LearnThings.Online

Blockchain and FinTech: Basics, Applications, and Limitations

This course id from edX, scroll down & click “Read More” for more informations.

The course aims at targeting a wide audience: This course will provide learners a good understanding of the technological, applicability, limitations and “illegal” usage of the blockchain technology.

What you’ll learn

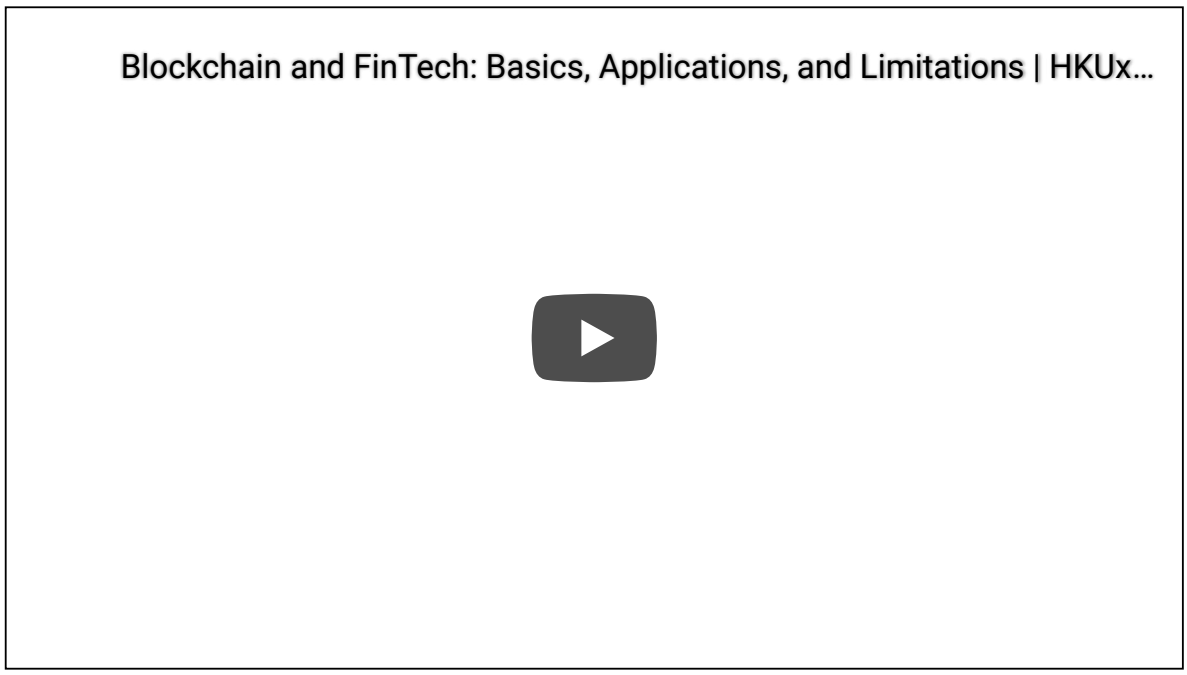
Skip What you’ll learn

- Understand the design rationale behind the blockchain technology.
- Understand the technological and cryptographic components of a blockchain.
- Understand the variations and differences of existing major blockchain platforms.
- Understand what types of applications best fit the characteristics of blockchain.
- Understand the limitations and outstanding issues of existing blockchain technology.
- Understand the negative impacts of, in particular, criminal activities in the context of blockchain.

Welcome and Course Administration

Welcome to Blockchain and FinTech: Basics, Application and Limitations

1. Hello everybody.
2. The upcoming Blockchain and FinTech course
3. will be launched in August this year.
4. It will be about blockchain technology,
5. blockchain platforms, applications and limitations.
6. This is a course aimed for layman learners.
7. Learners will be able to understand
8. the fundamental and industrial jargons,
9. so that you can interact with
10. key players of the industry.
11. I look forward to seeing you
12. in the blockchain course.
13. The big rise and crash in Bitcoin market
14. peaked peoples interest in blockchain technology.
15. But, is Bitcoin equivalent to blockchain?
16. Of course not.
17. Some even think that in the near future,
18. this new technology can change the way we live
19. and the way we do business.
20. In fact, we’ll be expecting
21. new business models
22. and new business opportunities.
23. There’ll even be new ways of
24. exchanging information online.
25. But do you know what blockchain actually is?
26. Take a look at the following questions.
27. Do you know much about these?



About this course

Blockchain is a core technology in FinTech. The original design of blockchain focused on the cryptocurrency “Bitcoin”. Due to its specific characteristics, many companies and users now find blockchain very useful for applications in many areas, not limited to cybercurrencies, including finance, logistics, insurance, medicine and even music. However, the design of blockchain involves cryptographic technology, which cannot be easily understood by those who are not professionals in the area of IT and security.

In order to better understand what kinds of applications best fit blockchain and other forms of distributed ledger technology and the potentials of these emerging technologies, it is important to understand the design rationale, the basic technology, the underlying cryptographic fundamentals, and its limitations. This 6-week online coursewill walk you through the following:

- The design rationale behind blockchain and the issues for such decentralized ledger (transaction) systems.
- The underlying technology (e.g. how the fundamental algorithms – the cryptographic primitives – work together) behind and how it makes blockchain works and safe.
- The differences of the various existing blockchain platforms and what these platforms can provide (e.g. pros and cons of the major platforms).
- What kinds of applications (both traditional and emerging) best fit the blockchain technology and how blockchain technology can benefit these applications.
- Blockchain does have its limitations. We will uncover the problems and the limitations of blockchain technology to enable developers and researchers to think about how to enhance the existing blockchain technology and practitioners to better address the issues when using blockchains in their applications.
- This course will also briefly discuss the downside of blockchain with respect to the protection of criminal activities (e.g. why ransomware always ask for bitcoins as ransom, and the money laundering problem).

28. Do you know what underlying technologies
29. make blockchain secure and powerful?
30. What kind of applications,
31. both financial related or non-financial
32. are best fit for blockchain?
33. How do these blockchain platforms differ?
34. For example, Bitcoin, Ethereum,
35. Hyperledger, Chinaledger?
36. Is blockchain 100% secure?
37. Can it protect your privacy?
38. If not, what kinds of protections are provided?
39. Why do ransomware
40. request Bitcoin as payment?
41. Why do people perceive cyber-currencies
42. as a means of money laundering?
43. If you want to get more insights,
44. join the Blockchain FinTech course.

Course Outline and Syllabus

Introduction to Blockchain and FinTech: Basics, Applications and Limitations – Course Outline

Introduction to Blockchain and FinTech: Basics, Applications and Limitations is a six-week six-module course. Each weekly module compiles 6-12 lesson units (or subsections). In addition to the main units of the lesson, there are also Industry use cases highlighting real world examples and applications from different industry sectors.

The major learning activities within each lesson unit include: video discussions of major aspects with peer learners, instructor and community TA, as well as continuous assessment in the form of Quick Check questions, Polling and Word Cloud activities. In addition to these, there are a range of additional resources provided, including blockchain industry news reports, studies and useful links. There is a Conclusion Quiz at the end of each module to draw out the main messages.

Please click the link to view and download the Course Syllabus.

