

“

KRYPTOWALUTY
Z PERSPEKTYWY INFORMATYKI
ŚLEDZECZEJ

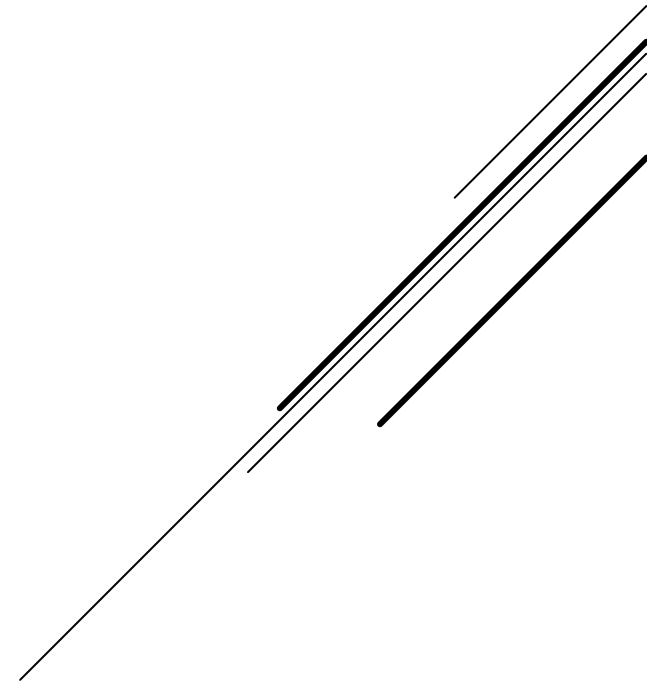
”

INTRO

dr inż. Przemysław RODWALD

- I. Trzy slajdy o mnie
- II. Oferta dla organów procesowych
- III. Tematyka szkolenia
- IV. Dalsze poszerzanie wiedzy

PLAN PREZENTACJI

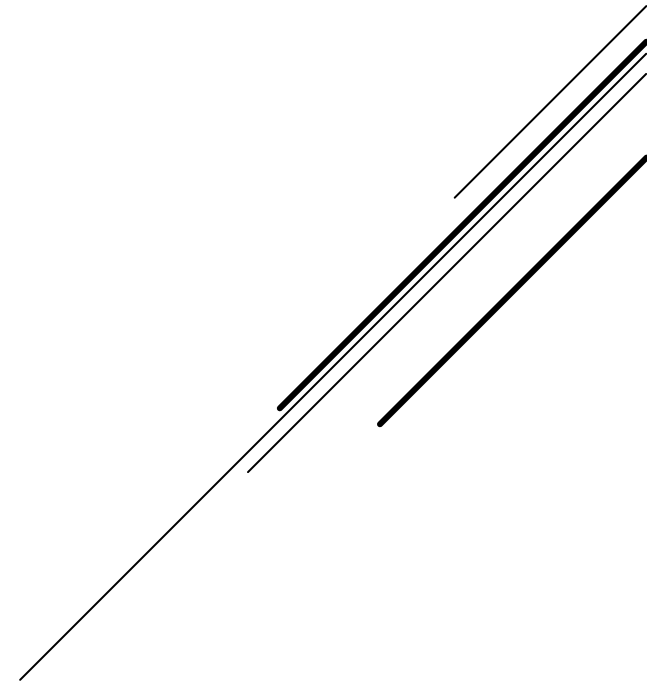


- ▶ Warszawa
- ▶ Gdańsk

INFORMATYKA :

