Blockchain Security Challenges and Solutions

B. RAMAMURTHY

Fulbright Scholar 2025-26

Manning author: Blockchain in action

PROGRAM DIRECTOR, DATA-INTENSIVE COMPUTING PROGRAM

COURSERA INSTRUCTOR (Blockchain, DeFi)

DIRECTOR, BLOCKCHAIN THINKLAB

HTTP://WW.CSE.BUFFALO.EDU/FACULTY/BINA

COMPUTER SCIENCE AND ENGINEERING

Wallet Addresses (Ethereum): bina.eth

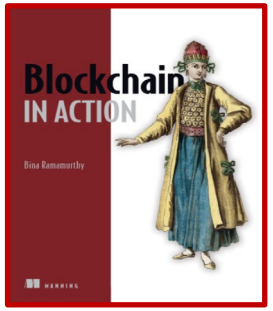
https://www.linkedin.com/in/bina-ramamurthy/

University at Buffalo
Blockchain ThinkLab

Introducing myself

Been in Buffalo, NY, USA for more than 40 years!
Ph.D. in Computer Engineering: Fault tolerance in distributed systems
Faculty at CSE and University at Buffalo (UB) for the past 3 decades
Launched a 4-courses certification on blockchain on Coursera MOOC (2018)
--More than 400,000 learners and 1,000,000 visitors from all over the world
Coursera Decentralized Finance (DeFi) – a 3-course certification (2024).

Funding: National Science Foundation ((> 1 million), SUNY IITG, industrial
And private donations.



SUNY chancellor's award for excellence in teaching 2019
IEEE Region 1 Outstanding Teacher Award (2022)
Author of a technical book: Blockchain in Action (Manning.com)
Co-author of Blockchain, Cryptocurrency and DeFi (World Scientific)

Fulbright Scholar

- Now I am Fulbright Scholar at St. Polten University of Applied Science
- Expanding on my deep involvement in
- Blockchain, Cryptocurrency and Decentralized Applications.

Technical level of the talk

- **User/participant level** ✓
- Application level
- Code /programming level
- Algorithmic /Fundamental Protocol level

However, if you have any questions do not hesitate to ask me.

