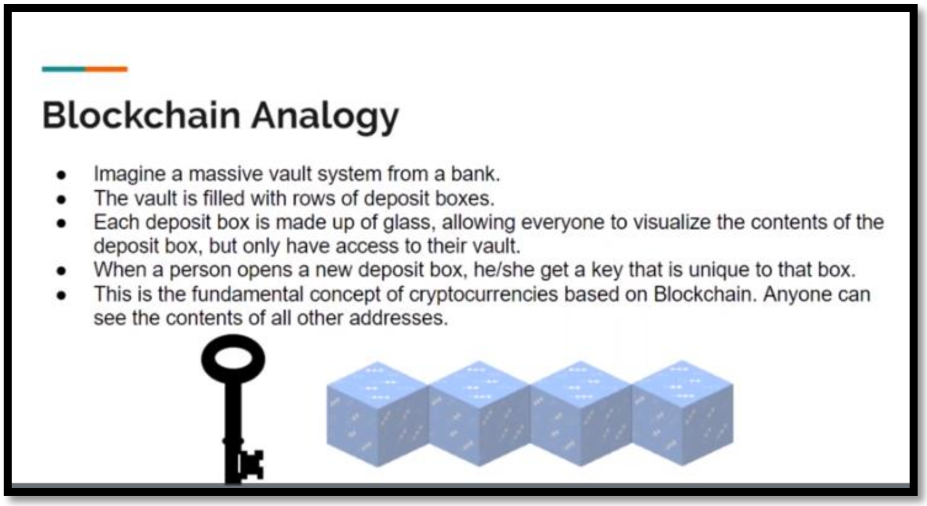
DAILY ASSESSMENT

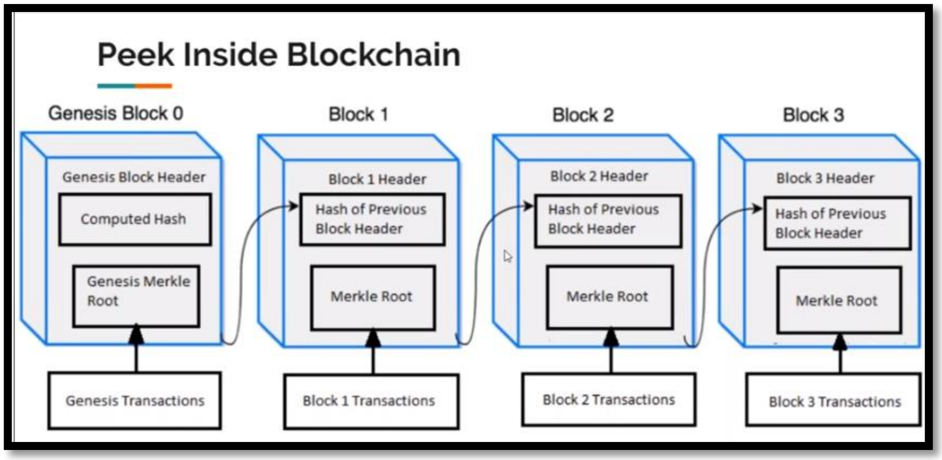
Date:	**16/06/2020**	**Name:**	**Davis S. Patel**
Course:	**Introduction to Cyber Security**	**USN:**	**4Al16EC045**
Topic:	**Block chain and cyber Security Career and industry landscape**	**Semester & Section:**	**8th- A**
GitHub Repository:	**Davis**		