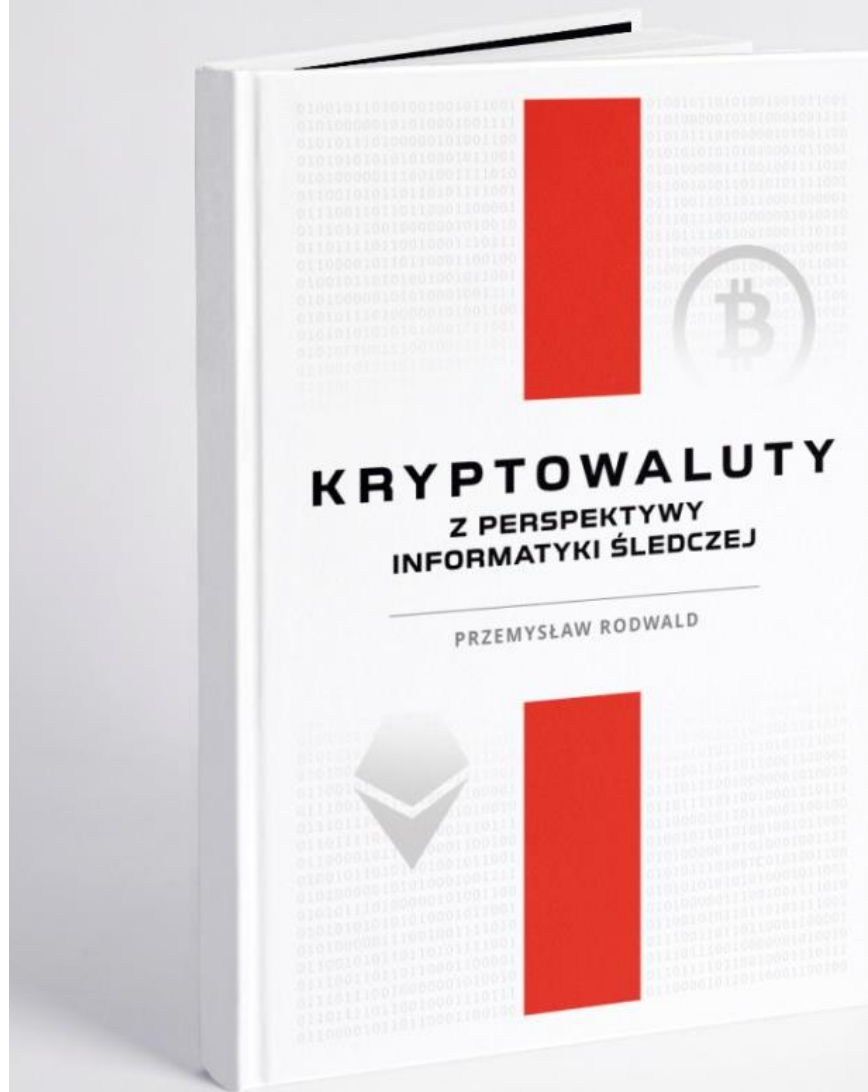
- **kryptowaluty i technologia blockchain** (*kilkadziesiąt opinii*)
- kryptologia i bezpieczeństwo systemów teleinformatycznych
- informatyka śledcza w tym analiza urządzeń mobilnych

O MNIE
I.BIEGŁY SĄDOWY



- ▶ **Monografia:**
 - ▶ „Kryptowaluty z perspektywy informatyki śledczej”, Wydawnictwo AMW, 2021
 - ▶ Wydziały Cyber KWP (17)
 - ▶ Prokuratury Regionalne i Okręgowe (53)
- ▶ **Artykuły:**
 - ▶ „Metody deanonimizacji użytkowników wybranych kryptowalut na przykładzie bitcoina”, 2019
 - ▶ „Wybór strategii łamania hasła przy nałożonych ograniczeniach czasowych”, 2019

○ MNIE
II.AUTOR



- ▶ **AKADEMIA MARYNARKI WOJENNEJ**
 - ▶ **KATEDRA INFORMATYKI (KI)**
 - ▶ Przełamywanie zabezpieczeń kryptograficznych
 - ▶ Jak długo łamiemy? Spersonalizowane słowniki !!!