Module 1 Blockchain technology: Why, What, How	
1.1.1	Why Do We Need a Decentralised Ledger System? Part 1
1.1.2	Why Do We Need a Decentralised Ledger System? Part 2
1.2	Having a Centralised Trusted Party – Advantages and Disadvantages
1.3	Security, Integrity and Privacy Issues of a Decentralized System

1.4	Blockchain – A Technology that Makes Sense with Trust and Coordination (An Interview with Charles d'Haussy from ConsenSys)
1.5	What Are the Main Barriers to Blockchain Adoption? (Charles d'Haussy from ConsenSys)
1.6	Why Use Blockchain Technology? (Henri Arslanian from PwC)
Ref	Reference Videos from Introduction to FinTech
	Introduction to FinTech Module 2.9A What is Blockchain? (Part 1)
	Introduction to FinTech Module 2.9B What is Blockchain? (Part 2)

Module 2 Technological and Cryptographic Elements in Blockchain

2.1.1	Cryptographic Elements: Public Key & Private Key
2.1.2	Cryptographic Elements: Digital Signature & Hash Value
2.1.3	Cryptographic Elements: Real-life Scenario Challenges
2.2.1	Cryptographic Technology: Key Questions for Blockchain
2.2.2	Cryptographic Technology: Who can Modify Transactions?
2.2.3	Cryptographic Technology: Who will Maintain Transactions?
2.2.4	Cryptographic Technology: How to Protect Our Privacy?
2.2.5	Public-key Cryptography (Prasanna Mathiannal from MaGEHold)

Module 3 Blockchain Platforms

3.1.1	Classification of Blockchain Platforms (Part 1) – An Overview of the 5 Key Perspectives
3.1.2	Classification of Blockchain Platforms (Part 2) – Perspectives No. 1 and 2
3.1.3	Classification of Blockchain Platforms (Part 3)

	– Perspective No. 3
3.1.4	Classification of Blockchain Platforms (Part 4) – Perspectives No. 4 and 5
3.1.5	Highlights of Major Blockchain Platforms
3.2.1	What is Ethereum? (Charles d'Haussy from ConsenSys)
3.2.2	What is Ethereum's Place in Today's FinTech Ecosystem? (Charles d'Haussy from ConsenSys)
3.4.1	Trustlessness and Immutability of Blockchain Technology (Charles d'Haussy from ConsenSys)
3.4.2	Proof of Work and Proof of Stake (Charles d'Haussy from ConsenSys)
3.5.1	Tokenizing (Charles d'Haussy from ConsenSys)
3.5.2	What is a Token? (Charles d'Haussy from ConsenSys)
3.5.3	Tokenizing Shares and Fund Raising (Charles d'Haussy from ConsenSys)
3.6	What is Hyperledger?

Module 4 Blockchain Applications

4.1.1	6 Selection Criteria for Blockchain Applications (Part 1) Key Factors 1, 2, 3
4.1.2	6 Selection Criteria for Blockchain Applications (Part 2) Key Factors 4, 5, 6
4.1.3	6 Selection Criteria for Blockchain Applications (Part 3) Best Fit Applications
4.1.4	6 Selection Criteria for Blockchain Applications (Part 4) Decision Making

4.2.0	Blockchain and Enterprise – A Technology of Coordination (Charles d'Haussy from ConsenSys)
4.3.1	Why Permissioned Blockchains Are Used in Enterprise Network? (Dr. Paul Sin, Consulting Partner from Deloitte, China)
4.3.2	Use Case: Blockchains for Trade Finance (Dr. Paul Sin, Consulting Partner from Deloitte, China)
4.3.3	Use Case: Blockchains for Supply Chain Financing (Dr. Paul Sin, Consulting Partner from Deloitte, China)
4.3.4	Use Case: Cross Border Connectivity – Trusted Data Transfer (Dr. Paul Sin, Consulting Partner from Deloitte, China)
4.4.1	How to Deploy an Application on the Ethereum Blockchain? (Charles d'Haussy from ConsenSys)
4.4.2	Use Case: Bounties Award Ethereum for Cleaning Beaches (Charles d'Haussy from ConsenSys)
4.4.3	ConsenSys and the Ethereum Platform (Charles d'Haussy from ConsenSys)
4.4.4	ConsenSys Use Case: Project i2i (Charles d'Haussy from ConsenSys)
4.5.1	Blockchain Use Case: More on Trade Finance and Supply Chain (Anil Kudalkar from MaGESpire Partners)
4.5.2	Blockchain Use Case: Capital Markets (Anil Kudalkar from MaGESpire Partners)
4.5.3	Blockchain Use Cases on General Government Services & Sustainable Livelihood (Anil Kudalkar from MaGESpire Partners)

Module 5 The Limitations, Opportunities and Challenges of Blockchain

5.1.1	5 modules in Blockchain system
5.1.2	Limitations of Blockchains (Part 1)

5.1.3	Limitations of Blockchains (Part 2)
5.2.1	Risks and Limitations of Blockchain: Privacy (Malcolm Wright from Diginex)
5.2.2	Risks and Limitations of Blockchain: Security (Malcolm Wright from Diginex)
5.2.3	The Five Security Risks of Blockchain (Alan Cheung from Hong Kong Applied Science and Technology Research Institute (Astri))
5.3.1	Applied Smart Contracts: Opportunities, Risks, and Applications for Enterprise (Jon Rout from Digital Asset)
5.3.2	Applied Smart Contracts (DAML): Step-by-Step Example (Jon Rout from Digital Asset)
5.4.1	Use Case: Blockchain for Health Insurance (Alan Cheung from Hong Kong Applied Science and Technology Research Institute (Astri))
5.4.2	Use Case: Blockchain & PropTech (Alan Cheung from Hong Kong Applied Science and Technology Research Institute (Astri))
5.4.3	What Are the Benefits of Blockchain in Banking? (Johnny Cheung from B.C. Holdings)
5.4.4	How Can Blockchain Technology Benefit the Healthcare Industry? (Johnny Cheung from B.C. Holdings)
5.4.5	Institutional Investment Opportunities in the Digital Asset Space (Henri Arslanian from PwC)
5.5.1	Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 1) (Brian Tang from Asia Capital Markets Institute (ACMI))
5.5.2	Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 2) (Brian Tang from Asia Capital Markets Institute (ACMI))

5.5.3	Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 3) (Brian Tang from Asia Capital Markets Institute (ACMI))
5.5.4	Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 4) (Brian Tang from Asia Capital Markets Institute (ACMI))

Module 6 The "Evil Sides" of Blockchain and Legal Regulations for Blockchain

6.1.1	The Evil Sides of Blockchains Part 1 Ransomware
6.1.2	The Evil Sides of Blockchains Part 2: Money Laundering
6.1.3	The Evil Sides of Blockchains Part 3: Cyber Currencies
6.1.4	The Evil Sides of Blockchains Part 4 Cyber Security Exchanges
6.2	The "Dark" Side of Blockchain (Bowie Lau from MaGESPire)
6.3	Criminal Use of Payment Blockchains (Malcolm Wright from Diginex)
6.4	The Role of Financial Regulations for Blockchain (Professor Douglas Arner, Faculty of Law at the University of Hong Kong)
6.5	Does Blockchain Need Legal Regulations? (An Interview with Charles d'Haussy)
6.6	Global Digital Assets Regulatory Trends (Henri Arslanian from PwC)

Module 1 Blockchain Technology: Why, What and How

Welcome to Module 1

Meet Module 1 Guest Speakers

Guest Speakers in this Module

Charles d'Haussy

Director Strategic Initiatives, Consensys

"The main barriers to blockchain adoption today would be defining and launching the right products. Everyone is experimenting a lot on this ecosystem…"

Henri Arslanian

FinTech & Crypto Leader, Asia, PwC

"Imagine if you're able to put your identity on the blockchain, and then you can let people access it as you want it or not. If you want to send money back home, or supply chains, smart contracts, trade finance, the list goes on and on."

Module 1 Learning Objectives

After completing Module 1, learners should be able to:

- Understand the differences between a distributed system and a decentralised system;
- Understand the advantages and disadvantages of having a centralised trusted party to process and store transaction data of an application;
- Understand the advantages and issues to be resolved of a decentralised system.

Think about this

Think about this ...

Do you know the difference between a “decentralised” and “distributed” systems?

Why do we need a decentralised ledger?

