nedelja informatike 3

Napredne tehnike kriptografije

Stefan Crnojević

Matematički fakultet
Nedelja informatike 3

15. decembar 2016.

Uvod

Pregled prezentacije

- **Uvod**
- Zajedničko računanje

Pauza

- Kriptovalute (Bitcoin)
- **Reference**

Uvod

Predznanje

- Simetrična kriptografija (sigurni kanal)
- Asimetrična kriptografija (RSA)
- Kriptografske jednosmerne heš funkcije

Uvod

Predznanje

- Simetrična kriptografija (sigurni kanal)
- Asimetrična kriptografija (RSA)
- Kriptografske jednosmerne heš funkcije
- **Protokol nesvesnog prenosa**

Uvod

Nesvestan prenos

en.: *Oblivious transfer*

Problem: Alisa ima dve vrednosti, W_0 i W_1. Kako Bob da sazna **jednu** od tih vrednosti (njegov izbor) a da **Alisa ne zna koju**?

Uvod

Nesvestan prenos

en.: *Oblivious transfer*
Problem: Alisa ima dve vrednosti, W_0 i W_1. Kako Bob da sazna **jednu** od tih vrednosti (njegov izbor) a da **Alisa ne zna koju**?

Zašto bi ovo ikad ikome trebalo? (Saznaćemo - za sada vežbamo vijuge)

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	**Eva**	**Bob**
W_0, W_1	n, d_b	e_b, c

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	**Eva**	**Bob**
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	**Eva**	**Bob**
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	Eva	Bob
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	
		$v = x_b + r^{e_b} \mod n$

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	Eva	Bob
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$(x_0, x_1) \longrightarrow$	
		$v = x_b + r^{e_b} \mod n$
	$\longleftarrow v$	

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	Eva	Bob
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	
		$v = x_b + r^{e_b} \mod n$
	$\xleftarrow{v}$	
$k_0 = (v - x_0)^{d_b}, k_1 = (v - x_1)^{d_b}$		

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	Eva	Bob
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	
		$v = x_b + r^{e_b} \mod n$
	$\xleftarrow{v}$	
$k_0 = (v - x_0)^{d_b}, k_1 = (v - x_1)^{d_b}$		
$W_0' = W_0 + k_0, W_1' + k_1$		

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	Eva	Bob
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	
		$v = x_b + r^{e_b} \mod n$
	$\xleftarrow{v}$	
$k_0 = (v - x_0)^{d_b}, k_1 = (v - x_1)^{d_b}$		
$W_0' = W_0 + k_0, W_1' + k_1$		
	$\xrightarrow{(W_0', W_1')}$	

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	Eva	Bob
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	
		$v = x_b + r^{e_b} \mod n$
	$\xleftarrow{v}$	
$k_0 = (v - x_0)^{d_b}, k_1 = (v - x_1)^{d_b}$		
$W_0' = W_0 + k_0, W_1' + k_1$		
	$\xrightarrow{(W_0', W_1')}$	
		$W_c = W_c' - r$

1-od-2 Nesvestan prenos

Kriptografski protokol

Alisa	**Eva**	**Bob**
W_0, W_1	n, d_b	e_b, c
$x_0, x_1 \xleftarrow{U} \{0,1\}^n$		$r \xleftarrow{U} \{0,1\}^n$
	$\xrightarrow{(x_0, x_1)}$	
		$v = x_b + r^{e_b} \mod n$
	$\xleftarrow{v}$	
$k_0 = (v - x_0)^{d_b}, k_1 = (v - x_1)^{d_b}$		
$W_0' = W_0 + k_0, W_1' + k_1$		
	$\xrightarrow{(W_0', W_1')}$	
		$W_c = W_c' - r$

Razmislite kako se ovo može generalizovati! (npr **1-od-4**)

Zajedničko računanje

Pregled

Osobine ovakve šeme:

- Učestvuje dve ili više stranki, svaka sa svojim ulazom A_i.

Zajedničko računanje

Pregled

Osobine ovakve šeme:

- Učestvuje dve ili više stranki, svaka sa svojim ulazom A_i.
- Na kraju protokola, stranke su došle do vrednosti koja je jednaka $f(A)$.

Zajedničko računanje

Pregled

Osobine ovakve šeme:

- Učestvuje dve ili više stranki, svaka sa svojim ulazom A_i.
- Na kraju protokola, stranke su došle do vrednosti koja je jednaka $f(A)$.
- Na kraju protokola, ni jedna stranka ne zna tuđ ulaz.

Goldreich-Micali-Wigderson Protokol

Pregled

- Radi za **proizvoljan broj stranaka** (ovde 2), svaka sa proizvoljnim ulazom A_i.
- Radi za **proizvoljnu funkciju** $f(A)$ **proizvoljne dužine ulaza**.
- Na kraju protokola, ni jedna stranka ne zna ni o čijem ulazu više nego što je znala na početku.

Napomena

Svake dve partije imaju sopstven siguran kanal komunikacije.

Goldreich-Micali-Wigderson Protokol

Pojam udela

Udeo (*share*) je element niza vrednosti koji poseduje jedan učesnik, takav da rezultat XOR operacije nad svim udelima je deljena vrednost.

Goldreich-Micali-Wigderson Protokol

Pojam udela

Udeo (*share*) je element niza vrednosti koji poseduje jedan učesnik, takav da rezultat XOR operacije nad svim udelima je deljena vrednost.

$$S_1^A \oplus S_2^A \oplus S_3^A = A$$

Rekurzija: Šta ako imamo udeo udela? A udeo udela udela...?

