer able to exchange data records (CR, RR) or access Authcoin information on the blockchain.
Threat	Outside attacker performs a DDoS attack on the network infrastructure.	
Vulnerability	Network infrastructure can be overloaded by an outside attacker.	
Event	Outside attacker is able to perform a DDoS attack on the network Infrastructure.	
	1	Pending V&As might time out.
Impact	2	Users are not able to perform any new or pending V&A procedures.
	3	No information lookup on the global blockchain.
	4	General unavailability of Authcoin services.
Risk	Outside attacker performs a DDoS attack on the local or global network infrastructure used by Authcoin's users resulting in a general unavailability of the service. Furthermore pending V&As might time out and users cannot execute any operation of the protocol anymore.	

TREATMENT OF RISK

	Risk 1 & 2	Risk 3
Risk treatment	Risk reduction	Risk reduction
Security requirement	Integrity checks of submitted records	Mitigate service disruption
Controls	Signed hashes	Decentralization, load distribution and balancing

- Identifying these risks and mitigations does not guarantee other risks and security flaws in the protocol exist.
- Further risk-analysis method & penetration testing may show further risks.
- Examples of further risks
  - User mobile devices
  - Underlying communication networks
  - Blockchain systems used

TALLINN UNIVERSITY OF TECHNOLOGY

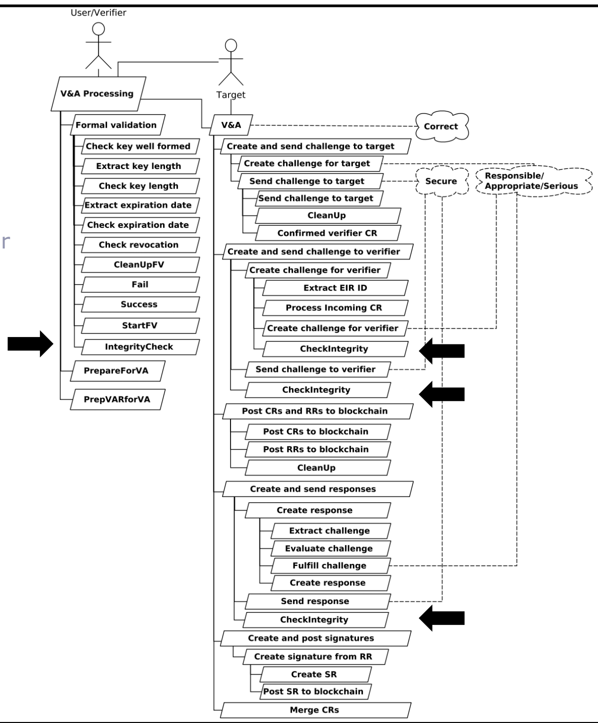
APPLYING SECURITY RISK-ORIENTED PATTERNS (SRP)

- SRP1: secures data from unauthorized access
  - Does not correspond to any identified risk
  - Not considered to be implemented
- SRP2: ensures secure data transmission between business entities
  - Suitable to mitigate issued of Risk 1 & Risk 2
  - Make data unreadable before transmission & hash checksums for outside-attack prevention
- SRP3: ensures secure business activity after data submission
  - Does not correspond to any identified risk
  - CPN modeling realizes this pattern
- SRP4: secures business services against distributed denial of service (DDoS) attacks
  - Authcoin is highly distributed service for DDoS protection
  - Partial DDoS attack against single service possible
- SRP5: secures storage of data and data retrieval from storage
  - Does not correspond to any identified risk
  - Not considered to be implemented

TALLINN UNIVERSITY OF TECHNOLOGY

UPDATED GOAL MODEL

- Four integrity-check subgoals added
  - IntegrityCheck under Formal validation
  - CheckIntegrity under CreateChallengeForVerifier
  - CheckIntegrity under CreateSendChallengeToVerifier
  - CheckIntegrity under CreateSendResponse



TALTECH | TALLINN UNIVERSITY OF TECHNOLOGY

UPDATED BEHAVIOR-INTERFACE MODEL (1)

Subgoal	Activity	Trigger	Precondition	Postcondition
Formal validation	Check key well formed	Started formal validation	VAE-ID, EIR	Key well formed result, public key, revocation information
	Integrity check	Key is well formed	VAE-ID, EIR	VAE-ID, result of integrity check based on hash sum
Validation and authentication	Create and send responses	Received incoming CR VAE-ID, verifier and target CR as well as EIRs	VAE-ID, target and verifier RRs as well as EIRs or failure message	
Create and send challenge to verifier	Received challenge from verifier VAE-ID, verifier EIR, target EIR, incoming CR Verifier and target CRs as well as EIRs, or failure message Create and post signatures	Received incoming RRs, CRs and RR posted to blockchain	VAE-ID, verifier and target RRs, verifier and target EIRs	SRs available on blockchain, validation and authentication finished
Create and send challenge to verifier	Create challenge for verifier	Target received challenge from verifier	VAE-ID, target CR, verifier and target EIR	VAE-ID, verifier CR, target challenge, verifier and target EIR
Check integrity	Original verifier receives CR from target	VAE-ID, verifier CR, target CR, verifier and target EIR	VAE-ID, verifier CR, target challenge, verifier and target EIR	
Create signatures from RR	Create Signature	Received a RR	VAE-ID, RR, signature lifespan, response evaluation, verifier and target EIRs	VAE-ID, SR

