Government Blockchain Association

Blockchain Consulting Series Course Handbook

Education & Training Working Group

Version: 1.0 (Baseline)
2018-07-10

1 Introduction

1.1 Purpose and scope of this Document

The purpose of this document is to guide course designers and instructors when developing GBA compliant training materials and assessment tools to facilitate GBA training certifications.

1.2 Distribution

This document is intended to be shared with the Education & Training Working Group and GBA Authorized instructors. Members of this community include blockchain experts from around the world and in many different industries.

1.3 Consulting Series Course Goals

The purpose of this series of courses is to help students develop the capability to consult with organizations and be able to transform business needs into blockchain solutions. This includes helping students develop the following capabilities:

- Be able to explain the technology and the general use of blockchain technology
- Provide a detailed analysis of the different types of blockchains.
- Discuss the legal and regulatory framework related to blockchain technology.
- Discuss the architectural and technical issues that must be considered before launching a blockchain development program.
- Discuss the steps to estimate, plan, track and manage blockchain development projects.
- Discuss the application of blockchains in different industries and real-world use cases.

1.4 Course Structure

The course will be organized into learning objectives. For example for Day 1:

Module 1: Blockchain Foundations

Lesson 1: Introduce the blockchain and why it is important
Lesson 2: Provide a basic understanding of blockchain technology
Lesson 3: Discuss blockchain benefits, risks and use cases
Lesson 4: Review current real-world use and adoption of blockchain technology
Lesson 5: Introduce smart contracts
Lesson 6: Introduce data storage on blockchain

For each module, provide a module overview at the beginning of each module. Also include a module summary or takeaways.

1.5 Certifications

The GBA certification program is organized the following way:

- Blockchain Associate
  - Blockchain Foundations
- Blockchain Specialist
  - Cryptocurrency Rules & Regulations
  - Solution Architecture
- Blockchain Consultant

- Managing Blockchain Projects
- Transformative Leadership

2 Course Learning Objectives

2.1 Blockchain Foundations

The purpose of this course is to provide students with a fundamental understanding of the technology and potential use cases. The learning objectives for this course are:

- Introduce the blockchain and why it is important
- Provide a basic understanding of blockchain technology
- Discuss blockchain use cases, benefits, and risks.
- Review current real-world use and adoption of blockchain technology.
- Introduce smart contracts.
- Introduce data storage on blockchain.

They are further explained in the following sub-paragraphs.

2.1.1 Introduce the blockchain and why it is important

Explain that a blockchain is a digital ledger in which transactions are recorded chronologically and publicly. People all over the world are using blockchain based products. One of the most common use of blockchain technologies is cryptocurrencies. However, there are many other uses of blockchain technology. Ensure that the students understand what the technology is and why it enables new capabilities that were not possible before.

2.1.1.1 Blockchain is a family of protocols

Ensure that students understand why blockchain technology is different from previous protocols and why it is appropriate for the transference of value. Blockchain protocols are like internet protocols. Where the internet protocol enabled the peer-to-peer movement of information, the blockchain protocol enables the peer-to-peer movement of value.

Internet protocols such as TCP/IP and HTTP are a set of rules that all computers on the network use so that people can share information without a third party. The blockchain is a set of rules that computers use to transfer the ownership of digital assets between peers without requiring a third-party intermediary to validate or facilitate the transaction.

2.1.1.2 What is blockchain?

Students should be exposed to the basic concepts of the bitcoin blockchain as an example of "A" blockchain. They should also be informed that this is just one example. But, it is illustrative of basic blockchain attributes. The illustration should describe a bitcoin transaction and include the following sequence of events

- Transaction initiation
- Transactions bundled into a block
- Miners guess the correct nonce and receive block reward
- The amount of guessing required to find a nonce small enough is periodically calculated every so many blocks to take a regular amount of time
- The new block added to the blockchain
- The new block distributed to all the nodes on the bitcoin network

- Nodes use the rules of the blockchain to confirm it is valid

Students should be reminded that this is just an example of a popular blockchain and that there are many other variations. Other types of blockchain technologies are presented during the Blockchain Technology Course.