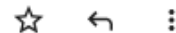
O MNIE
III.Z-CA KIEROWNIKA KI



Nie odpowiadaj na ten mail <powiadomienia.ekssip@kssip.gov.pl>

do mnie ▾

pt., 10 kwi 2020, 02:37



BD-I.0160.5.2020

Komunikat nr 19/2020 Dyrektora Krajowej Szkoły Sądownictwa i Prokuratury z dnia 8 kwietnia 2020 r.w sprawie stwierdzenia możliwości naruszenia ochrony danych osobowych

Krajowa Szkoła Sądownictwa i Prokuratury informuje, że stwierdzono istnienie dużego prawdopodobieństwa wystąpienia incydentu bezpieczeństwa, polegającego na uzyskaniu nieuprawnionego dostępu do danych poprzednio użytkowanej Platformy Szkoleniowej. Niezwłocznie po otrzymaniu informacji o tym fakcie wdrożone zostały wszystkie przewidziane przepisami procedury zmierzające do usunięcia skutków powyższego incydentu, w tym powiadomione zostały właściwe służby odpowiedzialne za bezpieczeństwo cyfrowe, a Krajowa Szkoła – jako podmiot pokrzywdzony – pozostaje z nimi w bieżącym kontakcie.

Informuję ponadto, że naruszenie bezpieczeństwa danych, w tym danych osobowych zgromadzonych na e-KSSiP (aktualnie wykorzystywanej Platformie Szkoleniowej) nie zostało stwierdzone, jednak w zaistniałej sytuacji ze względów bezpieczeństwa podjęta została decyzja o zresetowaniu wszystkich haseł użytkowników Platformy Szkoleniowej e-KSSiP. Logowanie do e-KSSiP jest możliwe tylko po ustanowieniu nowego hasła przy pomocy funkcji „Zapomniałeś hasła?” i postępowaniu zgodnie z kolejnymi instrukcjami.

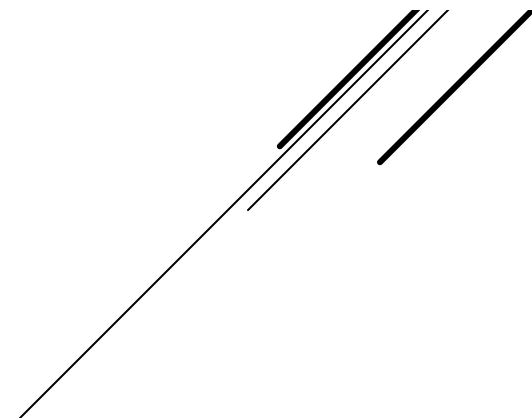
Dalsze informacje będą na bieżąco przekazywane za pomocą środków komunikacji elektronicznej.

DYREKTOR KRAJOWEJ SZKOŁY SĄDOWNICTWA I PROKURATURY

dr hab. Małgorzata Manowska sędzia Sądu Najwyższego

/pismo podpisane podpisem elektronicznym/

CO MOŻNA ŁAMAĆ?





Jak złamano hasła ofiar wycieku danych z KSSiP?

Autor: Wpis Gościnny dnia 6 września 2022 | 2 komentarze

Ponad dwa lata temu opisaliśmy wyciek danych kilkudziesięciu tysięcy pracowników polskiego wymiaru sprawiedliwości. Ujawniona wówczas baza zawierała hasze haseł, które wydawały się nie do złamania. Słowo „wydawały” zostało użyte celowo....

[Czytaj dalej](#)



Dane ponad 50 tysięcy polskich prokuratorów, sędziów i asesorów krążą po sieci

Autor: Adam Haertle dnia 13 kwietnia 2020 | 37 komentarzy

Wiele komunikatów o „wycieku danych” mówi o sytuacjach, gdy dane trafiły w ręce jednej niepowołanej osoby lub w takie ręce mogły trafić, a nie trafiły. Tym razem jest jednak inaczej – baza Krajowej Szkoły Sądownictwa i

Prokuratury leży w internecie....

[Czytaj dalej](#)

► Ile to może trwać?

- Złamanie wszystkich haseł 8-znakowych – 12h: 4 x GPU2080
- Złamanie wszystkich haseł 9-znakowych – 10 dni: 30x GPU2080
- ...

☐ PORADNIK BAZ DANYCH Fox 10/12/2022 (Wed) 19:44 [Preview] No.401 del
(14.21 KB 255x224 pov.jpg)



1. Pobierz bazy danych z Endchan.
2. Otwórz terminal we Whonix Workstation.
3. Wykonaj komendy grep, aby komfortowo przeglądać bazy.