TALTECH

UPDATED BEHAVIOR-INTERFACE MODEL (2)

Subgoal	Activity	Trigger	Precondition	Postcondition
	Check integrity	Received CR from verifier	VAE-ID, CR for target, verifier EIR	VAE-ID, target CR, verifier EIR
	Extract EIR-ID	CR passed integrity check	VAE-ID, CR for target, verifier EIR	VAE-ID, target CR, verifier EIR-ID, verifier EIR
Create challenge for verifier	Process incoming CR	Extracted verifier EIR-ID	VAE-ID, verifier EIR, verifier EIR-ID	VAE-ID, Verifier EIR
	Create challenge for verifier	Processed incoming CR	VAE-ID, verifier and target EIRs, challenge for verifier	VAE-ID, CR for verifier, verifier and target EIRs
	Create response	Verifier and target CRs received	VAE-ID, verifier and target CRs as well as EIRs	VAE-ID and RR and EIRs or failure message
Create and send response	Send response	Created response for CR	VAE-ID,RR	VAE-ID,RR
	Check integrity	User receives a RR	VAE-ID, RR, verifier and target EIR	VAE-ID,RR, verifier and target EIR or failure message
Create response	Evaluate challenge	Extracted challenge from CR	VAE-ID, CR, challenge, challenge evaluation, verifier and target EIRs	VAE-ID, CR and evaluation result, verifier and target EIRs or failure message
	Create response	User fulfilled challenge	VAE-ID, CR, fulfilled challenge, verifier and target EIRs	VAE-ID, RR, verifier and target EIRs
Create and post signature	Create signature from RR	Received RRs	VAE-ID, RRs, verifier and target EIRs	SRs available on blockchain

TAL TECH

UPDATED PROTOCOL SEMANTICS

Token color	Description	Type
EntityIdentityRecord	Contains all relevant information about an entity	EIR_ID, Timestamp, PublicKey, Identifiers, Revoked, hashEIR, EIRsig
ChallengeRecord	Contains all information about a V&A challenge	CR_ID, VAE_ID, Timestamp, ChallengeType, Challenge, VerifierEIR_ID, VerificationTargetEIR_ID, hashCR, CR sig
ResponseRecord	Contains all information regarding a V&A response	RR_ID, VAE_ID, Timestamp, CorrespondCR_ID, Response, hashRR, RRsig, RR receiver, RRSender
SignatureRecord	Contains all information regarding a V&A signature	SR_ID, VAE_ID, Timestamp, ResponseRR ID, ExpirationDate, Revoked, SuccessfulVA, hashSR, SR sig
VAR	Validation and authentication request	VAR_ID, CreationDate, LastUpdated, VerifierEIR_ID, TargetEIR_ID, Status, VAE_ID, hashVAR, VARsig