- In other distributed ledger technologies, transactions may not be organized in blocks
- In other distributed ledger technologies, blocks might not be regular

2.1.1.3 *Blockchain Properties*

Describe to students blockchains contain five properties. They are:

- Decentralized Systems
- Distributed ledger
- Safer & secure ecosystem
- Mining is used to validate blocks of transactions
- Transactions are immutable

2.1.1.4 *What makes this protocol so special?*

When people started to connect computers to each other (without going through a central location), the realized that they could create a network of computers. Originally, they were networked locally (LANs). Then they were networked in larger areas (WANs) and eventually these networks of networks became known as the internet. But, in the early days, people only used them for file transfers and emails. They had no idea that one day we would use them to jump into a stranger's car (Uber), drive across town and go into a stranger's house and sleep on their bed (Airbnb) and use our phones to shop, pay bills and find a spouse to marry.

What the internet did for information, the blockchain protocol will do for the transference of value. The possibilities are so enormous that at this point we can only imagine the opportunities (like they could for the internet in 1994). However, we probably have not even imagined all the possibilities.

2.1.1.5 *Blockchain components*

Students should be introduced to some basic concepts frequently used in blockchain discussions. They are:

2.1.1.5.1 Distributed Ledger Technology (DLT)

Explain to the students the relationship between distributed databases, distributed ledgers, public blockchains, consortium (Hybrid) blockchains and permissioned (Private) blockchains.

Blockchain DLT is different from a traditional database in the following ways:

Properties	**Blockchain**	**Traditional Database**
Operations	Only Insert Operations	Can perform (Create, Read, Update and Delete) C.R.U.D. operations
Replication	Full Replication of block on every peer	Master Slave Multi-Master

Consensus	Majority of peers agree on the outcome of transactions	Distributed Transactions (2 phase commit)
Invariants	Anybody can validate transactions across the network	Integrity Constraints

Other examples of distributed ledger technology include tangle, hashgraph, and hyperledger. Most of these involve organizing transactions in a web rather than a chain of blocks

2.1.1.5.2 Blockchain Types

There are three categories of blockchain engagement types. They are:

Public	Public blockchains use consensus using a method that is not controlled by any party but is instead collaboratively agreed on by all actors in the blockchain.
Consortium (Hybrid)	A consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered "partially decentralized".
Permissioned (Private)	A fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent.

2.1.1.5.3 Cryptography

Describe the difference between encryption and hashing.

Encryption is an approach that helps to keep data secure. The encrypted data is encoded or changed up to some extent before it is sent out of a network by the sender and only authorized parties can access that information. In Blockchain, this approach is useful because it simply adds more to the overall security and authenticity of blocks and helps to keep them secure.

Hash functions are valuable because they take arbitrary data and produce an output that:

- is of fixed size
- varies completely randomly
- Has as few collisions as possible, given its output size
- Is infeasible to reverse

Use the SHA-256 Hash function as an example of how cryptography is used in the bitcoin protocol. Explain that the SHA-256 Hash Function takes inputs of a variable length and converts it into a 256 bit Hexadecimal format.

Public and private keys - Using public and private keys are the core of digital signatures.

2.1.1.5.4 Consensus Algorithms

Describe what a consensus algorithm is and why it is important. Provide a listing of several consensus algorithms including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof-of-Stake (DPoS). Lightly touch on other algorithms such as: Proof-of-Capacity, Proof-of-Authority, Directed Acyclic Graphs (DAG), and Byzantine Fault Tolerance.

2.1.1.5.5 Mining

Describe blockchain mining in a proof of work system; whereby new transactions are continuously collected into a pool, hash functions with different nonce values are regularly calculated, and a block is only valid if it has a sufficiently small hash output value, which varies randomly and thus proves work was done to achieve.