Why Do We Need a Decentralised Ledger System? (Part 1)

1. Before we start,
2. there are two terms I want to clarify.
3. You always see these terms in the internet.
4. One is called decentralised system.
5. The other is distributed system.
6. Distributed system actually refers to
7. a system that can store or process data
8. in different locations.
9. But whether it is a decentralised system,
10. depends on how and where
11. the decision making is made.
12. Decentralised essentially means
13. there’s no single point or single party
14. who can make the final decision
15. of how the system behaves.
16. So, every party can make a decision
17. for its own behaviour,
18. and the resulting behaviour of the whole system
19. will be the aggregate responses
20. from the individual parties.
21. Simply speaking, decentralised means
22. that there’s no single authority
23. who can control or decide what the system should do.
24. In contrast, you can imagine Google search engine
25. is basically a distributed system,
26. but is not decentralised.
27. It still relies on thousands of computers
28. in different locations to check the web,
29. to crawl the web
30. from different locations of the world,
31. but then the whole system is owned
32. and controlled by Google.

33. So, in other words, Google is the only organisation,
34. only party who can control the whole system.
35. So, that's why it's not qualified
36. as a decentralised system.
37. Now, then the immediate follow-up question is:
38. Why do we need a decentralised ledger system?
39. Before I talk about this,
40. let's look at the history.
41. Let's start at the very beginning.
42. Why do we need banks?
43. We need banks because we need a trusted organisation
44. to help us to store our money.
45. Otherwise, it's really dangerous
46. to keep our money at home.
47. The bank, as a centralised trust party,
48. will keep track of all our money accounts
49. of all the customers.
50. In other words, the bank will keep a centralised ledger
51. for all these accounts.
52. And the bank is the only one who is responsible
53. for the integrity and validity,
54. that is, the correctness of all the transactions
55. in these accounts.
56. Let me give you an example.
57. If a Person A wants to transfer $100
58. to a Person B, the bank will try to track
59. if A has enough money in his bank account
60. before allowing the transaction.
61. And of course, the bank will also try to mark down
62. this transaction clearly in the ledger if it's completed.
63. And both the party A and B
64. will not have any worry about if the transaction is faked
65. because we all trust the bank.
66. Now but then, why the bank is willing to do this for us?
67. The bank can actually make use of our money
68. to invest and try to earn more money on their own.
69. That's why they are willing to provide this service for us.
70. Now, in order to attract more customers
71. to deposit the money in the bank,
72. the bank will give the customers interest in return.
73. So, it is basically the relationship
74. between the customer and the bank.
75. So far so good, right?
76. The customer right now has a trusted party, the bank,
77. to help handle his money account
78. with the benefit of getting interest as well.
79. Now, on the other hand, the bank can make use of

80. the customer's money to make more money.
81. As time went by, the services or the funds
82. of the bank has evolved a lot.
83. If you look at the current situation,
84. there're many, many services
85. provided by the bank now,
86. for example, bank loans, money exchange,
87. inter-bank transfer, electronic money transfer,
88. auto pay or even investment.
89. So, it seems like we are having
90. such a centralised authority,
91. it's very good.
92. However, let's now take a closer look at this
93. to see if it's really that good
94. to have a centralised party helping us
95. with all these transactions.

1.1.2 Why Do We Need a Decentralised Ledger System? (Part 2)

1. First, you all know that
2. these services may not come for free.
3. We probably have to pay transaction fees.
4. For example, is some countries we need to pay charges
5. when we are using ATM transactions,
6. cashier's cheques, money orders, bounced cheques
7. wire transfer, safety box, investment transaction,
8. or even they impose a minimum balance in the account,
9. otherwise, you have to pay a charge.
10. Pick the wire transfer as an example.
11. If you have a son studying abroad in the U.S.,
12. you want to send him some money
13. from Hong Kong to the U.S.
14. both the banks in Hong Kong and the U.S.
15. will charge you a transaction fee.
16. They may also have minimum
17. or maximum requirements
18. on the amount of money that can be transferred.
19. Now, having a middle man,
20. a trusted centralised party
21. for transactions and business is not uncommon
22. in the real world.
23. There are many, many examples.
24. Now, let's try to look at a few.
25. In China, there's a place called Guiyang.
26. They established something called
27. the Global Big Data Exchange.
28. This exchange has been established

29. for three years already.
30. It provides a centralised platform for the customer
31. to trade, buy and sell the data.
32. So, basically it's a data trading centre.
33. How it works, the data owners deposit their data
34. into the platform just like what we do for the bank.
35. We deposit the money in the bank.
36. And the buyers could go to the platform
37. and try to purchase the selected data from the platform,
38. based on what data are provided by the data owner
39. and what data will be required by the buyers.
40. And the centralised party,
41. the platform, will try to coordinate
42. this buying and selling activities or provide services
43. to help match the buyers and sellers.
44. You all know it, right?
45. Of course, the service is not for free.
46. The platform charges a transaction fee.
47. The transaction fee can be as high as
48. 40% of the whole transaction amount.
49. For example, if you are going to pay $1,000
50. to buy and sell data,
51. you are going to pay $400 to the platform.
52. Now this is only one example.
53. There are many, many other examples.
54. Let me give you another remarkable example.
55. Matchmaking service is very common now.
56. You can see that the company,
57. the platform providing this service,
58. can be considered as our centralised trusted party,
59. and of course the service is not for free.
60. To use the service,
61. to find the potential dating partners or candidates,
62. in most cases,
63. a customer has to pay membership fee
64. and, if they successfully arrange a dinner
65. for you and the potential candidate,
66. they may even charge you another service charge.
67. Think about it.
68. If it's possible to eliminate the centralised party,
69. we may not need to pay this transaction fee.
70. Now, in fact, having a centralised party
71. to look after our transaction
72. also comes with the privacy issues.
73. It's very obvious that
74. the bank, the centralised party, the platform,
75. is able to look at all your transactions.

76. For example, to whom you want to give your money to,
77. how much money you have exchanged
78. for foreign currencies,
79. how much money you have wired to your children,
80. and of course, all of your investment via the bank.
81. If you look at the love matching example,
82. the privacy issue is quite obvious, right?
83. Because you need to pass your personal information
84. to the platform and also the criteria
85. for choosing your partner, for example,
86. what kind of girls you like, etc, and of the privacy,
87. you totally rely on the service provider.
88. And this service provider
89. will have full access to the information,
90. which couples have communicated
91. and when and where they go for dinner
92. and who want to date which one.
93. And, of course, you may not even want others to know
94. that you have register for this kind of service.
95. And for the big data exchange example,
96. there are also some privacy issues.
97. The platform, because you deposit your data over there,
98. so the platform has all the authority
99. to look at every single piece of data,
100. and there is no absolute guarantee
101. that the platform will not use your data
102. for other purposes.
103. And, of course, the platform also know
104. every single transaction of every trade,
105. who buys a piece of data, who sells it, who owns it
106. or for how much the data was sold.
107. Sometimes, time is also a concern
108. because we have to rely on the centralised party
109. to process the transaction.
110. In most of the cases, it will take time.
111. For example, if you want do a wire transfer
112. to someone in another country,
113. it may take the bank days to complete the transaction.
114. And the bank probably may also have other restrictions,
115. for example, they may have a restriction
116. on the minimum or maximum amount
117. that you can transfer for one time.
118. And depending on the nature of the transaction
119. and/or the applications,
120. some transactions may involve multiple parties
121. and many steps in the procedures.
122. As a simple example,

123. let's consider a mortgage loan.
124. From the time you want to apply for a mortgage loan
125. till you really get the mortgage loan,
126. maybe you have the experience.
127. It will take more than 20 days, or a few weeks, right?
128. In fact, inside this process,
129. there are many parties to be involved.
130. For example, the borrowers need to work with
131. different parties to provide proofs of his salary,
132. his employment, his credit history, etc,
133. And the bank may also need to work with
134. many other parties, for example, surveyors
135. to evaluate the property for the loan
136. based on the current market price.
137. And the bank may also need to
138. interact with other parties,
139. such as the land registry
140. to verify the ownership of the property.
141. Then, you can imagine that
142. everything goes back to the centralised party,
143. that's the bank in our case,
144. then it would become the bottleneck of the procedure.
145. And, of course, if you want to look for a mortgage loan,
146. you are not going to ask a single bank to do it.
147. Usually we try to seek services
148. or make enquiries from multiple banks.
149. And of course the banks will not work together.
150. They will not share information at all.
151. So, it creates a lot of redundancy
152. in the transactions as well.
153. Now, you think about it.
154. Imagine that if there's a platform in which
155. some information is given access to every bank
156. if the customer agrees,
157. the validation process of opening a bank account
158. in different banks for the same customer
159. would be a lot easier,
160. and you can save a lot of time.
161. But if we are having the concept
162. of a centralised system,
163. this platform is not easy to build
164. because no one is going to trust one single authority
165. who have full control of this platform
166. with the exception of the government.
167. In other words,
168. it's not easy to have a commonly trusted party
169. to manage the operation of the system.