TAL TECH TALLINN UNIVERSITY OF TECHNOLOGY

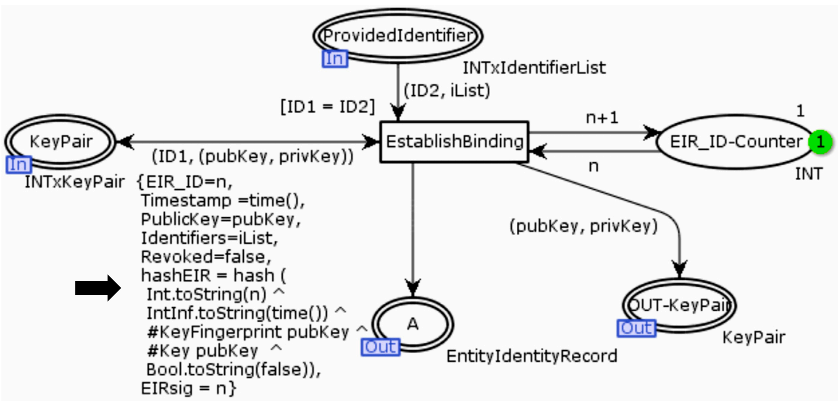
UPDATED OF CPN MODULES WITH DETAILED DESCRIPTION

CPN-Module name	Update description
KeyGenerationEstablishBinding	Added a hash calculation for created EIRs
FormalValidation	Added a hash-based *IntegrityCheck* and updated affected transitions accordingly
V&A	Added a new place *VT_EIRs* to accommodate EIRs required to create and verify signatures on data records
CreateSendChallengeToVerifier	Added a hash-based *IntegrityCheck* and updated connecting arcs accordingly
CreateSendResponses	Added a hash-based *IntegrityCheck* and updated connecting arcs accordingly
CreateSignatures	Added a new place *VTSR_EIRs* to accommodate EIRs required to create and verify signatures on data records
CreateChallengeForTarget	Added a hash calculation for created CRs
CreateChallengeForVerifier	Added a hash-based *IntegrityCheck* for incoming CRS and updated connecting arcs accordingly
CreateResponse	Added a hash calculation for created RRs
CreateSignaturesFromR	Added calculation of a hash-based checksum for each created SR
VARCreation	Added a hash calculation for created VARs
ProcessVAR	Added a hash calculation for created VARs
FinishVAR	Added a hash calculation for created VARs
EIRRevocation	Added calculation of a hash-based checksum for updated and revoked EIRs
SignatureRevocation	Added calculation of a hash-based checksum for updated and revoked SRs

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

UPDATED CPN MODEL OF THE ESTABLISHBINDING MODULE

- Added a hash calculations for created EIRs
- Other CPN module updates in the publications



TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

LESSONS LEARNED FROM SRP APPLICATION TO CPN

- First time application of SRPs to CPN models
- If CPN models complex then SRP integration and implementation is time consuming
- CPN model updating with many sub-models requires good comprehension of domain and system
- Manual SRP detection poses risk of missing occurrences
- Automated pattern detection is future work
- CPN/Access for interfacing with complex hash functions from other languages, e.g., Java
- Modeling to external systems is currently symbolic
  – SRP application limitation
- Authcoin designed already with security in mind

TAL TECH TALLINN UNIVERSITY OF TECHNOLOGY

EVALUATION OF UPDATED CMP MODEL WITH SRP PATTERNS

- Second state space is the same as for the first state space

Module	Loops	Home markings	Dead markings	Dead transition	Live transition
Key Generation Establish Binding	No	No	Yes*	No	No
Formal Validation	No	No	Yes*	Yes*	No
Validation & Authentication	No	No	Yes*	Yes*	No
VAR Creation	No	No	Yes*	No	No
Process VAR	No	No	Yes*	Yes*	No
Revocations	No	No	Yes*	Yes*	No

- State-space complexity comparison of both models based on nodes and arcs

Module	Nodes*	Arcs*	Nodes**	Arcs**
Key Generation Establish Binding	466	772	466	772
Formal Validation	708	2523	2877	13,588
Validation & Authentication	308	601	372	830
VAR Creation	355	911	373	971
Process VAR	2502	6288	6067	21,884
Revocations	13	12	13	12

TAL TECH TALLINN UNIVERSITY OF TECHNOLOGY

CONCLUSION

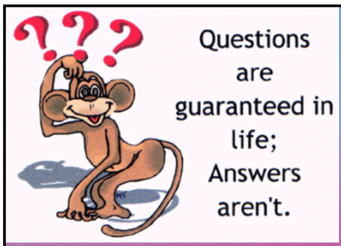
- Blockchains have massive socio-technical implications
  - Abolishment of qualitative, human-driven governance
  - Replacement with quantitative, mathematics-rooted e-governance
- Blockchain technology solves several problems
  - Byzantine general's problem solved
  - Double-spend problem solved
  - Triple-entry ledger management possible
- Smart contracts are currently neither contracts, nor smart
- We secure a government-independent identity-authentication protocol
  - Blockchain-based, currently in implementation with Qtum.org
  - Security risk-oriented pattern application for securing protocol
  - We show patterns are partially applicable onto CPN models
  - Updated goal models and CPN models as consequence

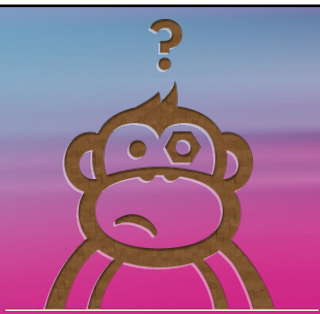
TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY

FUTURE WORK

- Automatic detection of security risk-oriented patterns
- Properly specify security risk-oriented patterns
- Implement Authcoin with different smart-contract systems
  - Currently we try Qtum.org
- Authcoin application in diverse cases
  - E-governance
  - B2B Dapps
  - Cyberphysical systems
  - Automobile industry
  - Etc.

TAL TECH | TALLINN UNIVERSITY OF TECHNOLOGY





BLOCKCHAIN TECHNOLOGY GROUP

TAL TECH

Thank you very much for your attention!

Q & A?

TALLINN UNIVERSITY OF TECHNOLOGY

blockchain.taltech.ee

IEEE BLOCKCHAIN™