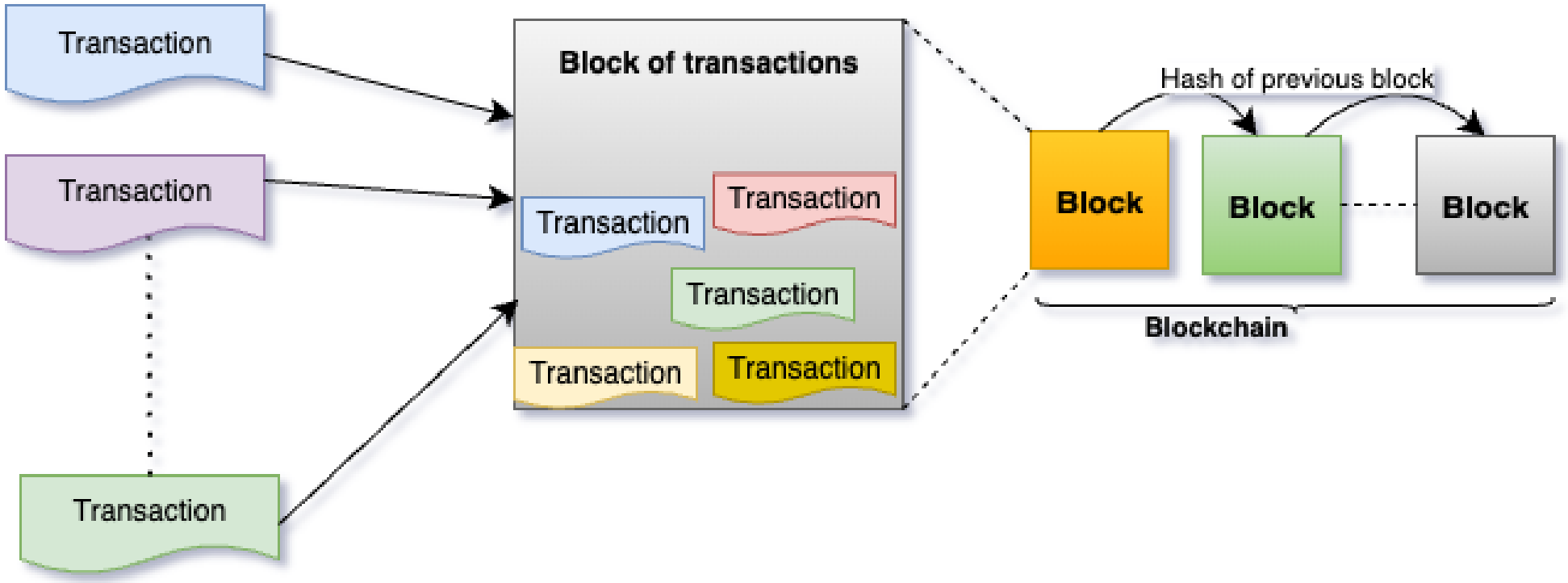
Plan for the talk

- What is a blockchain? What can it do?
- Blockchain ecosystem and its security challenges
- Subset of challenges facing participants
- Solutions to address these challenges

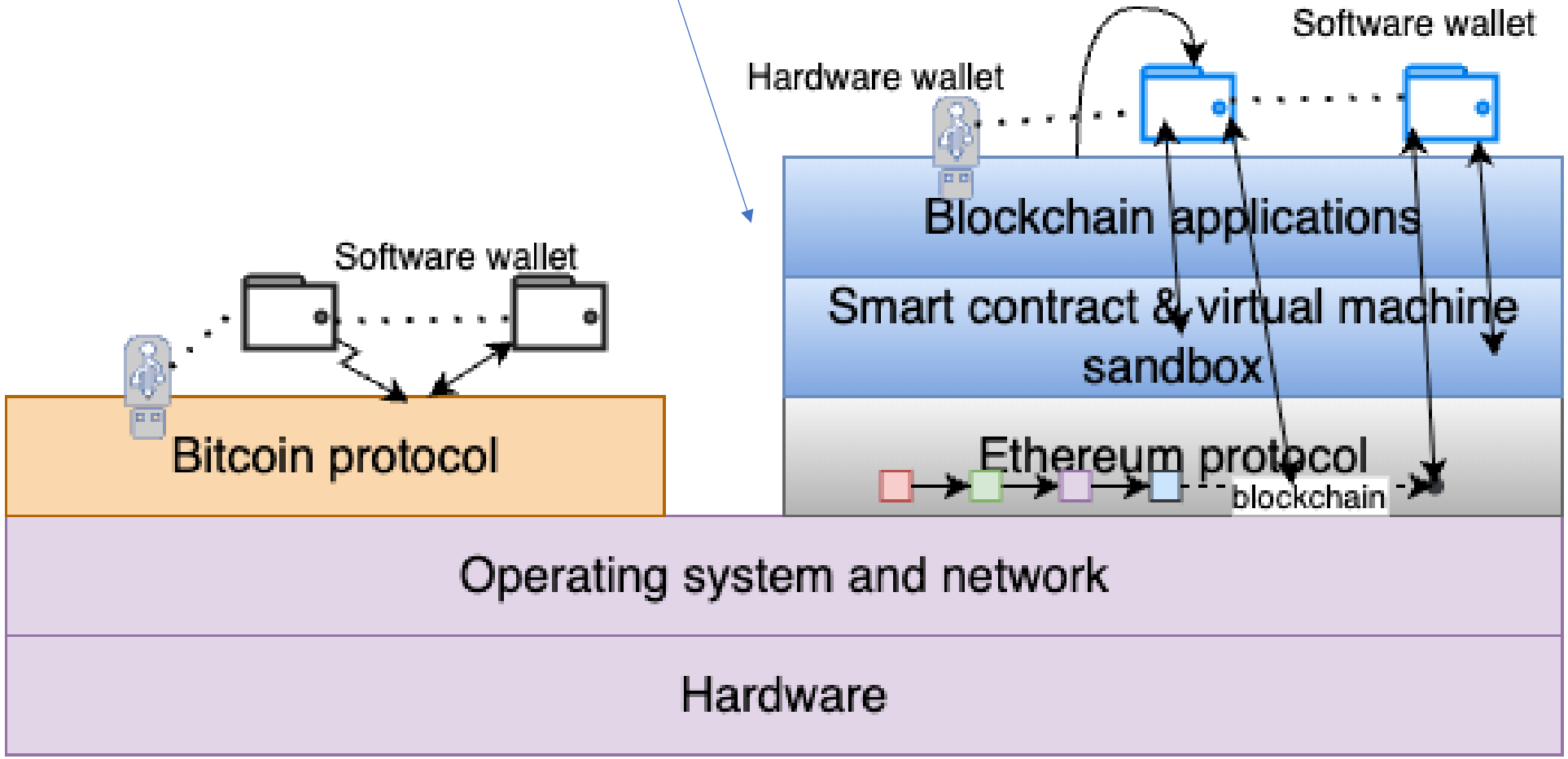
■We will discuss the above items with examples.