170. If you can follow what we have discussed so far,
171. you may wonder is it possible to do all these
172. without a centralised party?
173. For example, without a bank,
174. you know, this is the reason why blockchain
175. or a decentralised ledger system was proposed.
176. But on the other hand,
177. not all applications or systems are suitable to be a kind.
178. We've also discussed what kind of applications
179. are best fit for decentralised systems
180. in the later part of the course.

Think about this

Banking transactions demand adequate security. What are the advantages and disadvantages of a centralised and decentralised system in bank services such as payment and remittance?

1.2 Having a Centralised Trusted Party – Advantages and Disadvantages

1. I hope you are now convinced
2. why we need a decentralised system.
3. However, a decentralised system
4. is not owned by anyone
5. but by all the users who use the system,
6. so in other words
7. all the users of the system
8. have to work together
9. to maintain the whole system
10. so the big question is,
11. is it really feasible?
12. What will be the issues there?
13. To understand the issues
14. of building a decentralised system
15. for an application,
16. let's try to look at the bank accounts
17. as an example.
18. Now assume that
19. we have already opened an account in a bank.
20. We have mentioned that the bank can help us
21. to maintain our account ledgers,
22. deposit money into the account,
23. withdraw money from the account

24. and transfer some money from one account
25. to another account.
26. Now imagine that I try to deposit 15 coins
27. into my own account.
28. The bank provides you a deposit slip
29. and the account balance is recorded.
30. Now on the other hand,
31. if you do not have a bank,
32. how can you confirm
33. that you have actually deposit 15 coins
34. into the account?
35. Another example.
36. If Bob wants to transfer 10 coins to David
37. with a bank, you can sign a transfer slip
38. to authorise it and both you and Bob
39. has no doubt about the transfer.
40. The bank has processed it.
41. However, if we don't have a bank,
42. how can one authorise the transfer?
43. How can one check if the transaction is valid?
44. In other words,
45. how can we guarantee that Bob
46. has 10 coins in the account
47. so that he can transfer the coins to David?
48. Now with a centralised party,
49. the bank will keep track
50. of all transactions for its customers
51. and account balance for its customers,
52. so if one person wants to transfer
53. a certain amount to another account,
54. the bank will verify if the person
55. has enough money to do so or not,
56. but then if you're without a bank,
57. without a centralised party,
58. how can this be done?
59. One simple solution is
60. how about we just put
61. all the transaction details,
62. all our accounts on the internet.
63. Then everybody can get a copy
64. and help to check it.
65. Now if A wants to transfer $60 to B,
66. then everybody can see whether A has enough money
67. in the account
68. and whether the transfer can be done legitimately
69. and of course now that the transaction has been done,
70. a new record of the transaction can be written

on the internet-based ledger as well.
Then both A and B can see clearly the changes
in the account and the transaction can be done
very fast too.
Since we put all the details
of all the transactions and the accounts on the internet
so everybody can check it
and all actions are transparent, am I right?
But the problem is in the bank,
the bank will be responsible for all the accounts,
all the transactions.
More importantly the transaction details
and the accounts are kept by the bank
and the bank can make sure
that nobody, no unauthorised people
can modify the transaction
or the account can easily be changed.
But now the whole ledger is available
in the internet, everybody is authorised
has the right to download a copy,
so can anybody modify the transaction easily?
Do we have a mechanism to make sure
that this is not possible?
Or can anyone add/delete transactions easily?
How to give the authorization
to transfer money from your account
to another account,
who actually is responsible to maintain the account?
Maintain the ledger?
Who's going to check the validity of a transaction?
You see there are many, many problems.

1.3 Security, Integrity and Privacy Issues of a Decentralised System

Now, let's try to talk about the issues in more detail.
To make it very simple, if it's very easy for one
to modify the transaction details,
then the system becomes useless
because we cannot trust
the ledger that we download from the internet.
For example, if I transfer $10 to B today,
but then, tomorrow, I don't want to transfer
the money to B, so what can I do?
I go to the internet,
download the ledger, erase my record,
or even say that B actually transferred $6 to me instead.
Then, I put the ledger back in the internet.

14. Then, everybody will download my new ledger
15. and think that B actually transferred
16. $6 to me instead of I transfer $10 to B.
17. Then, you can see that the system becomes useless.
18. Nobody's going to trust it.
19. So how to guarantee that only the account owner
20. can initiate a transaction of his own money?
21. This is actually a security issue.
22. Now, if it cannot guarantee
23. the transactions are error-free,
24. for example, if the transaction is transferred
25. even if the paying account
26. does not have enough money,
27. then we will think that the system is useless as well.
28. Therefore, you can imagine that integrity
29. is really, really a big issue.
30. So whether we can trust the transaction detail
31. on the internet is of question.
32. Now, of course,
33. you can see that with a centralised system,
34. the bank can check every transaction,
35. whether it's valid or not, but in a decentralised system,
36. everybody's an owner.
37. We don't know who is going to check
38. if the transaction is valid.
39. This is also an integrity issue.
40. Now, if the ledger is maintained
41. by all users, so everybody may get a copy.
42. So if some problems occur,
43. which copy is the correct one?
44. Which copy can we trust?
45. You can see that there are many, many questions
46. related to security and integrity.
47. In fact, who is responsible for adding new transactions
48. into this global ledger is also an issue,
49. is also a problem.
50. Now, if you look at it very carefully,
51. there's one more important question.
52. If you put everything on the internet,
53. every transaction on the internet,
54. so everybody can have the authority to look
55. at all the details, all the accounts, all the transactions,
56. as they are all the owners of the platform,
57. then it seems like the protection of privacy
58. in comparison to a bank is even worse.
59. You think about it.
60. In case of a bank, only the bank can look

61. at all the transactions for its customers,
62. but in a decentralised system,
63. it seems like everybody can
64. go to the blockchain platform
65. and look at all the transactions.
66. Now, I hope you learned enough to understand that if
67. we are going to have a decentralised system,
68. there are many, many issues to be resolved.
69. Okay, let me summarise the lecture of this module.
70. Now, if we are going to have a centralised party,
71. like a bank, to help us to keep our money,
72. there are some disadvantages,
73. such as we need to pay high transaction fee,
74. the privacy concern because the bank
75. can know everything about us, about the transactions,
76. and also the processing time
77. may depend on the centralised party,
78. and if we are going for multiple parties,
79. multiple service providers, you may need to repeat
80. the same tedious procedures for every provider
81. because they don't share information.
82. Now, on the other hand,
83. if we try to go for a distributed ledger,
84. the ledger is going to be maintained by all users
85. and we may have other concerns
86. to maintain the system,
87. such as security, integrity, and a privacy issue.
88. Now, in the next lecture, we'll try to take a closer look
89. at the blockchain technology
90. on how these issues can be resolved.