Baza KSSiP

Baza sędziów i prokuratorów. 50 000 osób i adresów e-mail. 10 000 numerów telefonów.

Do pobrania na Endchan po kliknięciu [>>73](#)

```
grep -i 'Legnica' kssip.gov.pl.csv  
awk -F '\t' '{print $13}' kssip.gov.pl.csv > emaile.txt  
awk -F '\t' '{print $20}' kssip.gov.pl.csv > telefony.txt  
awk -F '\t' '{print $21}' kssip.gov.pl.csv > telefony2.txt  
sort telefony.txt > telefonsort.txt  
uniq telefonsort.txt > telefonyuniq.txt
```

A CO Z PAŃSTWA HASŁAMI?

część jawna (publicznie dostępna) *

część niejawna

▶ **TEORIA**

- ▶ zasady działania kryptowalut
- ▶ klucze, adresy, łańcuch bloków
- ▶ pseudoanonimowość

▶ **PRAKTYKA**

- ▶ pozyskiwanie kryptowalut
- ▶ przechowywanie (portfele)
- ▶ rodzaje przestępstw

▶ **PRZEWODNIK**

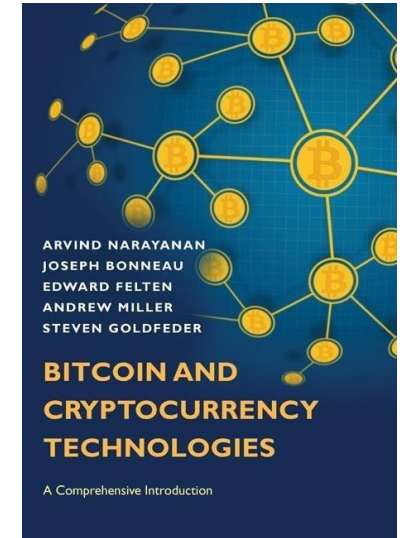
- ▶ **deanonimizacja**
- ▶ **zabezpieczenie majątkowe**
- ▶ **case studies**
- ▶ **wyzwania**

TEMATYKA SZKOLENIA / AGENDA

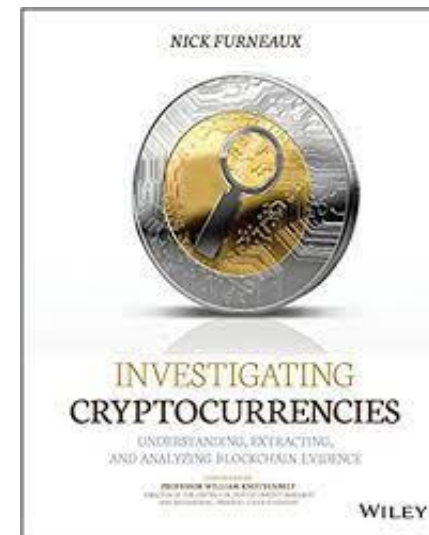
WERSJA STACJONARNA

* materiały pod adresem: <https://rodwald.pl/blog/2023>

- ▶ Bitcoin and cryptocurrency technologies : a comprehensive introduction
 - ▶ Narayanan, Bonneau, Felten, Miller, Goldfeder. Oxford, Princeton University Press, 2016