Describe blockchain mining in a proof of stake system; whereby new transactions are continuously collected into a pool, coin holders may regularly and easily calculate new blocks, but only one new block at a time may be accepted, and the probability of a stakeholder successfully publishing a block is proportional to the amount of coins he/she owns.

Explain why it is so difficult (if not impossible) to alter information once it has been added to the blockchain. Explain the 51% attack.

2.1.1.6 Why is it important

Explain that blockchain technologies is important because:

- The rate of blockchain interest and application is growing rapidly
- Blockchain solutions have such a wide scope of application
- Blockchain technology could bring huge efficiencies to existing business processes by eliminating intermediaries and streamlining business processes.

2.1.2 Discuss blockchain benefits, risks and use cases

2.1.2.1 Benefits

Describe the benefits of using a blockchain solution. Describe how a blockchain solution can provide:

- Shared common view of the transaction history and status of transactions
- Security of transaction integrity
- Transparency, openness, and trust

2.1.2.2 Risks

Describe the risks of using a blockchain solution. Describe how a blockchain solution can result in the following risks

- Solutions may not be scalable
- Theft or loss of digital assets
- Legal and regulatory violations, fines, or other enforcement activity

2.1.3 Discuss ICOs, cryptocurrency creators and users

Describe what an Initial Coin Offering (ICO) is. Describe the process typically involved in an ICO. Describe

- Price and volatility issues. What impacts the price of cryptocurrencies and tokens?
- Discuss the topic of crypto economics in terms of supply, demand and governance models to manage the supply and demand of tokens and the impact on price.

2.1.3.1 Use Cases

There are three primarily uses for blockchains. They are Cryptocurrencies, Utility Tokens and Process Automation. They are briefly described below:

• Cryptocurrencies	A special kind of virtual currency that reside on existing blockchains and represent an asset or utility.
• Utility Tokens	A special kind of virtual currency that reside on existing blockchains and represent an asset or utility.
• Process Automation	The use case of blockchain technology and smart contracts to eliminate the need for middlemen to enforce contracts, verify transactions, or perform background checks. This serves as basis for fully automating the business processes and manage new technology embedded in the process.

Describe how blockchain solutions could be used to for a variety of use cases associated with GBA working groups listed here: www.gbaglobal.org/working-groups. Any use case described on the GBA slides should also be uploaded as a blog enter on the GBA website. Blogposts can be uploaded by any GBA Professional Member. All use cases on slides must have a link to the blog post on the GBA site with additional details including source information and other validating content.

2.1.4 Review current real-world use and adoption of blockchain technology

Training should include local examples of blockchain adoption. When possible, use specific companies that are GBA members. GBA Corporate Members can be found on the www.GBAglobal.org site. Specific companies can be found in domain specific directories on the site. For example:

Domain	GBA Organizational Directory
Energy	www.gbaglobal.org/organizations/categories/energy
Identity Management	www.gbaglobal.org/organizations/categories/identity-management
Records Management	https://www.gbaglobal.org/organizations/categories/records
Supply Chain Management	www.gbaglobal.org/organizations/categories/supply-chain-management

Voting	www.gbaglobal.org/organizations/categories/voting

2.1.5 Introduce smart contracts

Describe the similarities and differences between the bitcoin protocols and the Ethereum protocols. Describe what a smart contract is. Describe ow they are and potentially can be used. Also describe the risks related to the immutability of smart contracts and the importance of auditing smart contracts before they are implemented. Site some examples of smart contract use.

2.2 Cryptocurrencies Rules & Regulations

The purpose of this course is to provide students with a fundamental understanding of cryptocurrencies, rules and regulations. The learning objectives for this course are:

- Cryptocurrencies Rules & Regulations
- Introduce cryptocurrencies and how they are related to blockchain technology.
- Discuss different types and uses of cryptocurrencies.
- Discuss legislation and regulation related to cryptocurrencies.
- Discuss ICOs, cryptocurrency creators and users.