■My goal is to give you actionable takeaways you can use immediately.

What is a blockchain? Structurally …



Where is it stored? Here is just one node in a blockchain network of nodes.



Bitcoin[1] and Ethereum[2] are two leading blockchain protocols.

What does the blockchain do?

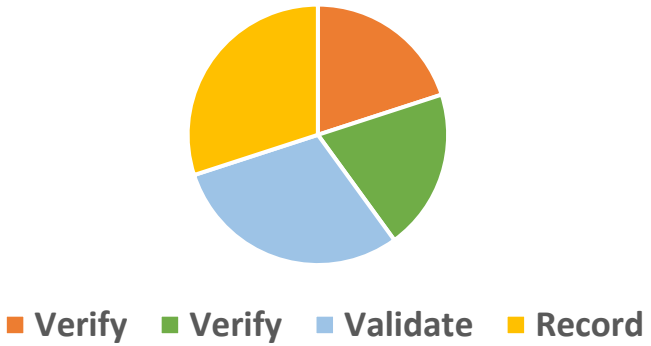
Blockchain is a **trust layer** over the Internet.

It can serve as a digital **intermediary**, much like a bank or other trusted third party.

It can enable peer-to-peer transfer of value without an intermediary.

How to establish **trust?** Consider Hotel check in:

1. You arrive at the check-in counter. Show your ID.
2. You show your reservation.
3. Then you provide your credit card.



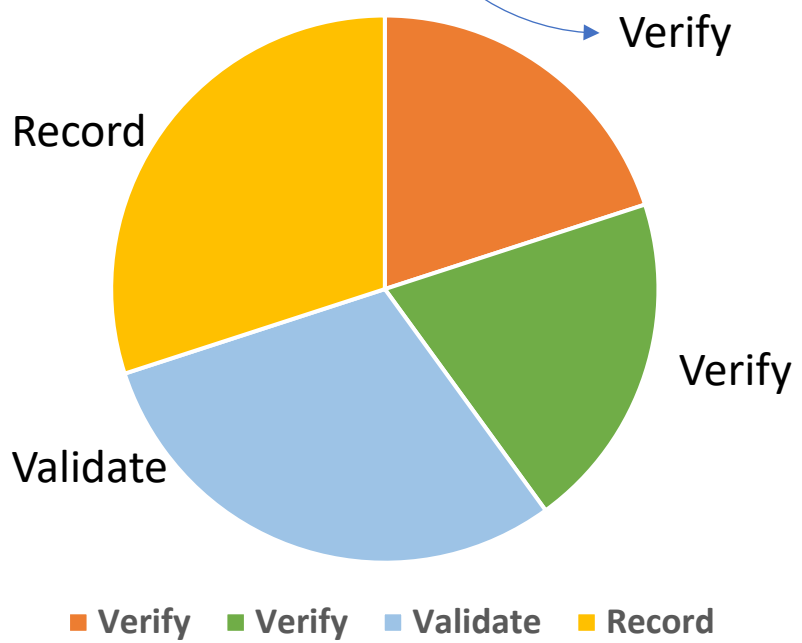
1. Check-in clerk VERIFIES the ID.

2. Check in clerk VERIFIES the reservation by looking it up on a database or ledger.
3. The clerk VALIDATEs the credit card and RECORDs it in the database or the ledger for the payment.
4. Hands the keys and shows you to your room.