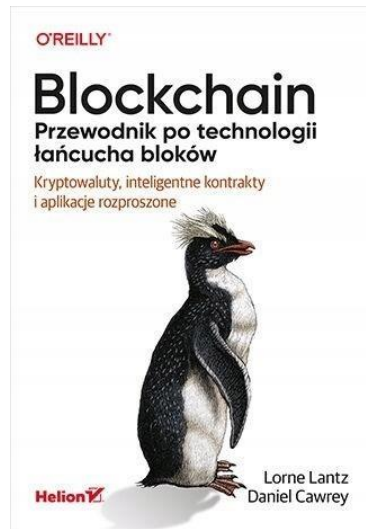
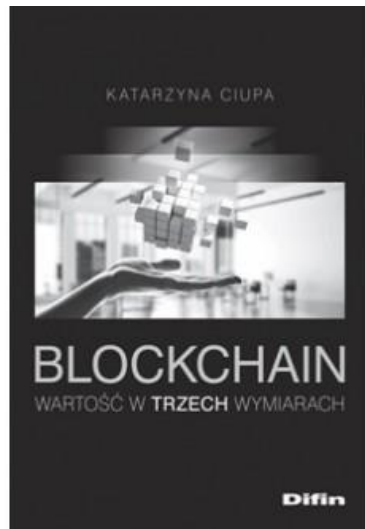
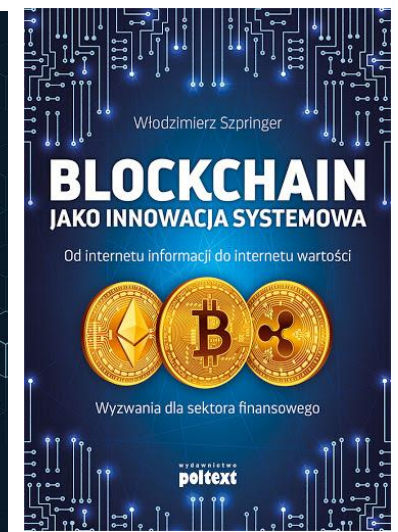
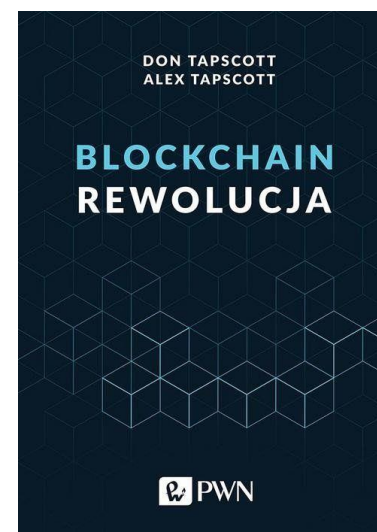
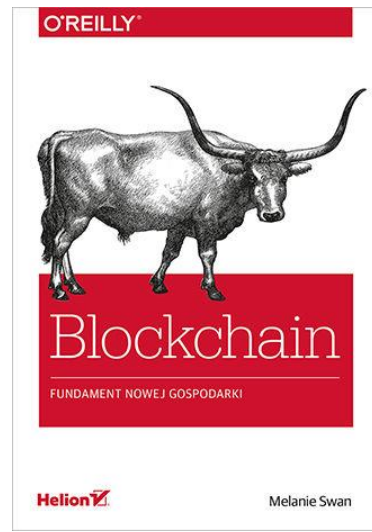


- ▶ Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence
 - ▶ Nick Furneaux. WILEY, 2018