FORENOON SESSION DETAILS
Image of session

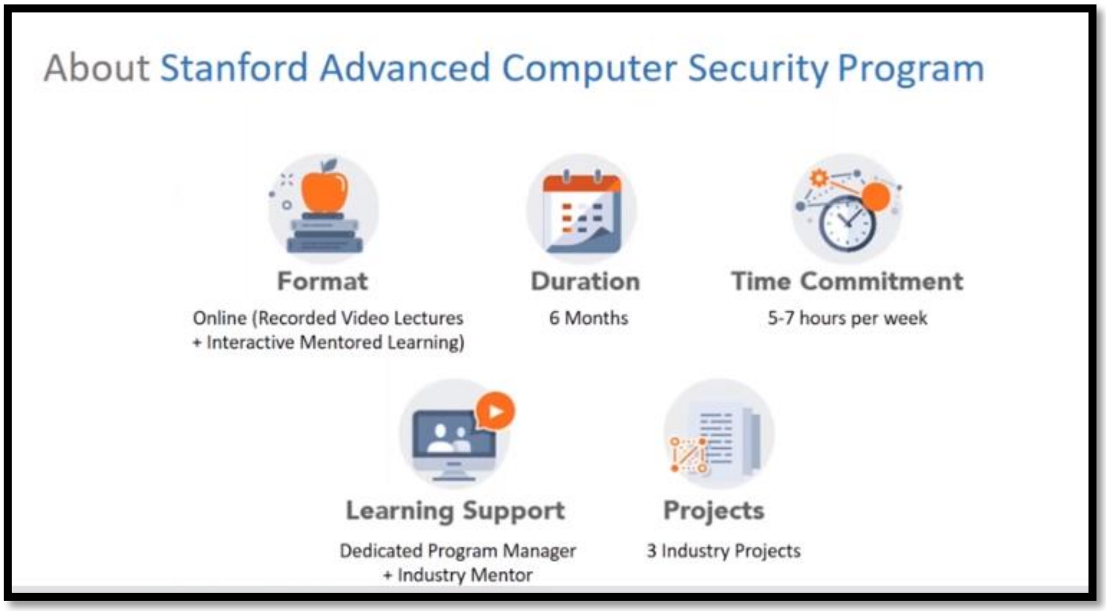


Blockchain Analogy

- Imagine a massive vault system from a bank.
- The vault is filled with rows of deposit boxes.
- Each deposit box is made up of glass, allowing everyone to visualize the contents of the deposit box, but only have access to their vault.
- When a person opens a new deposit box, he/she get a key that is unique to that box.
- This is the fundamental concept of cryptocurrencies based on Blockchain. Anyone can see the contents of all other addresses.



Peek Inside Blockchain



About Stanford Advanced Computer Security Program

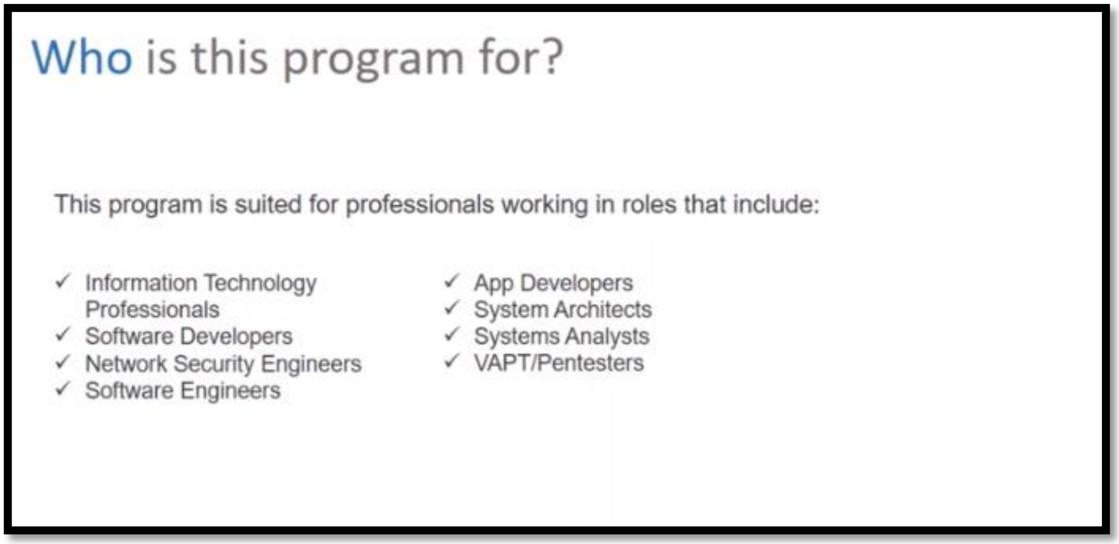
Format
Online (Recorded Video Lectures
+ Interactive Mentored Learning)

Duration
6 Months

Time Commitment
5-7 hours per week

Learning Support
Dedicated Program Manager
+ Industry Mentor

Projects
3 Industry Projects



Who is this program for?