Goldreich-Micali-Wigderson Protokol

Pojam udela

Udeo (*share*) je element niza vrednosti koji poseduje jedan učesnik, takav da rezultat XOR operacije nad svim udelima je deljena vrednost.

$$S_1^A \oplus S_2^A \oplus S_3^A = A$$

Rekurzija: Šta ako imamo udeo udela? A udeo udela udela...?
Isto!

$$\underbrace{(S_1^{S_1} \oplus S_2^{S_1} \oplus S_3^{S_1})}_{S1} \oplus S_2^A \oplus S_3^A$$

Goldreich-Micali-Wigderson Protokol

Pojam udela

Udeo (*share*) je element niza vrednosti koji poseduje jedan učesnik, takav da rezultat XOR operacije nad svim udelima je deljena vrednost.

$$S_1^A \oplus S_2^A \oplus S_3^A = A$$

Rekurzija: Šta ako imamo udeo udela? A udeo udela udela...?
Isto!

$$\underbrace{(S_1^{S_1} \oplus S_2^{S_1} \oplus S_3^{S_1})}_{S1} \oplus S_2^A \oplus S_3^A$$

$$= A$$

Goldreich-Micali-Wigderson Protokol

Osnovna ideja

Kako izračunati bilo koju funkciju sa bilo koliko učesnika (ulaza), tako da ni jedan učesnik ne sazna vrednost tuđih ulaza?
Svaki od učesnika ima 1 bit kao ulaz. Svaka funkcija se može predstaviti kao niz AND i XOR logičkih operacija.

Goldreich-Micali-Wigderson Protokol

Osnovna ideja

Kako izračunati bilo koju funkciju sa bilo koliko učesnika (ulaza), tako da ni jedan učesnik ne sazna vrednost tuđih ulaza?
Svaki od učesnika ima 1 bit kao ulaz. Svaka funkcija se može predstaviti kao niz AND i XOR logičkih operacija.

- Svaki učesnik neka da svakom drugom učesniku udeo svog ulaza.

Goldreich-Micali-Wigderson Protokol

Osnovna ideja

Kako izračunati bilo koju funkciju sa bilo koliko učesnika (ulaza), tako da ni jedan učesnik ne sazna vrednost tuđih ulaza?
Svaki od učesnika ima 1 bit kao ulaz. Svaka funkcija se može predstaviti kao niz AND i XOR logičkih operacija.

- Svaki učesnik neka da svakom drugom učesniku udeo svog ulaza.
- Ako je sledeća operacija XOR, promeniti svaki udeo tako da postanu udeli rezultata XOR funkcije.

Goldreich-Micali-Wigderson Protokol

Osnovna ideja

Kako izračunati bilo koju funkciju sa bilo koliko učesnika (ulaza), tako da ni jedan učesnik ne sazna vrednost tuđih ulaza?
Svaki od učesnika ima 1 bit kao ulaz. Svaka funkcija se može predstaviti kao niz AND i XOR logičkih operacija.

- Svaki učesnik neka da svakom drugom učesniku udeo svog ulaza.
- Ako je sledeća operacija XOR, promeniti svaki udeo tako da postanu udeli rezultata XOR funkcije.
- Ako je sledeća operacija AND, promeniti svaki udeo tako da postanu udeli rezultata AND funkcije.

Goldreich-Micali-Wigderson Protokol

Osnovna ideja

Kako izračunati bilo koju funkciju sa bilo koliko učesnika (ulaza), tako da ni jedan učesnik ne sazna vrednost tuđih ulaza?
Svaki od učesnika ima 1 bit kao ulaz. Svaka funkcija se može predstaviti kao niz AND i XOR logičkih operacija.

- Svaki učesnik neka da svakom drugom učesniku udeo svog ulaza.
- Ako je sledeća operacija XOR, promeniti svaki udeo tako da postanu udeli rezultata XOR funkcije.
- Ako je sledeća operacija AND, promeniti svaki udeo tako da postanu udeli rezultata AND funkcije.
- Uraditi tako za celo drvo. Na kraju će svi imati udeo rezultata funkcije

Goldreich-Micali-Wigderson Protokol

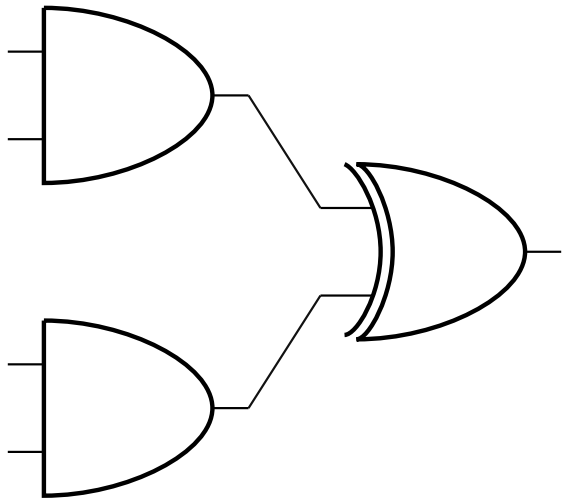
Osnovna ideja

Kako izračunati bilo koju funkciju sa bilo koliko učesnika (ulaza), tako da ni jedan učesnik ne sazna vrednost tuđih ulaza?
Svaki od učesnika ima 1 bit kao ulaz. Svaka funkcija se može predstaviti kao niz AND i XOR logičkih operacija.

- Svaki učesnik neka da svakom drugom učesniku udeo svog ulaza.
- Ako je sledeća operacija XOR, promeniti svaki udeo tako da postanu udeli rezultata XOR funkcije.
- Ako je sledeća operacija AND, promeniti svaki udeo tako da postanu udeli rezultata AND funkcije.
- Uraditi tako za celo drvo. Na kraju će svi imati udeo rezultata funkcije
- Udeli se sabiraju i rezultat se objavljuje

Goldreich-Micali-Wigderson Protokol

Primer



(ovo stvarno moram na tabli)

Goldreich-Micali-Wigderson Protokol

XOR operacija

	A	**B**	$\oplus$
A	S_A^A	S_B^A	$S_A^A \oplus S_B^A = A$
B	S_A^B	S_B^B	$S_A^B \oplus S_B^B = B$

Goldreich-Micali-Wigderson Protokol

XOR operacija

	A	B	$\oplus$
A	S_A^A	S_B^A	$S_A^A \oplus S_B^A$
	$\oplus$	$\oplus$	$\oplus$
B	S_A^B	S_B^B	$S_A^B \oplus S_B^B$

Goldreich-Micali-Wigderson Protokol

XOR operacija

	A	B	$\oplus$
A	S_A^A	S_B^A	$S_A^A \oplus S_B^A$
	$\oplus$	$\oplus$	$\oplus \quad = A \oplus B$
B	S_A^B	S_B^B	$S_A^B \oplus S_B^B$