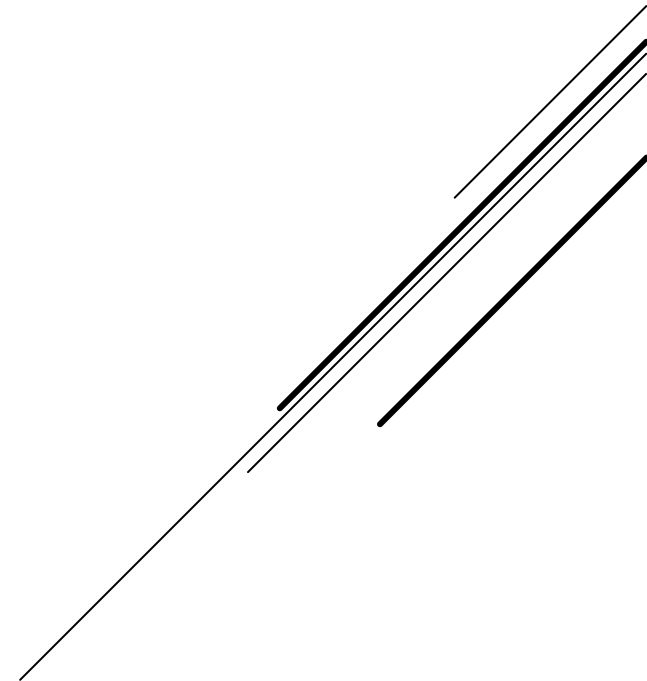


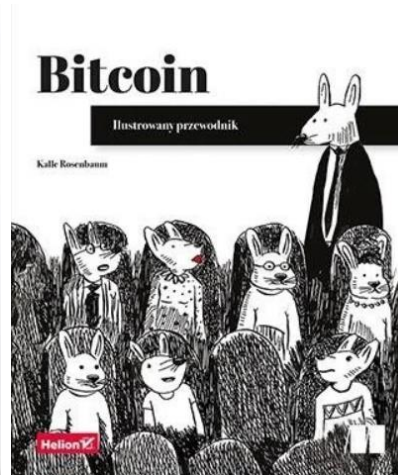
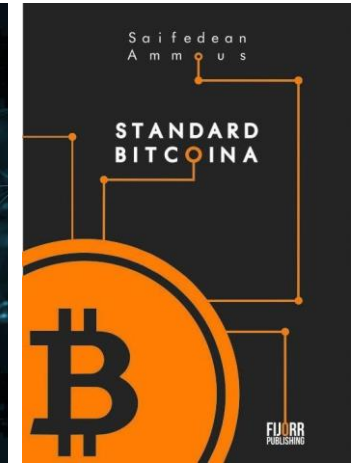
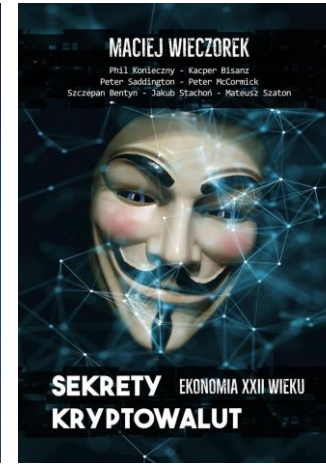
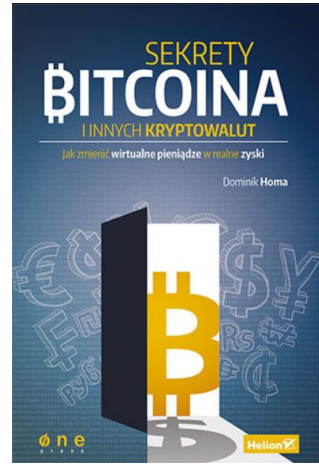
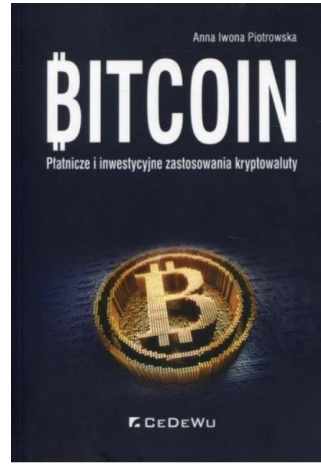
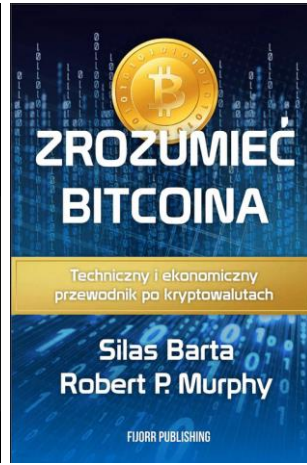
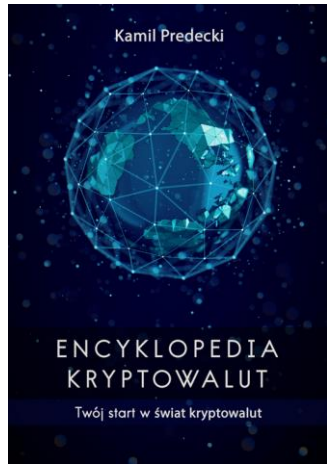
POSZERZANIE WIEDZY