Meet Guest Instructor Charles d'Haussy (ConsenSys)

1.4 Blockchain – A Technology that Makes Sense with Trust and Coordination (An Interview with Charles d'Haussy from ConsenSys)

1. I would like to give you my definition of blockchain,
2. because blockchain is a very complex technology
3. and it makes it a very difficult technology
4. to explain sometime.
5. So, some people go in the technical explanations,
6. explaining to user,
7. there's a distributed ledger infrastructure
8. as information is shared.
9. But when you talk to a large audience,

it's actually hard for the people to start to picture
what is this flow of information.
So the way I like to explain,
what is blockchain technology,
is really to explain that
it is a technology about coordination.
It's a technology helping people,
helping organisations to organise themselves
in a trustless manner.
And if you're a technical person,
we can talk about the ledger,
as in the way the information is encrypted
and shared between different databases.
But the overall takeaway,
it's a technology which never exists before,
and it's a technology which main objective
is to help coordination.
So the worst case of blockchain
is trying to use blockchain
for the sake of using blockchain,
for every use case you want to address,
you can always execute them
without using blockchain.
A central database is always possible.
But if you want start to coordinate work
between many, many more parties,
and you want these parties to have a platform
which is a trust.
So they don't have to trust one single player,
but they can start to trust each other,
then blockchain start to make sense.
So I think a blockchain which is centralising things,
but still using the blockchain
for distributing things
do not capture all the value proposition
of the blockchain technology.
So you really want to have a use case
where there is so many different parties
with such a complex coordination work
that a blockchain will actually makes sense
because it will be easy
for the platform to onboard them,
and it will be also making everyone comfortable
to work that if you claim something
or if you owe me something
because I deliver your work,
the platform is actually coordinating this work,

57. and I do not need to have such a high level
58. of trust with you, if I deliver a work,
59. if I deliver something to you,
60. I knew I'm going to be paid
61. because I will trust the platform itself.
62. So to speak, to the idea of having a distributed ledger
63. or blockchain being distributed,
64. what's decentralisation and does it matter
65. if a blockchain is decentralised or not?
66. So, decentralisation is one of the value proposition
67. of the blockchain's technologies, right?
68. In some cases you want to decentralise
69. between a short, a small group of players,
70. maybe between a bank and their customers,
71. maybe between different banks
72. or maybe different organisations.
73. In this case, you decentralise,
74. but you kind of not totally decentralise.
75. So it should not be an obsession.
76. Decentralisation makes sense,
77. but it should not be the only obsession.
78. I think we always have to come back to the problem
79. you want to fix.
80. You want to come back
81. if you design a product
82. to make sure that this product has a fit
83. with the market and start your kind
84. of product design journey from the customer
85. and not from the technology capacities.

What Are the Main Barriers to Blockchain Adoption? (Charles d'Haussy from ConsenSys)

1. So what are the main barriers
2. to blockchain adoption?
3. The main barriers to blockchain adoption today
4. would be defining
5. and launching the right products.
6. Everyone is experimenting a lot on this ecosystem,
7. and we see some use cases
8. which are getting traction.
9. So the financial use cases are
10. getting a lot of tractions.
11. Identity use cases
12. starting to have a lot of attention.
13. What we find is when there is technologies,
14. the technologies are way faster than people.
15. If you think of the use of the internet back in the '90s,

16. people at the beginning were very scared of the internet.
17. I remember people telling me
18. I will never use my credit card on the internet.
19. And nowadays everyone uses credit card
20. on the internet,
21. because the people and the habits of the people
22. have been changing.
23. So today the technology is here,
24. the technology is ready,
25. the technology is evolving and growing every day,
26. but it's kind of practised by
27. a small circle of technologists.
28. And step by step, we see
29. more and more people using
30. these technologies
31. sometimes without even knowing.
32. If you think about the CryptoKitties,
33. the CryptoKitties users and
34. fans are not all technologists.
35. They're realising there is new type of products,
36. there is new type of online interactions
37. and online gaming happening.
38. But slowly, slowly the use of
39. the blockchain products is expanding.
40. So the technology is always faster than people.
41. So we have to be patient and always fine-tuning
42. and finding the right products
43. which will drive the adoption.

Meet Guest Instructor Henry Arslanian (PcW)

1.6 Why Use Blockchain Technology? (Henri Arslanian from PwC)

1. Hi there, very excited to be there.
2. As most of you know, my name is Henri Arslanian
3. and really my passion and my focus in life
4. is the future of the financial service industry.
5. Ok, now you may be wondering
6. what's happening with blockchain,
7. and when it comes to institutional players.
8. Well, there's also a lot of activity there as well.
9. For example, the vast majority
10. of financial institutions around the world now
11. are working on some kind of blockchains.
12. And there's many inherent advantages.

13. For example, a lot of the benefits,
14. like transparency, traceability, immutability,
15. are actually very beneficial in many use cases.
16. However, we are still at the early days
17. when it comes to blockchain technology
18. becoming mainstream.
19. For example, a lot of financial institutions today
20. are still at the experimentation level.
21. They are doing what we call proof of concept (PoC)
22. pilots potentially.
23. But very few are moving it to production,
24. or using blockchain inside
25. their current infrastructure.
26. There's numerous use cases going on right now
27. in the world that are very, very interesting.
28. Not only issues like digital identity.
29. Imagine if you're able to
30. put your identity on the blockchain,
31. and then you can let people
32. access it as you want it or not.
33. Or remittance, like we discussed.
34. If you want to send money back home,
35. or supply chains, smart contracts, trade finance,
36. the list goes on and on.
37. Let me cover some of them in more detail.
38. For example, let's start with one
39. that is a big problem today, supply chain.
40. Think about elements like diamonds,
41. or elements like, you know,
42. companies like Walmart
43. or other big grocery stores,
44. who want to track where their food is coming.
45. We're seeing now increasingly use cases
46. where people are using it for food traceability.
47. For example, if you're a young mom in Shanghai,
48. who wants to go buy their milk at a grocery store,
49. you want to make sure
50. that it's actually coming
51. from that farm in New Zealand
52. you believe it comes from.
53. And blockchain actually enables us
54. to these traceability opportunities.
55. But also, imagine
56. if you're buying a diamond,
57. for a close friend, for your future wife, or whatever.
58. You want to be able to trace that diamond
59. is not a blood diamond,

60. that it actually had a source,
61. you know where it was coming,
62. there was no human trafficking involved.
63. And blockchain technology enables this,
64. and we're going to see over
65. the next couple of years
66. a number of use cases
67. when it comes to traceability.
68. Another one is smart contracts.
69. This has been very interesting as well.
70. The beauty of a smart contracts
71. within blockchain technology
72. enables you to actually code a language
73. inside the smart contracts,
74. and whenever you have an independent event
75. that is happening, you have basically
76. the contract operates on its own.
77. A great example of this was
78. in the insurance sector.
79. One of the large insurance companies in Europe,
80. launched a test, AXA,
81. where they did kind of a flight insurance
82. on flight delays.
83. All flight times, arrival times
84. and take-off times are all public,
85. so whenever the flight was
86. delayed more than two hours,
87. automatically, you can get paid for
88. your insurance payment on the spot.
89. And then there's many other use cases.
90. For example, we look at the remittance space.
91. For me personally, it really bothers me
92. to see how much fees are still paid
93. every year in remittance,
94. especially by those
95. who cannot afford them,
96. who can afford the least.
97. The beauty with blockchain technology
98. now is we're really having
99. more and more mainstream cases
100. of how we can use blockchain technology,
101. but especially digital currencies,
102. in facilitating these cross border
103. payments and remittances.
104. But then again, we have a lot of challenges.
105. Make no mistake, implementing
106. blockchain technology is not easy.