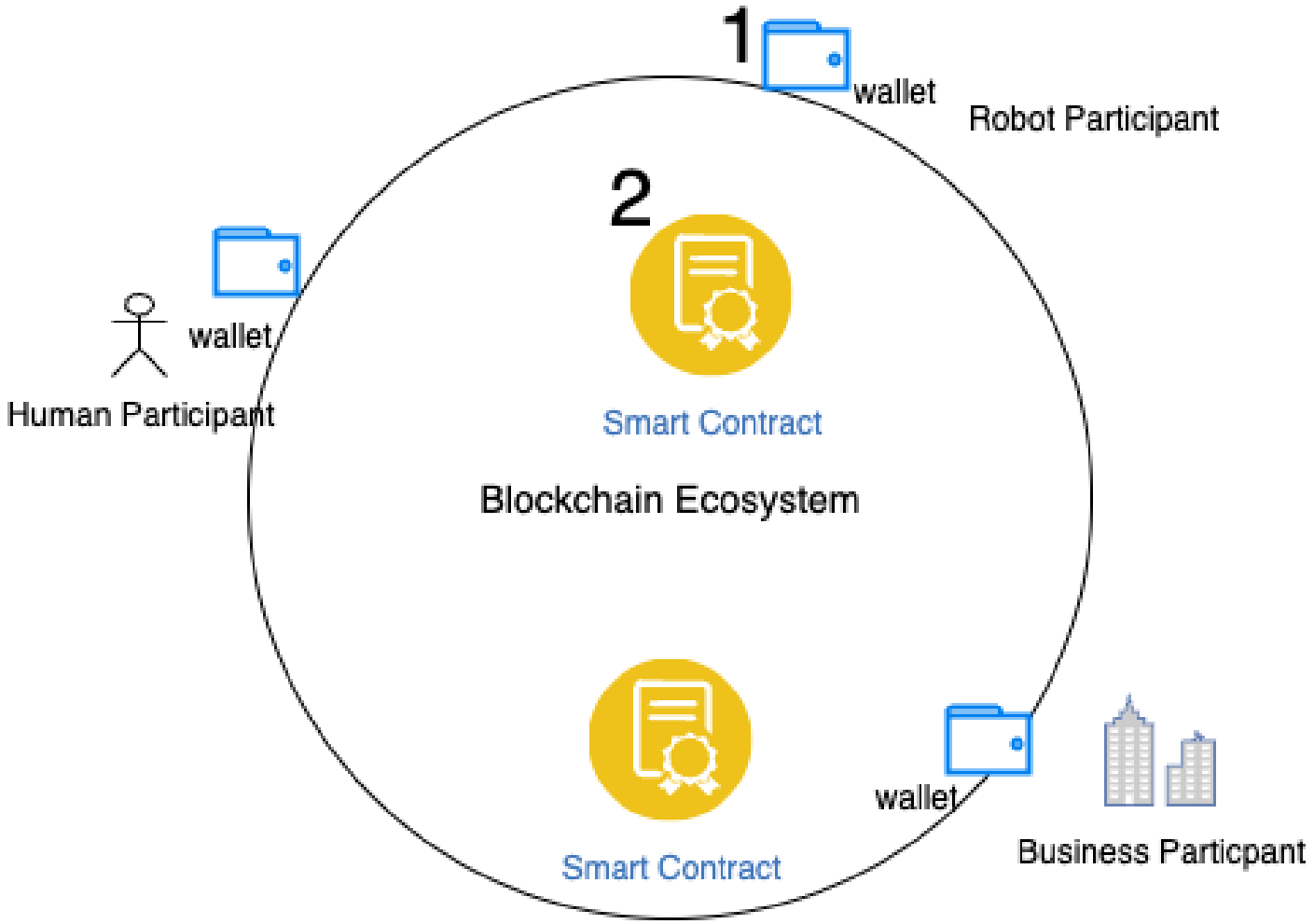
Trust Intermediation

Blockchain does trust intermediation
through verification, validation, and immutable recording.

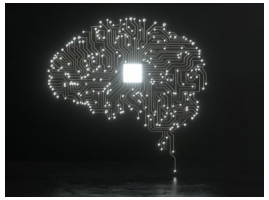
That's what a blockchain protocol
and distributed ledger do.



Security Risk Analysis: Now Consider blockchain ecosystem.



Why wallets? Wallets hold the ”keys to the kingdom” --- The private keys defining your account numbers!



Why smart contracts? They are the “brain or the control center” enforcing rules, policies and regulations.