Goldreich-Micali-Wigderson Protokol

AND operacija

Treba nam skup udela $C = AB$

Goldreich-Micali-Wigderson Protokol

AND operacija

Treba nam skup udela $C = AB$

$$C = \bigoplus_{i=1}^{n} S_i^C = A \oplus B$$

$$= \left[\bigoplus_{i=1}^{n} S_i^A\right] \left[\bigoplus_{i=1}^{n} S_i^B\right]$$

Goldreich-Micali-Wigderson Protokol

AND operacija

Treba nam skup udela $C = AB$

$$C = \bigoplus_{i=1}^{n} S_i^C = A \oplus B$$

$$= \left[\bigoplus_{i=1}^{n} S_i^A\right] \left[\bigoplus_{i=1}^{n} S_i^B\right]$$

$$= \bigoplus_{i,j} (S_i^A S_j^B)$$

Goldreich-Micali-Wigderson Protokol

AND operacija

Treba nam skup udela $C = AB$

$$C = \bigoplus_{i=1}^{n} S_i^C = A \oplus B$$

$$= \left[\bigoplus_{i=1}^{n} S_i^A\right]\left[\bigoplus_{i=1}^{n} S_i^B\right]$$

$$= \bigoplus_{i,j} (S_i^A S_j^B)$$

$$= \bigoplus_{i} (S_i^A S_i^B) \oplus \bigoplus_{i \neq j} (S_i^A S_j^B)$$

Goldreich-Micali-Wigderson Protokol

AND operacija

Treba nam skup udela $C = AB$

$$C = \bigoplus_{i=1}^{n} S_i^C = A \oplus B$$

$$= \left[\bigoplus_{i=1}^{n} S_i^A\right]\left[\bigoplus_{i=1}^{n} S_i^B\right]$$

$$= \bigoplus_{i,j} (S_i^A S_j^B)$$

$$= \bigoplus_{i} (S_i^A S_i^B) \oplus \bigoplus_{i \neq j} (S_i^A S_j^B)$$

$$= \bigoplus_{i} (S_i^A S_i^B) \oplus \bigoplus_{1 \leq i < j \leq n} (S_i^A S_j^B \oplus S_j^A S_i^B)$$

Goldreich-Micali-Wigderson Protokol

AND operacija

$$C = \bigoplus_{i} (S_i^A S_i^B) \oplus \bigoplus_{1 \leq i < j \leq n} (S_i^A S_j^B \oplus S_j^A S_i^B)$$

Goldreich-Micali-Wigderson Protokol

AND operacija

$$C = \bigoplus_{i} (S_i^A S_i^B) \oplus \bigoplus_{1 \leq i < j \leq n} (S_i^A S_j^B \oplus S_j^A S_i^B)$$

$$C = \bigoplus_{i=1}^{n} S_i^C$$

Goldreich-Micali-Wigderson Protokol

AND operacija

$$C = \bigoplus_{i} (S_i^A S_i^B) \oplus \bigoplus_{1 \leq i < j \leq n} (S_i^A S_j^B \oplus S_j^A S_i^B)$$

$$C = \bigoplus_{i=1}^{n} S_i^C$$

$$S_i^C = S_i^A S_i^B \oplus \bigoplus_{i \neq j} S_i^{S_i^A S_j^B \oplus S_j^A S_i^B}$$

Goldreich-Micali-Wigderson Protokol

AND operacija

$$S_i^C = S_i^A S_i^B \oplus \bigoplus_{i \neq j} S_i^{S_i^A S_j^B \oplus S_j^A S_i^B}$$

Goldreich-Micali-Wigderson Protokol

AND operacija

$$S_i^C = \underbrace{S_i^A S_i^B}_{\text{Samostalno izračunljiv}} \oplus \bigoplus_{i \neq j} S_i^{S_i^A S_j^B \oplus S_j^A S_i^B}$$

Goldreich-Micali-Wigderson Protokol

AND operacija

$$S_i^C = \underbrace{S_i^A S_i^B}_{\text{Samostalno izračunljiv}} \underbrace{\oplus \bigoplus_{i \neq j} S_i^{S_i^A S_j^B \oplus S_j^A S_i^B}}_{\text{Poseban protokol!}}$$

Goldreich-Micali-Wigderson Protokol

AND operacija

Stranke i i j se dogovaraju o svojim udelima u izrazu $S_i^A S_j^B \oplus S_j^A S_i^B$, tj S_i^* i S_j^*

Goldreich-Micali-Wigderson Protokol

AND operacija

Stranke i i j se dogovaraju o svojim udelima u izrazu $S_i^A S_j^B \oplus S_j^A S_i^B$, tj S_i^* i S_j^*

Postavimo stvar ovako:

$$S_i^* = R_{ij}$$
$$S_j^* = R_{ij} \oplus S_i^A S_j^B \oplus S_j^A S_i^B$$

To je validno zato što je njihov zbir jednak $S_i^A S_j^B \oplus S_j^A S_i^B$.
To jest $S_i^* \oplus S_j^* = *$

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A S_j^B \oplus S_j^A S_i^B \oplus R_{ij}$ ima **4** mogućih vrednosti

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A \underbrace{S_j^B}_{?} \oplus \underbrace{S_j^A}_{?} S_i^B \oplus R_{ij}$

  ima **4** mogućih vrednosti

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A \underbrace{S_j^B}_{?} \oplus \underbrace{S_j^A}_{?} S_i^B \oplus R_{ij}$

  ima **4** mogućih vrednosti
- Partija i izračuna sve 4 moguće vrednosti i uradi **1-od-4 nesvesni transfer** sa partijom j

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A \underbrace{S_j^B}_{?} \oplus \underbrace{S_j^A}_{?} S_i^B \oplus R_{ij}$

  ima **4** mogućih vrednosti
- Partija i izračuna sve 4 moguće vrednosti i uradi **1-od-4 nesvesni transfer** sa partijom j
- Partija j preuzme jednu od 4 vrednosti **na osnovu svoja dva bita**