107. For example, in many cases it's still
108. quite costly to actually implement it.
109. The other big thing is, as is often
110. in many cases, still we are not seeing
111. direct cost reduction or cost savings.
112. One of the reasons for that
113. is actually cloud offerings
114. are becoming increasingly cheaper,
115. and in many cases
116. have a lot of security features
117. that are available as well.
118. Another big challenge is scalability.
119. Think if you're a large company
120. that has operations in 150 or 200 countries,
121. and over a billion customers.
122. You need to be able to use some technology
123. that is very scalable.
124. And this is actually one of the challenges
125. we see with some blockchains,
126. is actually that they have scalability limits.
127. That they are not able to process
128. as many transactions every second
129. as many were expected.
130. The other big difficulty
131. is actually regulatory uncertainty.
132. You know, unless you are able to get
133. some regulatory clarity,
134. many traditional financial institutions
135. are reluctant to get more involved,
136. because they don't know
137. how regulators will react.
138. A final last one,
139. last trend that we are seeing
140. when it comes to blockchain adoption,
141. it really depends on the people
142. inside your organisation.
143. For example, you know, if you are
144. 6 months away from retirement,
145. and you don't want to rock the boat too much
146. and shake things up too much before you retire,
147. you are unlikely to come and pitch for blockchain
148. to be implemented inside your organisation.
149. So it really depends on where people are.
150. These are risky projects.
151. Anybody who has done any kind of deployment
152. of a new technology inside of financial institutions
153. knows how difficult it is,

154. and how risky it is,
155. and if it goes wrong,
156. normally somebody gets fired.
157. So there's been in this current environment,
158. what is actually less and less banking jobs,
159. that are generally quite well paid,
160. a lot of people are becoming
161. a bit more risk averse,
162. to actually push some of these innovations
163. like blockchain in it as well.
164. In many cases,
165. we have seen some innovation teams
166. take the lead.
167. But again, the problem that has been there
168. is that innovation teams are often great,
169. but they are great for
170. public relations perspective,
171. for marketing purposes,
172. to do some of the initial experimentation.
173. But again, when you want to
174. have it deployed at scale,
175. you need to have the whole
176. broader organisation involved,
177. from IT to compliance,
178. to the management, to finance,
179. to bring these things forward
180. from that perspective.
181. But again, a lot of exciting things
182. are going on when it comes to blockchain
183. in financial institutions.
184. Again, a lot of activity,
185. a lot of developments are going on,
186. and this is one of the most exciting times
187. to be in finance.
188. Not only because of
189. blockchain and digital assets,
190. but because of all of these changes
191. we're going through right now in the world.
192. That's all, my Fam folks.
193. Thank you very much.
194. It was a pleasure sharing with you all.

*Reference Videos What is Blockchain? [Introduction to FinTech Video 2.9A) by Professor Douglas Arner

1. Cryptocurrencies, blockchain, ICOs.
2. These are three terms

3. that are in the headlines daily all over the world.
4. Blockchain is the underlying technology
5. which came to prominence with
6. the launch of Bitcoin in 2009,
7. but what is blockchain?
8. Blockchain combines two long-standing
9. technological developments.
10. On one side, distributed ledger technology,
11. and on the other, cryptography.
12. If we look at Bitcoin, if we look at cryptocurrencies,
13. cryptocurrencies at their base
14. are blockchain systems combining
15. distributed ledger systems and cryptography.
16. Distributed ledger system,
17. what is a distributed ledger system?
18. For a system like Bitcoin,
19. the distributed ledger
20. means that the information in the system
21. are not stored in one single place.
22. Rather, they exist in multiple locations,
23. multiple identical ledgers
24. throughout the users of the system.
25. So, if we think about this idea of ledgers,
26. the traditional example is to think
27. of something like a bank.
28. A bank is a place where
29. a certain amount of money is stored,
30. it is a single place,
31. it is a silo, it is a single ledger.
32. At the other extreme, are distributed ledgers.
33. Distributed ledgers mean that there is no single place
34. where the information, the valuables,
35. the data are stored,
36. rather they are stored
37. across a variety of identical locations.
38. In between these structures of
39. centralised and distributed,
40. we also have network-based structures
41. where perhaps you have a single centralised structure
42. and a variety of spokes,
43. a hub and spoke structure
44. whereby the individual spokes connect to the hub.
45. So, distributed ledger technology
46. combined with cryptography.
47. Cryptography is a technology that involves
48. the secure storage,
49. the encryption of information.

50. It has a very long history with important points
51. going back to code breaking,
52. particularly in the Second World War.
53. If we combine distributed ledger technology
54. with cryptography, we have a system
55. of secure distributed ledgers
56. where entries have to be proven,
57. proven through the use of a variety of structures
58. which then encrypt the data into blocks.
59. So, transactions 1 through 50,
60. packaged in a block, encrypted together.
61. The next set of transactions build on that first block,
62. transactions 51 through 100
63. encrypted as a second block.
64. This structure provides
65. a number of very important attributes
66. to a blockchain-based system.
67. In particular, it provides for security.
68. The layers of cryptography across multiple blocks
69. make it very hard, but importantly not impossible,
70. to necessarily break those blocks
71. making blockchain potentially a highly secure system.
72. Second, it's a permanent system.
73. In other words, each of those transactions
74. is recorded permanently in each of those blocks.
75. That means that there is always a traceable history
76. of all of the financial transactions
77. going back to the very beginning.
78. So, with each Bitcoin,
79. you can trace back the life of that Bitcoin
80. from it's creation and into each account
81. that it has been transferred to over time.
82. And finally, transparency.
83. Transparency means that the combination of visibility
84. allows you to see what is happening in the blockchain.
85. This combination of security, permanence,
86. transparency, makes blockchain a potentially
87. very powerful platform technology
88. across a number of areas.

*Reference Video What is Blockchain? [Introduction to FinTech Videos 2.9B) by Professor Douglas Arner

1. Cryptocurrencies, blockchain, ICOs.
2. These are three terms
3. that are in the headlines daily all over the world.
4. Blockchain is the underlying technology

which came to prominence with
the launch of Bitcoin in 2009,
but what is blockchain?
Blockchain combines two long-standing
technological developments.
On one side, distributed ledger technology,
and on the other, cryptography.
If we look at Bitcoin, if we look at cryptocurrencies,
cryptocurrencies at their base
are blockchain systems combining
distributed ledger systems and cryptography.
Distributed ledger system,
what is a distributed ledger system?
For a system like Bitcoin,
the distributed ledger
means that the information in the system
are not stored in one single place.
Rather, they exist in multiple locations,
multiple identical ledgers
throughout the users of the system.
So, if we think about this idea of ledgers,
the traditional example is to think
of something like a bank.
A bank is a place where
a certain amount of money is stored,
it is a single place,
it is a silo, it is a single ledger.
At the other extreme, are distributed ledgers.
Distributed ledgers mean that there is no single place
where the information, the valuables,
the data are stored,
rather they are stored
across a variety of identical locations.
In between these structures of
centralised and distributed,
we also have network-based structures
where perhaps you have a single centralised structure
and a variety of spokes,
a hub and spoke structure
whereby the individual spokes connect to the hub.
So, distributed ledger technology
combined with cryptography.
Cryptography is a technology that involves
the secure storage,
the encryption of information.
It has a very long history with important points
going back to code breaking,

52. particularly in the Second World War.
53. If we combine distributed ledger technology
54. with cryptography, we have a system
55. of secure distributed ledgers
56. where entries have to be proven,
57. proven through the use of a variety of structures
58. which then encrypt the data into blocks.
59. So, transactions 1 through 50,
60. packaged in a block, encrypted together.
61. The next set of transactions build on that first block,
62. transactions 51 through 100
63. encrypted as a second block.
64. This structure provides
65. a number of very important attributes
66. to a blockchain-based system.
67. In particular, it provides for security.
68. The layers of cryptography across multiple blocks
69. make it very hard, but importantly not impossible,
70. to necessarily break those blocks
71. making blockchain potentially a highly secure system.
72. Second, it's a permanent system.
73. In other words, each of those transactions
74. is recorded permanently in each of those blocks.
75. That means that there is always a traceable history
76. of all of the financial transactions
77. going back to the very beginning.
78. So, with each Bitcoin,
79. you can trace back the life of that Bitcoin
80. from it's creation and into each account
81. that it has been transferred to over time.
82. And finally, transparency.
83. Transparency means that the combination of visibility
84. allows you to see what is happening in the blockchain.
85. This combination of security, permanence,
86. transparency, makes blockchain a potentially
87. very powerful platform technology
88. across a number of areas.

