Cryptoseminar project proposals

Fall 2017
Michal Zajac
michal.zajac@ut.ee
Bitcoin
What is bitcoin?

- Bitcoin is a **crypto currency**
  - **crypto** since it uses cryptographic means to assure security of transactions and assets
  - **currency** since you can use it to pay for goods
Bitcoin transactions are public

t1: Alice has 4B, Bob has 2B
Bitcoin transactions are public.

I, Alice, pay Bob 2B.

t1: Alice has 4B, Bob has 2B.
Bitcoin transactions are public

I, Alice, pay Bob 2B

t1: Alice has 4B, Bob has 2B
Bitcoin transactions are public

I, Alice, pay Bob 2B

t1: Alice has 4B, Bob has 2B

Alice pays Bob 2B

Alice has 2B, Bob has 4B
What if?
What if?

I, Alice, pay Bob 2B
What if?

I, Alice, pay Bob 2B
I, Alice, pay John 3B
What if?

I, Alice, pay Bob 2B
I, Alice, pay John 3B
I, Alice, pay Barbara 4B
What if?

I, Alice, pay Bob 2B
I, Alice, pay John 3B
I, Alice, pay Barbara 4B

All transactions seem legal (Alice does not spend more she had at the beginning), yet sth. is not ok
Easy solution

I, Alice, pay Bob 2B  
\[ \text{time} = 00436180432 \]

I, Alice, pay John 3B  
\[ \text{time} = 00543288742 \]

I, Alice, pay Barbara 4B  
\[ \text{time} = 00754324485 \]
Easy solution

I, Alice, pay Bob 2B  
\[ \text{time} = 00436180432 \]  
\[ \text{Alice has 4B - OK} \]

I, Alice, pay John 3B  
\[ \text{time} = 00543288742 \]  
\[ \text{Alice has 2B - ERROR} \]

I, Alice, pay Barbara 4B  
\[ \text{time} = 00754324485 \]  
\[ \text{Alice has 2B - ERROR} \]
Easy solution

I, Alice, pay Bob 2B  
	time = 00436180432  
	Alice has 4B - OK

I, Alice, pay John 3B  
	time = 00543288742  
	Alice has 2B - ERROR

I, Alice, pay Barbara 4B  
	time = 00754324485  
	Alice has 2B - ERROR

The key idea of bitcoin is decentralisation
Easy solution

I, Alice, pay Bob 2B  
I, Alice, pay John 3B  
I, Alice, pay Barbara 4B

time = 00436180432  
Alice has 4B - OK

time = 00543288742  
Alice has 2B - ERROR

time = 00754324485  
Alice has 2B - ERROR

The key idea of bitcoin is **decentralisation**
There is **no timeserver** to track the **order** of transactions
Transactions are gathered into blocks

I, Marvin, pay Bob 1B
I, Vitaly, pay Jose 0,5B
I, Mo, pay Ahmed 7B
I, Bingsheng, pay Helger 3B
Transactions are gathered into blocks

l, Marvin, pay Bob 1B
l, Vitaly, pay Jose 0,5B
l, Alice, pay Bob 2B
l, Mo, pay Ahmed 7B
l, Bingsheng, pay Helger 3B

\[ \text{time} = \ldots \]
Transactions are gathered into blocks

- l, Marvin, pay Bob 1B
- l, Vitaly, pay Jose 0.5B
- l, Alice, pay Bob 2B
- l, Mo, pay Ahmed 7B
- l, Bingsheng, pay Helger 3B

After some time, blocks are confirmed.

New transactions can be gathered to a new block.
Why block confirmation matters?

- No central server - confirmed blocks create **blockchain** that determines the order of transaction.
- **Only** after a block is confirmed receiver can be sure she will get her money.
- Block confirmation is the **only** way to **produce new bitcoins**.
- Party who confirms the block **gets reward**.
How to confirm a block?

- **Proof-of-work**
  - parties have a **puzzle** to solve
  - puzzle needs a lot of **computational power**
  - solving puzzle is a waste of energy — (huge) computation performed have no other utilisation than confirming a block

- **Proof-of-stake**
  - Party to confirm is picked randomly among the parties participating in transactions included in a block
  - Probability that a party is chosen to confirm a block (and gain reward) is proportional to the stake of that party.

- **Proof-of-space**
  - Instead of showing that parties can perform huge computations, parties show they have a big storage space.
Projects

- **Project 1:** *Proof-of-work* needs carefully designed puzzle to solve. In this project the participant needs to read, understand and present a paper that shows how securely pick a puzzle. (paper provided)

- **Project 2:** *Proof-of-stake* is a new concept introduced this year at Crypto conference. In this project the participant needs to read, understand and present a paper introducing this concept. (paper provided)

- **Project 3:** *Proof-of-space* is a fairly new concept also (2Y old). In this project the participant needs to read, understand and present a paper introducing this concept. (paper provided)

- **Project 4:** Since block confirmation takes some time, the original bitcoin scheme is not very useful for everyday shopping. In this project participant needs to read, understand and present a paper that proposes a workaround for this obstacle. (paper provided)
SNARGs
Succinct Non-Interactive Arguments
Zero knowledge

- Let Alice know that some statement is true and she has a proof for it.
- E.g. she proved $P \neq NP$.
- She does not want to share the proof of the theorem, but she wants to convince Bob that she really has it.

There are protocols that allows Alice to produce an argument $\pi$ such that
- Bob can verify $\pi$ and if it is correct, he knows that Alice in fact has a proof for $P \neq NP$
- Bob, seeing $\pi$ has no clue about how the proof goes
- Alice cannot convince Bob that she has a proof if that is not true
- If $\pi$ is short we call it succinct
- It is important $\pi$ to be succinct to be efficient
Zero knowledge

- Let $L$ be an NP language
- Say that Alice knows that $x \in L$
- but she does not want to reveal the witness $w$

There are protocols that allows Alice to produce an argument $\pi$ such that

- Bob can verify $\pi$ and if it is correct, he knows that $x \in L$
- Bob, seeing $\pi$ has no clue about witness $w$
- Alice cannot convince Bob that $x' \in L$ if that does not hold
- If $\pi$ is short we call it succinct
- It is important $\pi$ to be succinct to be efficient
Falsifiable assumption

**Assumption is falsifiable** if it is possible to conceive of an observation or an argument which could negate it.

For example, the universal generalisation that **All swans are white** is falsifiable since it is logically possible to falsify it by observing a single black swan. Thus, the term *falsifiability* is sometimes synonymous to *testability*.

source: https://en.wikipedia.org/wiki/Falsifiability
Bad news

It is not possible to build a SNARG from falsifiable assumptions
Bad news

It is not possible to build a SNARG from falsifiable assumptions

**Project 5**: Read, understand and present the paper that provides this negative, yet important result. (paper provided)
Thank you

michal.zajac@ut.ee