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A \underbrace{S_j^B}_{?} \oplus \underbrace{S_j^A}_{?} S_i^B \oplus R_{ij}$ ima **4** mogućih vrednosti
- Partija i izračuna sve 4 moguće vrednosti i uradi **1-od-4 nesvesni transfer** sa partijom j
- Partija j preuzme jednu od 4 vrednosti **na osnovu svoja dva bita**
- Partija j ima svoj udeo jednak $S_i^A S_j^B \oplus S_j^A S_i^B \oplus R_{ij}$

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A \underbrace{S_j^B}_{?} \oplus \underbrace{S_j^A}_{?} S_i^B \oplus R_{ij}$ ima **4** mogućih vrednosti
- Partija i izračuna sve 4 moguće vrednosti i uradi **1-od-4 nesvesni transfer** sa partijom j
- Partija j preuzme jednu od 4 vrednosti **na osnovu svoja dva bita**
- Partija j ima svoj udeo jednak $S_i^A S_j^B \oplus S_j^A S_i^B \oplus R_{ij}$
- Partije i i j obe imaju svoj udeo

Goldreich-Micali-Wigderson Protokol

AND operacija

- Partija i generiše slučajan bit R_{ij}. Stoga on ima S_i^*
- Partija i ima R_{ij}, S_i^A i S_i^B. Stoga izraz $S_i^A \underbrace{S_j^B}_{?} \oplus \underbrace{S_j^A}_{?} S_i^B \oplus R_{ij}$ ima **4** mogućih vrednosti
- Partija i izračuna sve 4 moguće vrednosti i uradi **1-od-4 nesvesni transfer** sa partijom j
- Partija j preuzme jednu od 4 vrednosti **na osnovu svoja dva bita**
- Partija j ima svoj udeo jednak $S_i^A S_j^B \oplus S_j^A S_i^B \oplus R_{ij}$
- Partije i i j obe imaju svoj udeo
- Partije i i j nisu saznale ništa o tuđim ulazima

Goldreich-Micali-Wigderson Protokol

Poređenje složenosti

- AND: potrebno jedno samostalno množenjei 1-od-4 nesvesni transfer između svakog para i, j (sporo)

Goldreich-Micali-Wigderson Protokol

Poređenje složenosti

- AND: potrebno jedno samostalno množenjei 1-od-4 nesvesni transfer između svakog para i, j (sporo)
- XOR: samostalno računanje, 1 sabiranje (veoma brzo)

Goldreich-Micali-Wigderson Protokol

Poređenje složenosti

- AND: potrebno jedno samostalno množenjei 1-od-4 nesvesni transfer između svakog para i, j (sporo)
- XOR: samostalno računanje, 1 sabiranje (veoma brzo)
- NOT: potrebno da jedna osoba obrne svoj bit (veoma veoma brzo)

Goldreich-Micali-Wigderson Protokol

Poređenje složenosti

- AND: potrebno jedno samostalno množenjei 1-od-4 nesvesni transfer između svakog para i, j (sporo)
- XOR: samostalno računanje, 1 sabiranje (veoma brzo)
- NOT: potrebno da jedna osoba obrne svoj bit (veoma veoma brzo)

Još jedan način da uspostavimo ovaj protokol bi bilo da koristimo samo NAND operacije umesto AND i XOR (manje efikasno).

Primene

Big Data + **Privatnost** = **Secure Computations**

(u najboljem slučaju za nas)

Primene

Big Data + **Privatnost** = **Secure Computations**
(u najboljem slučaju za nas)

- Privacy-Preserving Data Mining

Primene

Big Data + **Privatnost** = **Secure Computations**
(u najboljem slučaju za nas)

- Privacy-Preserving Data Mining
- Privacy-Preserving Statistical Studies

Primene

Big Data + **Privatnost** = **Secure Computations**
(u najboljem slučaju za nas)

- Privacy-Preserving Data Mining
- Privacy-Preserving Statistical Studies
- Financial Data Analysis

Primene

Big Data + **Privatnost** = **Secure Computations**
(u najboljem slučaju za nas)

- Privacy-Preserving Data Mining
- Privacy-Preserving Statistical Studies
- Financial Data Analysis
- **Internet of Things** Statistical Studies

Pauza! :)

Kriptovalute

Osnovni problem

U odsustvu centralne banke, šta može da potkrepi vrednost novca?

Kriptovalute

Osnovni problem

U odsustvu centralne banke, šta može da potkrepi vrednost novca?

Bitkoin: Demokratija! (ili tako nešto)

Blockchain

Opis

- Korisnik slepo veruje samo "većini"mreže (računski najmoćnijem delu) koja gradi **blockchain**.

Blockchain

Opis

- Korisnik slepo veruje samo "većini"mreže (računski najmoćnijem delu) koja gradi **blockchain**.
- Blockchain je dinamična baza podataka koja sadrži **blokove**.

Blockchain

Opis

- Korisnik slepo veruje samo "većini"mreže (računski najmoćnijem delu) koja gradi **blockchain**.
- Blockchain je dinamična baza podataka koja sadrži **blokove**.
- Bitcoin mreža svakih **10 minuta** generiše nov blok koji sadrži **Merkleov koren** nekog skupa transakacija

Blockchain

Opis

- Korisnik slepo veruje samo "većini"mreže (računski najmoćnijem delu) koja gradi **blockchain**.
- Blockchain je dinamična baza podataka koja sadrži **blokove**.
- Bitcoin mreža svakih **10 minuta** generiše nov blok koji sadrži **Merkleov koren** nekog skupa transakacija
- Ako se transakcija nalazi u bloku, ona je **validna**.

Blockchain

Opis

- Korisnik slepo veruje samo "većini"mreže (računski najmoćnijem delu) koja gradi **blockchain**.
- Blockchain je dinamična baza podataka koja sadrži **blokove**.
- Bitcoin mreža svakih **10 minuta** generiše nov blok koji sadrži **Merkleov koren** nekog skupa transakacija
- Ako se transakcija nalazi u bloku, ona je **validna**.
- Svaki blok sadrži i transakciju koja **stvara novac** ni iz čega.

Blockchain

Opis

- Korisnik slepo veruje samo "većini"mreže (računski najmoćnijem delu) koja gradi **blockchain**.
- Blockchain je dinamična baza podataka koja sadrži **blokove**.
- Bitcoin mreža svakih **10 minuta** generiše nov blok koji sadrži **Merkleov koren** nekog skupa transakacija
- Ako se transakcija nalazi u bloku, ona je **validna**.
- Svaki blok sadrži i transakciju koja **stvara novac** ni iz čega.
- Kada “mreža“ dođe do novog bloka, **nema spora oko toga da li je validan**, i generisanje ulazi u nov krug.