*Reference Video What is Blockchain? [Introduction to FinTech Videos 2.9B) by Professor Douglas Arner

1. Now, if we look at blockchains,
2. within this general structure
3. we will often have a third level added.
4. So, DLT plus cryptography plus smart contracts.
5. What are smart contracts?
6. Smart contracts are automated systems

7. that on the occurrence of pre-determined actions
8. something else happens.
9. If I provide A, you provide B
10. we pre-agree that A and B will be added together
11. to create a new C,
12. and this occurs on an automatic basis,
13. this is a smart contract.
14. There is an old joke that smart contracts
15. are neither smart nor contracts,
16. they are not smart because they are automated,
17. they happen automatically,
18. on the occurrence of something / events.
19. And they are not necessarily contracts,
20. but that is a more complicated legal question for later.
21. Within this idea of blockchain,
22. we can also add in a second important determination.
23. Blockchains can either be
24. permissionless, or permissioned.
25. A permissionless blockchain, like bitcoin,
26. means that it is open,
27. anyone can participate that downloads the software.
28. You download the software, you become a node,
29. you'll have a full picture of the ledger,
30. that distributed ledger is distributed to your node,
31. anyone can enter.
32. But, we also have what are called
33. permissioned blockchains.
34. A permissioned blockchain,
35. involves requirements or governance structures
36. or restrictions on entry.
37. In other words, only individuals or organisations
38. or computers or devices which have been pre-approved
39. can join into the network,
40. can access the information
41. and can potentially contribute transactions.
42. Now, when we think about blockchain,
43. it may or may not involve cryptocurrencies.
44. A cryptocurrency will involve a blockchain,
45. but a blockchain does not necessarily
46. involve a cryptocurrency.
47. In other words if we think of a blockchain based system
48. at its base, it is a distributed ledger
49. which is encrypted, maybe with an additional layer
50. of smart contracts on top.
51. Those individual data entries, can be anything.
52. The communications between those data entries
53. do not necessarily involve any sort of currency.

54. One of the most interesting and powerful applications
55. for this sort of thing,
56. is in production processes,
57. the food market where the providence of a chicken,
58. or a bottle of whiskey
59. can be proven by the blockchain system
60. from its creation, its history, its movements
61. documented throughout that system.
62. So, any eventual possessor
63. can document both the origin
64. as well as the lifespan of that particular chicken,
65. bottle of whiskey, diamond, artwork,
66. whatever it may be.
67. And that is the real power of blockchain.
68. To build systems
69. which are potentially highly secure,
70. permanent and highly transparent.
71. But, blockchain is not the solution
72. for every problem, why?
73. Because not every blockchain is created equally.
74. not every blockchain is necessarily secure.
75. Big blockchain systems like Ethereum or Hyperledger
76. or R3's quarter, or bitcoin,
77. these are highly secure.
78. But if I create a blockchain in my basement,
79. probably not that secure.
80. Just because it's a blockchain, doesn't mean it's secure.
81. Second, from the standpoint of
82. permanence and transparency,
83. this raises two problems.
84. One, is the garbage in, garbage out problem
85. in other words if you put that information in,
86. it's in there forever, and that is a big problem
87. in the context of building histories,
88. building information, the permanence problem.
89. And finally, privacy concerns.
90. If information goes into,
91. a permissionless public blockchain,
92. that information may be permanently
93. on public display and access,
94. and this can create all sorts of problems
95. in that not necessarily do we want
96. every piece of information permanently on view.
97. So, looking at blockchain,
98. and this is something that we talk about
99. a great deal throughout this course,
100. and in other courses.

101. Blockchain is a very important technology,
102. being used across all aspects
103. of the financial sector and beyond.
104. But it's not the solution for every problem,
105. but it is giving us an excuse to re-look,
106. to reconsider many of our existing systems
107. and infrastructure to build better systems.
108. (upbeat music)

Module 1 Reference Reading

References and Suggestions for Further Reading in Module 1

(1) Differences between a distributed system and a decentralized system:

- **What is the difference between decentralized and distributed systems? (Industry Article)**
- **Difference Between Centralized, Decentralized & Distributed Systems Oversimplified (Industry Article)**

(2) Advantages and disadvantages of a centralized system and a decentralized system:

- **Centralized vs. Decentralized: Pros And Cons (Industry Article)**

Module 2 Technological and Cryptographic Elements in Blockchain

Welcome to Module 2

Dear Learners,

Welcome to Module 2 Technological and Cryptographic Elements in Blockchain.

In Module 1, learners had an overview of the advantages and disadvantages of a decentralised system and a centralised trusted party in processing, and storing transaction data and you also had a glimpse of some issues to be resolved in a decentralised system.

In Module 2, you will see how blockchain technology works. Blockchains are designed to be immutable. You will see how the cryptographic elements including public-private key pairs, digital signatures and hash values are at work to achieve the special properties of blockchain. In addition to hearing from chief instructor Dr Siu Ming Yiu, you will also meet our guest speaker Prasanna Mathiannal (Co-Founder of MaGEHold) later in the module.

Happy learning and have a great week.

HKU Blockchain and FinTech Course Team

Module 2 Learning Objectives

After completing Module 2, learners should be able to:

- understand the basic usages of three cryptographic elements, public-private key pair, digital signature, and hash value;
- understand how the three cryptographic elements are used in blockchain to guarantee the properties of blockchain, such as immutability and privacy;
- understand basically how blockchain works such as how a new transaction can be appended, how to achieve consensus of miners, and why a miner would like to help.

Video 2.1.1 Cryptographic Elements: Public Key & Private Key

1. Welcome to Module 2 of our Blockchain course.
2. In the last module,
3. we have discussed two issues.
4. The first one is why we need to have a blockchain.
5. In particular, we do not want to have
6. a centralised authority to handle our transactions.
7. And then, the second issue is about the technical issues
8. for having a blockchain, namely, the security,
9. integrity, and the privacy issues.
10. Now, so in this module, we start to look deeper
11. into the technical elements of a blockchain
12. and how these elements work
13. together to form the blockchain.
14. The first elements I want to talk about are the public key,
15. private key, and digital signature.
16. In fact, they are mainly used
17. for encryption and decryptions.
18. The public key and private key,
19. they always go in pairs.
20. So basically, each user will have a pair
21. of public key and private key.
22. The public key can be open to the public,
23. so everybody can know your public key.
24. But on the other hand,
25. for the private key,
26. we need to keep it secret.
27. If you know one's public key,
28. you are not able to deduce his private key.
29. So in other words,
30. even if you can see people's public key,
31. it's very, very difficult to deduce what his private key is.
32. In encryption, how are we going to use this public key

33. and private key pair?
34. For example, if Alex wants to send
35. an email or a document to Bob,
36. so Bob is the receiver and Alex is the sender.
37. Alex wants to keep the email confidential,
38. so one way they can do it is:
39. Alex tries to encrypt the document
40. before it's sent over through the internet.
41. Now, then we try to use
42. public key / private key encryption.
43. Alex will use Bob's public key to encrypt the document.
44. So in other words, we are using the recipient
45. or the receiver's public key to encrypt the document.
46. And once the document is encrypted,
47. even if the hacker over the network can get a hold
48. of your encrypted version of the document,
49. he has no idea what will be the content.
50. When the receiver, Bob, gets the
51. encrypted message from Alex,
52. he use his private key, then he's able to decrypt
53. the message to see the real content of the documents.
54. So this is how the public key and private key
55. can be used together in order
56. to keep things confidential.
57. So we try to use the receiver's public key to encrypt
58. the document and when the receiver receives
59. that encrypted version of the document,
60. he will use his own private key
61. to decrypt the message
62. inside the encrypted documents.
63. And the important property is
64. if you do not have the right private key,
65. it's very, very difficult to decrypt the message.