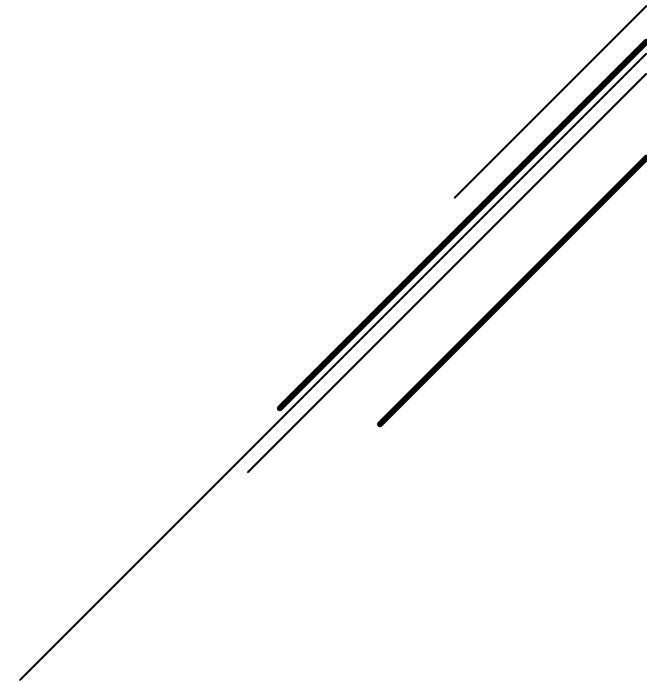


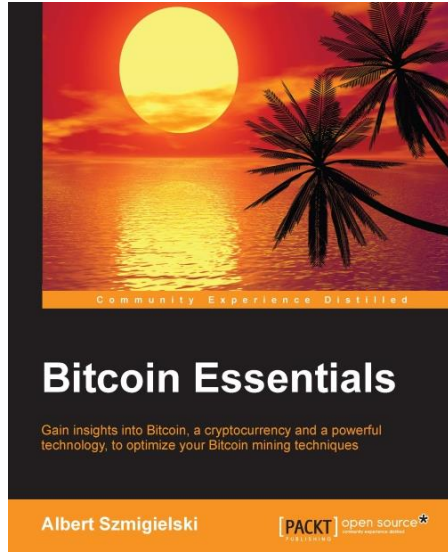
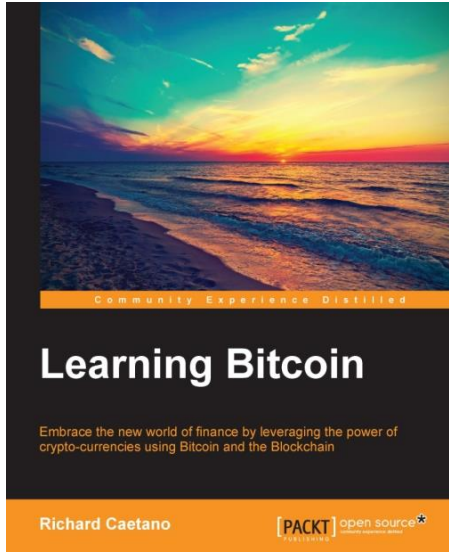
...





...





...



- ▶ MOOC (Massive Open Online Course - masowy otwarty kurs online)
 - ▶ <https://www.coursera.org/learn/cryptocurrency>
- ▶ Studia podyplomowe
 - ▶ <https://ssl-oferta.sgh.waw.pl/pl/studiapodyplomowe/blockchain-biznes-prawo-technologia/>
- ▶ Studia zagraniczne
 - ▶ <https://digitalcurrency.unic.ac.cy/>



UNIVERSITY
of NICOSIA

DO POSTUDIOWANIA

► <https://rodwald.pl>

► wizytówki

KONTAKT

KMDR POR. DR INŻ.
**PRZEMYSŁAW
RODWALD**



Katedra Informatyki

+48 261 262 719
p.rodwald@amw.gdynia.pl

Akademia Marynarki Wojennej
Śmidowicza 69, 81-127 Gdynia

DR INŻ.
**PRZEMYSŁAW
RODWALD**

Biegły sądowy z informatyki

+48 888 218 869
www.rodwald.pl

01010010
01101111
01100100
01110111
01100001
01101100
01100100

01010010
01101111
01100100
01110111
01100001
01101100
01100100