Transakcija

Opis

- Transakcija šalje novac sa jedne ili više adresa pozivajući se rekurzivno na **proteklu transakciju**.
- **Baza rekurzije** je transakcija koja pravi vrednost ni iz čega (jedna u svakom bloku).

Vizuelizacija

Transakcija

Dokaz sigurnosti

Kako potvrditi *tačnost* transakcije?

- Proverimo da li se slaže sa **digitalnim potpisom**, koji se ne može imitirati

Transakcija

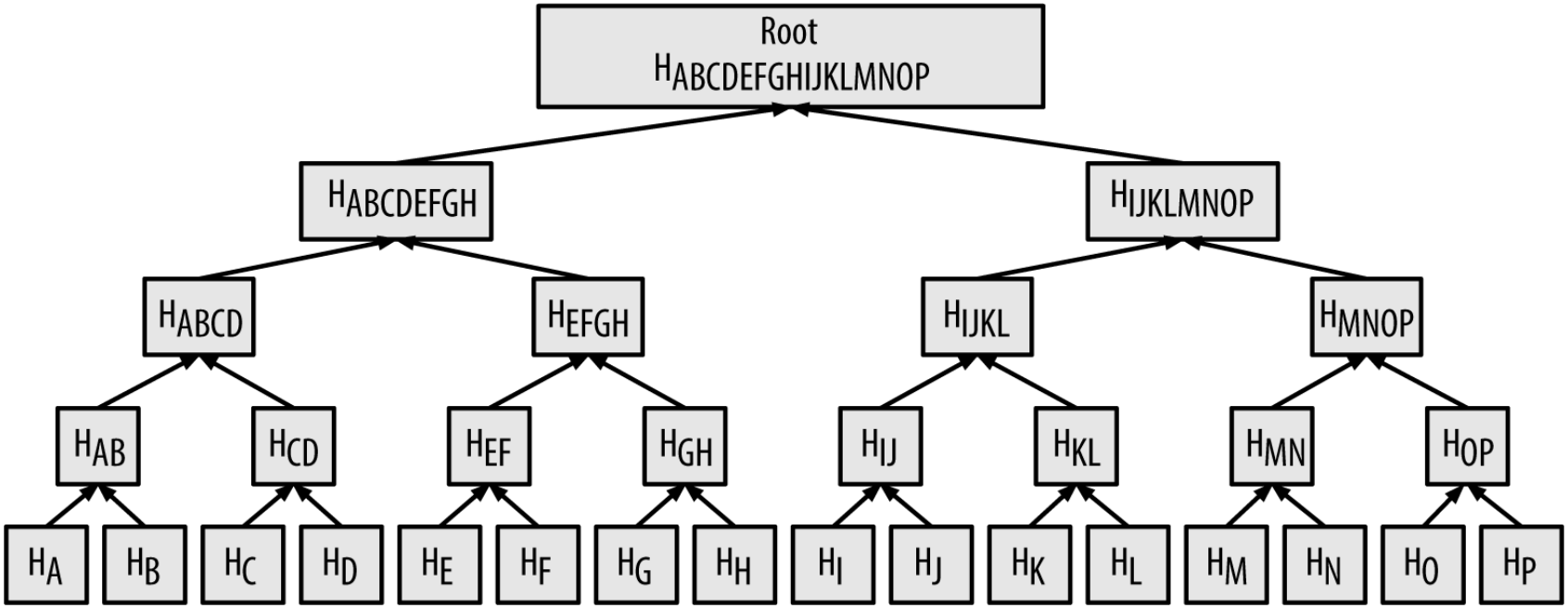
Dokaz sigurnosti

Kako potvrditi *tačnost* transakcije?

- Proverimo da li se slaže sa **digitalnim potpisom**, koji se ne može imitirati
- Korisnik može da potpiše transakciju i da ona bude ***tačna***, ali da bi bila i **validna** mora biti deo bloka (proveriti)

Transakcija

Merkleovo Drvo



Provera Transakcije

Dokaz sigurnosti

Kako da efikasno proverimo da li je transakcija **T** validna?
Validnost = deo je nekog od validnih Merkleovih stabla.

Provera Transakcije

Dokaz sigurnosti

Kako da efikasno proverimo da li je transakcija **T** validna?
Validnost = deo je nekog od validnih Merkleovih stabla.

Loše rešenje

Zatražimo od mreže sve transakcije i ponovo izračunamo drvo.
Proverimo da li je dobijen koren zapisan u nekom od blokova.
Složenost: $N \log N$

Provera Transakcije

Dokaz sigurnosti

Kako da efikasno proverimo da li je transakcija **T** validna?
Validnost = deo je nekog od validnih Merkleovih stabla.