Security Challenges

- Security challenges exists at various levels of the blockchain stack.
- User level
- **Wallet level**
- Application level
- **Smart contract level**
- Protocol level : Consensus

Wallet Artifacts (software wallet)

- A software wallet uses **cryptographic algorithms** to generate secure accounts.
- It connects to **blockchain networks** (recall it is portal or entry point to the blockchain networks)

It has:

- Accounts: accounts identified by **account numbers** or decentralized identifiers (DeIDs)
- Each account has a **balance** of cryptocurrency
- User specified **password** to lock the wallet
- Each account has underlying **private key** and public key (key-pair cryptography)
- **Secret recovery phrase** to generate, regenerate and recover a wallet.

Blockchain Wallet Security Challenges

- Here are some important practical challenges:

1. It is a **self-custody** wallet: you install it, you generate its account numbers and manage their balances.
2. You set the wallet **password** that you will have to remember and recall. There is no "central" authority that can resend the password information.
3. There is a **secret recovery phrase** (of 12 words for Ethereum) that can be used to repopulate/ regenerate the wallet if you forget the password.
4. Wallet has the **private keys** of the accounts, and these keys must be secured. If you give away the private key of an account, the account may be compromised.

39% of fraudulent loss[3] is due to phishing attacks for private keys or recovery phrase.

Wallet security Solutions

- Now you have/know about 4 items of a wallet: account number, **password, secret recovery phrase, and private keys.**
- You can give the account number to anyone if they need it. This may be to transact with you.
- You create the wallet password and must keep it secure. If you forget your password, you can regenerate the wallet using your secret recovery phrase and set a new password. However, if you lose the secret recovery phrase, **your wallet and its contents are lost forever.**
- Every wallet has a cryptographically generated secret recovery phrase that serves as its master key—never share this phrase with anyone or store it in your code.

Wallet Security

- You as a decentralized participant is responsible for the security of the ”password” , “secret recovery phrase” and the “private keys”.
- And “self-custody” of these wallet artifacts.
  - For the security of the wallet do not reveal these items to others.

- Here is my crypto wallet that I have using since 2017. My DeID is 0x3e6937bb87A66E3A4DbE5488A4863f5b29674cC3 and on Ethereum Namespace (ENS): bina.eth

But …that’s all I am going to tell you ;-)

Blockchain Smart Contract Security Challenges

- Securing a smart contract is much more complex.
- Let’s begin by understanding what is a smart contract.
- It is a piece of code.
- A smart contract code defines (i) data and (ii) functions.
- It is NOT compute-intensive code: but it codifies policies and rules.
- So, it is a gatekeeper, whereas a wallet is a gate!
- It is the “brain” or the “control center” of blockchain applications.
- Challenge: it is a piece of code: it can have bugs like any other code, it can be written to be malicious, it can result in “rug pulls”. It is immutable once deployed.
- So how to address smart contract security problem?

Smart contract Security Solutions

- Code only what is needed – lean coding techniques.
- No dynamic or large data structures. …
- Smart contract has an address and can hold cryptocurrency balance and transfer it – be aware of this feature.

- **Focus on secure coding practices**.
- **Security audits** of smart contract help in checking the code if it does what it is expected to do. This is a big industry now.

    - Especially, Check the crypto transfer functions within it and the policies controlling them.

Summary

- We learned about the blockchain structure, its purpose and functions.
- We reviewed security from a participant point of view: at a high level.
- We examined wallet level and smart control level security.
- Depending on the level of the blockchain stack you are interested in, please explore the references provided.
- Understand how to secure your wallets, participate in network decisions, and protect your digital assets.

Key takeaways for users: Safeguard private keys as the primary access credentials and thoroughly audit smart contract code that serves as the operational backbone of blockchain systems.

References

1. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.
2. https://www.bankless.com/read/the-secs-project-crypto-is-uniquely-bullish-ethereum
3. https://www.certik.com/resources/blog/hack3d-the-web3-security-report-2024
4. B. Ramamurthy and K. Madurai. (2025). World Scientific Publishers. https://www.worldscientific.com/worldscibooks/10.1142/12818
5. B. Ramamurthy.(2020) Blockchain in Action, Manning Publications.

Wallet and Smart Contract Details

- I have a full chapter describing wallet details in my recent book: Blockchain, Cryptocurrency, and Decentralized Finance[4].