They are further explained in the following sub-paragraphs.

2.2.1 Introduce cryptocurrencies and how they are related to blockchain technology

Before someone understands cryptocurrencies, they must understand the basic components, currency and cryptography.

2.2.1.1 What is money

Explain to students what money is. This may include a brief history of money. Describe the attributes and properties that define currency. This includes:

- Medium of exchange
- Measure of value
- Standard of deferred payment
- Store of value

2.2.1.2 Cryptocurrencies and blockchains

Discuss the role and functions of wallets, exchanges and how they read from and write to a blockchain. Describe the different types of wallets and exchanges and the features, benefits and limitations of each. Include:

- Wallets (Hardware, software and hosted)
- Exchanges (distributed, private)

2.2.1.3 What are Cryptocurrencies & Tokens

Explain to students that there are many cryptocurrencies, utility tokens and blockchains. Explain how blockchain protocols, platforms and products are layered and the interrelationship between them. Explain how some blockchains have associated currencies and tokens and other blockchains do not.

2.2.2 Discuss different types and uses of cryptocurrencies.

Let students know that there are many cryptocurrencies and tokens. Show them websites and online resources to demonstrate the number, variety and market cap of cryptocurrencies and tokens. Specifically address the difference between cryptocurrencies and tokens. Describe the various uses of cryptocurrency including currency, tokens and capital formation (Initial Coin Offerings - ICOs). Discuss the platforms used to crate cryptocurrencies and tokens including the ERC-20 tokens. Provide a brief example of to create an ERC20 token.

2.2.3 Discuss legislation and regulation related to cryptocurrencies

Discuss who the major institutions, organizations and parties that impact legal and regulatory requirements. Identify what their purpose and motivation is for the types of requirements they impose.

Explain how blockchain and cryptocurrencies are impacted by the following types of legal and regulatory topics:

- Privacy (GDPR) issues
- Taxation issues
- Investment (Security & Exchange) issues
- Banking and financial regulation

Identify any specific regulatory or legal requirements related to:

- Anti-money laundering (AML
- Know your customer (KYC)
- Consumer and investor Protection
- Tax Collection
- National security

2.3 Blockchain Solution Architecture

2.3.1 Do I need a blockchain?

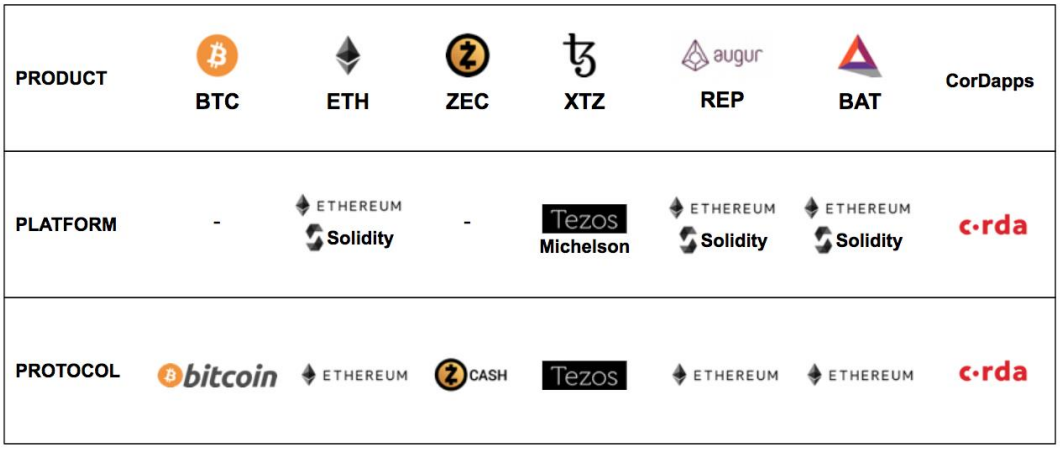
The very first question that should be addressed when considering a blockchain technology is “Do you even need a blockchain”. There are several models that help to address that question. Discuss on or more of those models. They include:

- D. Birch Model
- Birch-Brown-Parulava Model
- B. Suichies Model
- Sebastien Meunier 2017 Model

Other models may be used. The key is to provide a framework to help students understand under what conditions a blockchain is a better solution than other technologies.