Loše rešenje

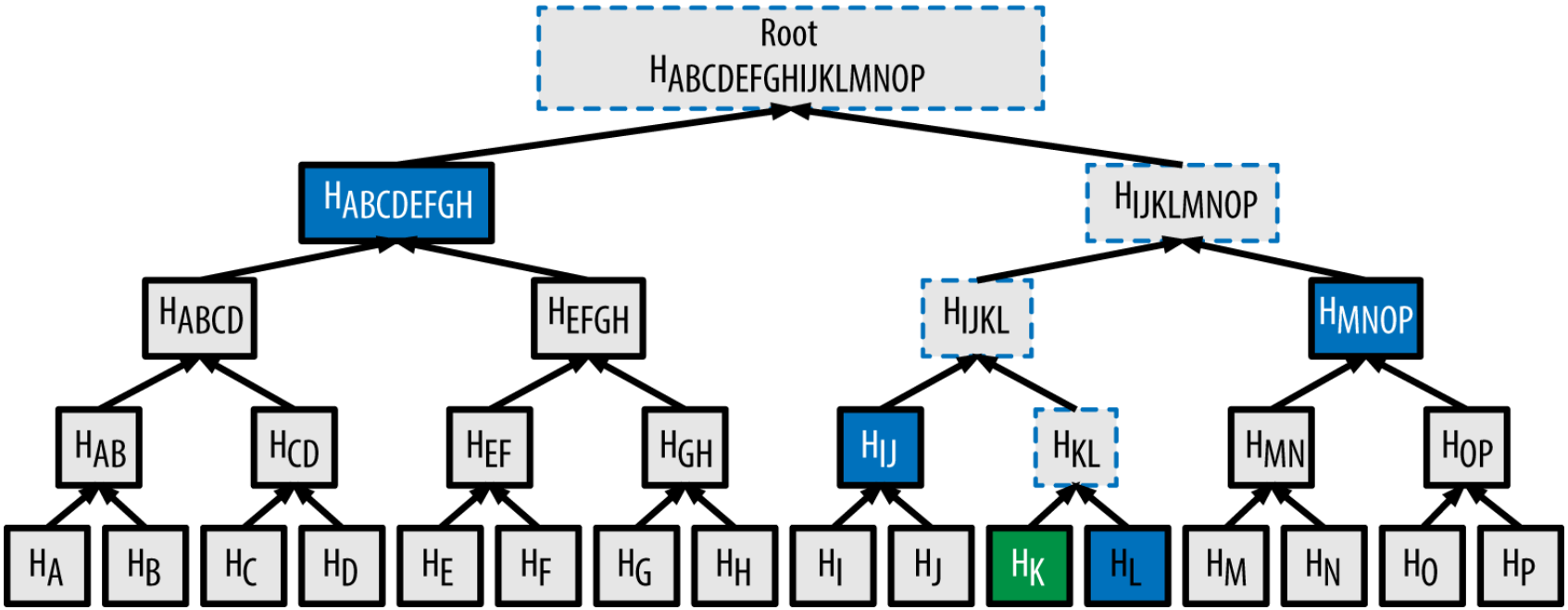
Zatražimo od mreže sve transakcije i ponovo izračunamo drvo.
Proverimo da li je dobijen koren zapisan u nekom od blokova.
Složenost: $N \log N$

Dobro rešenje

Zatražimo od mreže $\log_2 N$ vrednosti na osnovu kojih dolazimo do korena stabla.
Složenost: $\log N$

Provera Transakcije

Dokaz sigurnosti



Provera Transakcije

Dokaz sigurnosti

Da li neko iz mreže može da nas prevari (da li može da nas natera da poverujemo da je neka transakcija validna, ako nije)?

Provera Transakcije

Dokaz sigurnosti

Da li neko iz mreže može da nas prevari (da li može da nas natera da poverujemo da je neka transakcija validna, ako nije)?
Ne može! U slučaju $N = 16$ morao bi da generiše vrednosti x_1, x_2, x_3 i x_4 takve da:

$$H(H(H(H(x_1, T), x_2), x_3), x_4) = H_{ABCDEFGH}$$

Provera Transakcije

Dokaz sigurnosti

Da li neko iz mreže može da nas prevari (da li može da nas natera da poveruje da je neka transakcija validna, ako nije)?
Ne može! U slučaju $N = 16$ morao bi da generiše vrednosti x_1, x_2, x_3 i x_4 takve da:

$$\underbrace{H(H(H(H(x_1, T), x_2), x_3), x_4))}_{\text{Nasumična vrednost}} = \underbrace{H_{ABCDEFGH}}_{\text{Nasumična vrednost}}$$

Provera Transakcije

Dokaz sigurnosti

Da li neko iz mreže može da nas prevari (da li može da nas natera da poveruje da je neka transakcija validna, ako nije)?
Ne može! U slučaju $N = 16$ morao bi da generiše vrednosti x_1, x_2, x_3 i x_4 takve da:

$$H(\underbrace{H(H(H(x_1, T), x_2), x_3), x_4)}_{\text{Nasumična vrednost}}) = \underbrace{H_{ABCDEFGH}}_{\text{Nasumična vrednost}}$$

$$H(A \xleftarrow{R} \{0,1\}^{512}) = B \xleftarrow{R} \{0,1\}^{256}$$

Provera Transakcije

Dokaz sigurnosti

Da li neko iz mreže može da nas prevari (da li može da nas natera da poveruje da je neka transakcija validna, ako nije)?
Ne može! U slučaju $N = 16$ morao bi da generiše vrednosti x_1, x_2, x_3 i x_4 takve da:

$$H(\underbrace{H(H(H(x_1, T), x_2), x_3), x_4)}_{\text{Nasumična vrednost}}) = \underbrace{H_{ABCDEFGH}}_{\text{Nasumična vrednost}}$$

$$H(A \xleftarrow{R} \{0,1\}^{512}) = B \xleftarrow{R} \{0,1\}^{256}$$

Absurd! H onda nije sigurna heš funkcija.

Mining

Opis

Mining je problem nalaženja sledećeg bloka.

Mining

Opis

Mining je problem nalaženja sledećeg bloka.

Sadržaj	**Veličina [bajtovi]**
Verzija	4
Heš prethodnog bloka	32
Merkleov koren X transakcija	32
Timestamp	4
Teškoća generisanja	4
Nonce	4

Mining

Opis

Mining je problem nalaženja sledećeg bloka.

Sadržaj	**Veličina [bajtovi]**	
Verzija	4	} **Predvidljivo**
Heš prethodnog bloka	32	
Merkleov koren X transakcija	32	
Timestamp	4	
Teškoća generisanja	4	
Nonce	4	

Nema varijacije Blaga varijacija

Mining

Opis

Mining je problem nalaženja sledećeg bloka.

Sadržaj	**Veličina [bajtovi]**	
Verzija	4	**Predvidljivo**
Heš prethodnog bloka	32	
Merkleov koren X transakcija	32	
Timestamp	4	
Teškoća generisanja	4	
Nonce	4	

Nema varijacije Blaga varijacija Obavezna varijacija

Mining

C++ Algoritam

Validan blok je onaj čiji heš hedera počinje sa dovoljnim brojem nula.