This program is suited for professionals working in roles that include:

- ✓ Information Technology Professionals
- ✓ Software Developers
- ✓ Network Security Engineers
- ✓ Software Engineers
- ✓ App Developers
- ✓ System Architects
- ✓ Systems Analysts
- ✓ VAPT/Pentesters

REPORT –

The information age explosion of online data has brought with it lapses in security protocols that regularly expose our most sensitive information to malicious actors. Finding a reliable cybersecurity protocol, therefore, is more important than ever before. Industries across the board are latching onto new technology that promises to improve online security, including block chain.

Cybercrime is such a vast and burgeoning underworld industry that it prompted Ginni Rometty, Chairman, President and CEO of IBM, to declare that "cybercrime, by definition, is the greatest threat to every profession, every industry, and every company in the world". Both dangerous and costly, cybercrime costs individuals and businesses an estimated $500 billion a year. Our current security protocols simply cannot keep up with the relentless and clever attacks, especially when they're seemingly so simple (i.e., a phishing email to a credentialed employee can expose the data of millions).Blockchain, a Distributed Ledger Technology (DLT), is focused on creating trust in an untrusting ecosystem, making it a potentially strong cybersecurity technology.

The ledger system is decentralized, but information is transparently available to members of the specific blockchain. All members (or nodes) can record, pass along and view any transactional data that is encrypted onto their blockchain.

Blockchain's inherently decentralized nature makes it the perfect technology for cybersecurity. The ledger technology has virtually endless uses in everything from medical and financial data sharing to anti-money laundering monitoring and encrypted messaging platforms. This process creates trust while also maintaining a high level of data integrity. In essence, the distributed nature of blockchain provides no "hackable" entrance or point of failure that detrimentally exposes entire datasets.

The cybersecurity industry can benefit from Blockchain’s unique features, which create a virtually impenetrable wall between a hacker and your information. The transparent ledger allows for password-free entry. Using biometrics, including retina scans and fingerprints, the ledger can create a single-source, uncrackable form of entry into any private data. Decentralized storage ensures that each block contains only a small informational piece to a much larger puzzle, limiting hackable data to almost nothing.

Finally, blockchain’s public record keeping system gives each node an insight into any data manipulation, exposing potential cybercrime attempts in real-time. Blockchain in cybersecurity is widespread, and we've rounded up six industries that use it as a new weapon in the fight to protect our most sensitive information.

Not so long ago, information technology was the most in-demand career, and a cyber security career path was almost unheard of. As technology advanced, it brought with it sophisticated cybercrimes on a platter, literally. Due to this, the demand for information security skills is high and rising. As it is, no company, large or small, and individual is spared when it comes to cybercrimes. Cyber security has become such a concern that it tops the list among CEOs in the United States. The Bureau of Labor Statistics has established the demand rate of information security jobs to be 37% from 2012 to 2022.

Cybersecurity is one of the greatest challenges for modern enterprises, but SMEs and even larger corporations still struggle to implement the correct security strategies. As an auditor, you would take up a mid-level position and examine the effectiveness of an enterprise's current IT setup and provide a report detailing any improvements and changes required. Auditors need to evaluate factors such as regulations and compliance, as well as the efficiency and effectiveness of policies.

The Cybersecurity Analyst role ranks as the first runner-up for most in-demand security position. Cybersecurity Analysts are on the front lines of an organization's cyber defense. With the number of data breaches increasing by over 50% since last year, Cybersecurity Analysts keep constant tabs on threats and monitor their organization's network for any potential security vulnerabilities. Using information collected from threat monitoring tools and other sources, they identify, analyze, and report on events that have occurred or may occur on the network.