2.3.2 Blockchain Solution Considerations

What decisions need to be made? Explain the difference between a protocol, platform and product. This illustration may be helpful.



Explain that there are several design considerations. They include:

- What Type
- What Protocol
- What Platform
- What Programming Language
- What Product

2.3.2.1 Blockchain Types

Describe the reasons for and against use of the various types of blockchains. They include:

- Public
- Permissioned
- Private

2.3.2.2 Protocols

Selecting the correct protocol is extremely important. Describe the following:

- What protocols are
- How protocols are they established, used, and managed. Also discuss governance (eg. forking v. centralization), and how decisions are made to change the protocol.
- Select several protocol examples from the GBA publication library at www.gbaglobal.org/resources/categories/protocols

2.3.3 Consensus Models and Trust Algorithms

Discuss some of the popular trust algorithms and describe let students know that there are a variety to choose from. Let them know that this is not an exhaustive list. Provide a brief explanation of:

- Proof of Work
- Proof of Stake
- Proof of Activity
- Proof of Burn
- Proof of Capacity
- Proof of Elapsed Time
- Proof of Integrity
- Proof of Computation
- Federation Model
- Transaction Model

- Byzantine Fault-Tolerant
- Proof of Importance

2.3.3.1 *What Platform*

Describe some of the platform choices available. Describe alternative distributed architectures including DAGs (eg Hashgraph, IOTA) and Holochains.

2.3.3.2 *Programming Languages*

Discuss the impact of selecting the appropriate programming languages. Programming languages could include C/C#/C++, JavaScript, TypeScript (which compiles to JavaScript)

Google's Go (golang), Node.JS. Python, Perl, Java, Angular, and Ruby. Discuss the impact of selecting the appropriate coding language.

2.3.3.3 *What Product (Build, Buy or Re-Use Analysis)*

Discuss some of the blockchain infrastructure products that could be used as components to new systems. For example, there are already off-the shelf products that may be integrated into ne systems and solutions. Use products that are listed in this GBA Directory: https://www.gbaglobal.org/applicationsproducts/categories/product

2.3.3.4 *Design Considerations*

Discuss how the following topics impact the blockchain solution that should be implemented.

- Flexibility with membership
- Compute equity
- Shared business interests
- Governance

2.3.4 On-Chain Vs Off-Chain Storage Options

Describe the concept of on-chain and off chain. Explain how storing large data files may be done off-chain. Describe the concept of pointing to off-chain documents and data. Discuss how it may impact performance and some of the issues and risks associated with storing information on and off the blockchain.

2.3.4.1 *Record Management*

There are two types of records on a blockchain. They are block records and transactional records. Both these records can easily be accessed, and the best thing is, it is possible to integrate them with each other without following the complex algorithms.

For example, in Bitcoin, each block includes a hash of the previous block, a hash of the transactions in the block, the nonce, and a timestamp.

2.4 Managing Blockchain Projects

2.4.1 Create a business case for a blockchain proof of concept

2.4.2 Discuss how to assess and mitigate risks related to blockchain projects

2.5 Transformative Leadership – Through Disruptive Paradigm Shifts

2.5.1 Understanding blockchain technology in the context of prior transformative technologies

2.5.2 Understanding the financial and centralized and societal impact in transitioning from a centralized power to decentralized power.

2.5.3 Develop a white paper abstract that uses blockchain technology to solve a problem

3 Acknowledgements

Special thanks to the following individuals for reviewing this document and providing meaningful feedback.

- Atul Marathe
- Gerard Dache
- Jonathan Lehman
- Randall Pires
- Robert Perry
- Bryant Neilson
- Armand Gaetan Ngueti
- Nabeel Malik