Mining

C++ Algoritam

Validan blok je onaj čiji heš hedera počinje sa dovoljnim brojem nula.

$$H(\underbrace{const, nonce}_{\text{header}}) \stackrel{?}{=} 0000000000000000XX...X_2$$

$$H(\underbrace{const, nonce'}_{\text{header'}}) \stackrel{?}{=} 0000000000000000XX...X_2$$

$$H(\underbrace{const, nonce''}_{\text{header''}}) \stackrel{?}{=} 0000000000000000XX...X_2$$

...

Mining

BlockCHAIN

Lančana struktura (blockchain)

- Svaki blok zavisi od prethodnog.

Mining

BlockCHAIN

Lančana struktura (blockchain)

- Svaki blok zavisi od prethodnog.
- Znači svaki blok zavisi od svih blokova pre njega.

Mining

BlockCHAIN

Lančana struktura (blockchain)

- Svaki blok zavisi od prethodnog.
- Znači svaki blok zavisi od svih blokova pre njega.
- Ako tražite sledeći blok, vi prihvatate sve blokove pre njega kao ispravne!

Mining

U praksi

- Za svaki novi nonce, imate **minijaturnu šansu** da generišete validan paket

Mining

U praksi

- Za svaki novi nonce, imate **minijaturnu šansu** da generišete validan paket
- Teškoća se podešava tako da cela mreža generiše paket svakih **10 minuta** (*scaling*)

Mining

U praksi

- Za svaki novi nonce, imate **minijaturnu šansu** da generišete validan paket
- Teškoća se podešava tako da cela mreža generiše paket svakih **10 minuta** (*scaling*)
- Kolektivna računska moć Bitcoin mreže je **8000 puta veća** od kolektivne moći najbržih 500 superračunara

Mining

Motivacija

- Prva transakcija stvara vrednost **onome ko je našao blok**

Mining

Motivacija

- Prva transakcija stvara vrednost **onome ko je našao blok**
- Sve transakcije plaćaju proviziju **onome ko je našao blok**

Mining

Motivacija

- Prva transakcija stvara vrednost **onome ko je našao blok**
- Sve transakcije plaćaju proviziju **onome ko je našao blok**
- **Mining guilds** - rešavaju statistički nedostatak balansa

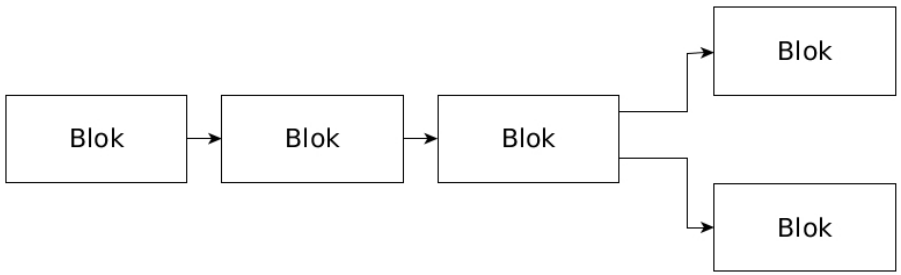
```
while (true)
    // network request
    uint32_t header[20] = get_work();

    // maksimalni hash
    t = f(header[19]);

    while ( header[20] < 0xffffffff ) {
        if (hash(header) < t )
            // network response
            announce_new_block(header);
        else
            header[20]++;
    }
}
```

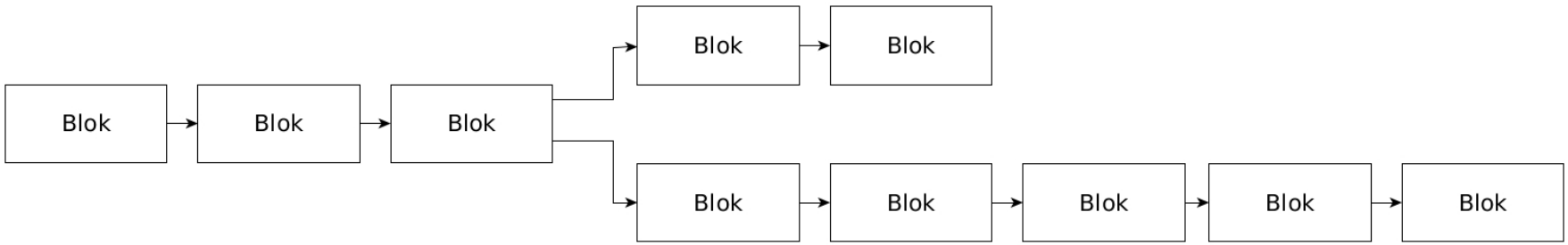
Problemi

Orphan Blocks, Soft Forking



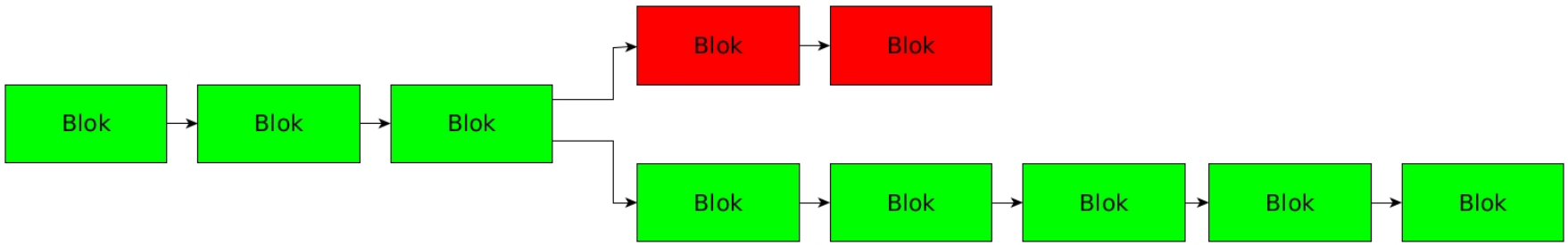
Problemi

Orphan Blocks, Soft Forking



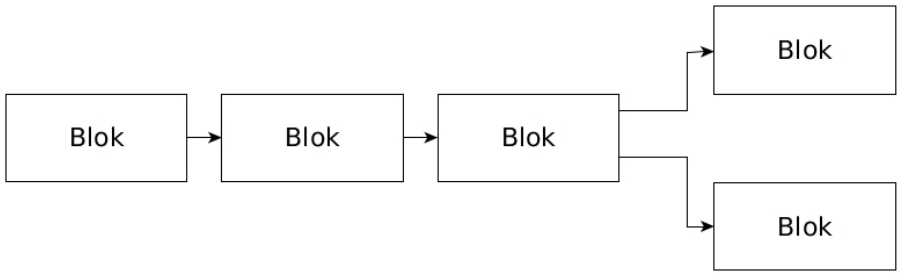
Problemi

Orphan Blocks, Soft Forking



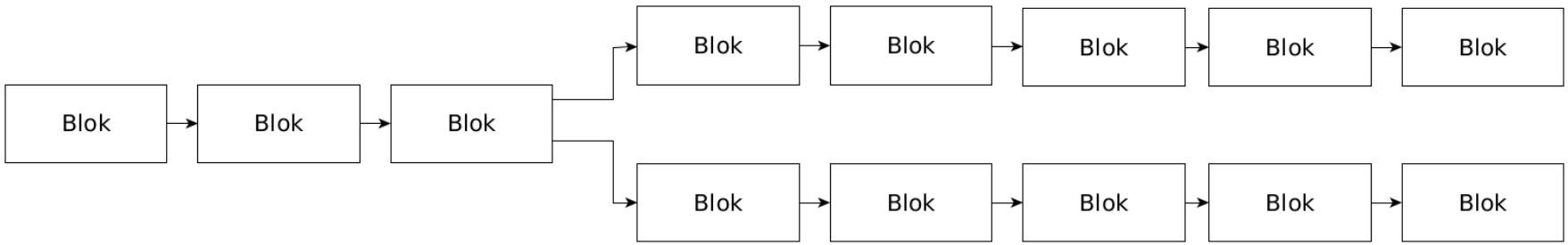
Problemi

Hard Forking



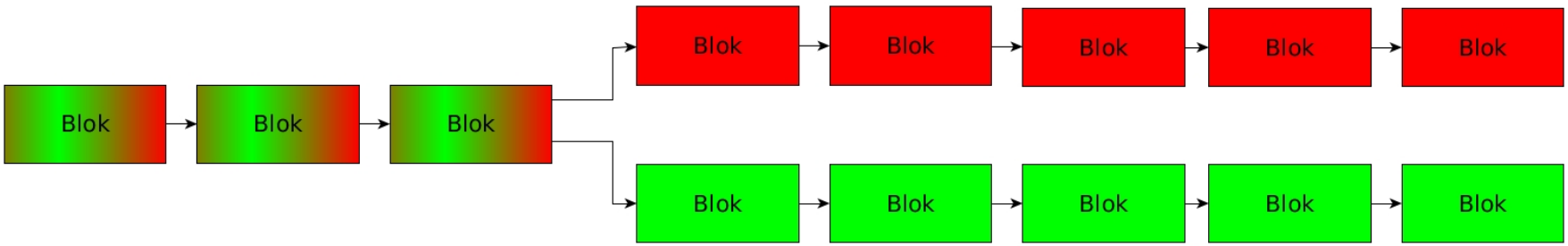
Problemi

Hard Forking



Problemi

Hard Forking



Napadi

51% Attack

51% Attack - Opis

Jednointeresni entitet kontroliše **više od 50%** kolektivne moći heširanja mreže.

Napadi

51% Attack

51% Attack - Opis

Jednointeresni entitet kontroliše **više od 50%** kolektivne moći heširanja mreže.

51% Attack - Posledice

- Kontrola nad svim budućim transakcijama
- Mogućnost prepisivanja proteklih transakcija (što stariji blok, to teže)

Napadi

51% Attack

51% Attack - Opis

Jednointeresni entitet kontroliše **više od 50%** kolektivne moći heširanja mreže.

51% Attack - Posledice

- Kontrola nad svim budućim transakcijama
- Mogućnost prepisivanja proteklih transakcija (što stariji blok, to teže)

51% Attack - Zaštita

Princip slepog verovanja većini je rekao svoje.

Napadi

Quantum Attack

Quantum Attack - Opis

Dovoljno moćan kvantni računar koji implementira **Šorov algoritam** je napravljen.

Napadi

Quantum Attack

Quantum Attack - Opis

Dovoljno moćan kvantni računar koji implementira **Šorov algoritam** je napravljen.

Quantum Attack - Posledice

- Potpun pristup svom BTC novcu za dat javni ključ adrese (sav poslat novac)

Napadi

Quantum Attack

Quantum Attack - Zaštita

- Korišćenje hešova dovoljno velikog izlaza. Integritet blokova ostaje netaknut (iako prepolovljen na 128 bita sigurnosti)

Napadi

Quantum Attack

Quantum Attack - Zaštita

- Korišćenje hešova dovoljno velikog izlaza. Integritet blokova ostaje netaknut (iako prepolovljen na 128 bita sigurnosti)
- Prelazak na **kvantno sigurni public-key sistem** (NTRU) ili **jednokratne potpise zasnovane na heševima** (Lamportovi potpisi, Merelova šema potpisa) izmenom protokola

Zaključak

Bitcoin u tri stavki

- Stvaranje i prenos vrednosti se vrši preko transakcija.

Zaključak

Bitcoin u tri stavki

- Stvaranje i prenos vrednosti se vrši preko transakcija.
- Blokovi čine tačne transakcije validnim.

Zaključak

Bitcoin u tri stavki

- Stvaranje i prenos vrednosti se vrši preko transakcija.
- Blokovi čine tačne transakcije validnim.
- Svako u mreži pravi, proverava i veruje u blokove iz sebičnih razloga.

Zaključak

Bitcoin u tri stavki

- Stvaranje i prenos vrednosti se vrši preko transakcija.
- Blokovi čine tačne transakcije validnim.
- Svako u mreži pravi, proverava i veruje u blokove iz sebičnih razloga.
- **Ako su ove tri činjenice tačne, sve radi :)**

Reference i kontakt


Andreas M. Antonopoulos, Mastering Bitcoin


Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System


Oded Goldreich, Silvio Micali and Avi Wigderson, Proofs that Yield Nothing But their Validity or All Languages in NP have Zero-Knowledge Proofs

Kontakt autora:
scrnojevic@protonmail.ch
LinkedIn