2.1.2 Cryptographic Elements: Digital Signature

1. Now, the second concept, also very important
2. in blockchain is called digital signature.
3. Now, a digital signature basically is very similar
4. to the physical signature we want to do on a document.
5. But, right now, we just put it in the digital world.
6. So if you're given a digital document,
7. what you can do is you can create a digital signature
8. on that particular document, using your own private key.
9. So when you sign a document,
10. you used your own private key,
11. because private keys and public keys,

12. they go in pairs,
13. so the corresponding public key can be used
14. by others to verify your signature,
15. see whether this signature is from the owner
16. of the private key.
17. Now, if you change even one character or just one bit
18. in a document, the signature won't match.
19. So in other words, if the document has been changed,
20. I can just verify the signature,
21. and then the signature will tell you that
22. this is not correct, it's invalid.
23. Then you know that the document has been modified
24. and the signature is not correct anymore.
25. So this is the second cryptographic element
26. that is important for the construction of the blockchain.
27. But then I want tell you an efficiency problem
28. for digital signature.
29. So, basically, for any document,
30. you can also create a digital signature
31. using your own private key.
32. But, the problem is if the document is long,
33. the signature that we created will be also long.
34. So in other words, the longer the document is,
35. the longer time to create the signature,
36. and also the longer the signature will be.
37. So this becomes an efficiency problem.
38. If you want to send a document
39. together with the signature,
40. over from one side of the internet to the other side,
41. then it wastes quite a lot of bandwidth
42. if the document is large
43. because the signature will
44. become much larger in this case.
45. How do people solve this problem?
46. So we also have another technique,
47. which is called the hash value.
48. So given any digital document,
49. no matter how long the document is,
50. we can always generate a fingerprint of fixed length.
51. For example, some of the
52. common hash value generation
53. will produce a 160-bit of a fingerprint for a document,
54. no matter how long the document is.
55. And this fingerprint, we give it a name
56. called hash value, and this hash value
57. has a very similar property as a digital signature.
58. So if people try to change one bit, or one letter,

59. in the document, the hash won't match.
60. So in other words, if I give you the document,
61. together with the hash value and, actually,
62. you can check whether the
63. document has been changed or not.
64. If the document has been
65. changed the hash won't match.
66. Another key point is this hash function
67. is not something secret.
68. So, in other words,
69. everybody knows how to calculate this hash.
70. Or you can get a hold of a function
71. to calculate this hash value,
72. so if I give you the same document,
73. everybody is going to create the same hash,
74. using the same function.
75. Now, so you can see that this hash value can serve
76. as a fingerprint for the integrity of the document.
77. So let me give you a quick example,
78. so if I want to tell people that
79. this is my document, D,
80. and I want to tell people that
81. this document, D,
82. has not been changed by others.
83. So what I can do is,
84. I can send you the document, D,
85. and then I create a hash value of D,
86. and then send you the hash value as well.
87. And after I send you the hash value,
88. because I do not want other people
89. to change the hash value,
90. so I can tell people that this hash value
91. is produced by me, so I can actually
92. sign on the hash value.
93. This gives us a very fast and safe way
94. to send documents, over the internet,
95. so that people cannot change it.

2.1.3 Cryptographic Elements: Real-life Scenario Challenges

1. Let me give you a real example.
2. If Alex is going to send a contract to a company X
3. over the internet, if you just send a message,
4. plain text over from Alex to the company X,
5. basically the hacker has the capability
6. to modify any content of the message.
7. For example, they can pretend that the contract

is not from Alex.
They can change the name of Alex to Devil.
And then try to send this message over to the company
together with the contract.
Then company X may think that
the contract is from Devil,
but not from Alex.
To make sure that this won't be able to happen,
we can actually use the technique,
what we have just talk about.
Let me ask you a few questions,
see whether you know how to answer these questions.
If you know the answer to this question
it means that you really understand this concept.
So the first method is:
So Alex tries to send over the contract C.
And together with a hash value of the contract C.
So do you think this is safe?
Now if you think about it, this is not safe.
The main reason is, if you still remember what I talked
about, the hash value can be produced by everybody.
So in other words, if the attacker gets a hold
of your contract C, and the hash value of C,
he is able to change the contract C into C-prime,
and at the same time,
re-compute another hash value
for the C-prime and try to send the C-prime
and the hash value of the C-prime
over to the company X.
When the company X gets a hold of
the tampered contract C-prime
and the hash value of C-prime,
he has no way to discover that the
contract has been changed.
Because the hash of the C-prime
will match with the tampered contact C-prime.
So this won't work.
So you cannot just send the contract C
plus the hash value over because the attacker
is able to modify the contract and the hash
at the same time, so that the receiver may not realise
that the contract has been changed.
So we need one more technique.
Alex, should try to send three things over
to the company X.
First, he needs to send the contract C,
and then the hash value of C,

55. and also he has to sign on the hash value of C.
56. So basically it's the contract, the hash value,
57. and the signature of the hash value.
58. Now in this way, if you think about it carefully,
59. even if the attacker gets a hold of these three content,
60. he might be able to change the contract C to C-prime,
61. and also he might be able to change the hash value of C
62. into hash C-prime, but the problem is,
63. he is not the owner of the private key, of the signature,
64. so he is not able to sign on the hash value correctly.
65. So in this case, then he is not able to change everything
66. so that the receiver will not notice it.
67. The receiver can verify the hash value
68. and the signature to check whether the document
69. has been tampered or not.
70. So this is basically the way we need to make sure
71. that the document has not been tampered.
72. Now, let me ask you another question,
73. see whether you really know how to answer it.
74. Now, then how about another student may give me
75. another answer saying, then how about Alex will try
76. to just send a contract C
77. and also sign on the contract C,
78. and send the signature of the contract
79. and the contract over to the company X.
80. So do you think this is safe enough?
81. From the security point of view, yes, it's safe.
82. Because even if the attacker
83. get a hold of these two contents,
84. he might be able to change the contract C to C-prime,
85. but he cannot sign on it,
86. because he is not the owner of the private key.
87. And the receiver once can verify the signature,
88. can know that the signature is not valid
89. for the contract C-prime.
90. So in other words, from the security point of view,
91. this operation is okay, is safe.
92. But I hope you still remember, if you make a signature
93. directly on a document, then the size of the signature
94. will be as big as the document.
95. So in other words, you are wasting bandwidth
96. in order to send a long contract together
97. with a long signature.

REMARKS from Chief Instructor Dr SM Yiu

2.2.1 Cryptographic Technology: Key Questions for Blockchain

1. Let's focus back to blockchain.
2. Now, for an easy understanding,
3. let's put blockchain in the context of bitcoins.
4. Let's talk about what is a transaction.
5. As a simple example,
6. a transaction is something like this.
7. A person, A, tries to pass X bitcoins to B.
8. For example, Alex may want to transfer 10 coins to Bob.
9. Or Bob can transfer, six coins to David.
10. All these – each one of them will be called a transaction.
11. Now think, what's a transaction chain?
12. So it's also very easy to understand.
13. So a transaction chain is a sequence of transactions
14. and they are ordered by the creation time
15. of the transaction.
16. Now, so at the beginning, you can assume that
17. Alex has 20 coins and Bob only has one coin.
18. And right now, Alex starts to transfer 10 coins to Bob,
19. so this basically is one transaction.
20. And after the transaction,
21. then you can see that Alex will have 10 coins
22. after transferring 10 coins to Bob
23. then Bob will have 11 coins.
24. And later on, Bob can also transfer
25. six coins to David, but then for the transaction
26. to be executed, usually, we need an authorization.
27. For example, in a bank, we're trying to ask Alex
28. to sign on a transfer slip,
29. so that the bank knows that it's authorised by Alex
30. to transfer 10 coins from Alex to Bob.
31. And similarly, if Bob wants to transfer six coins to David,
32. Bob also needs to sign on a transfer slip
33. before the bank will try to make the transfer for Bob.
34. And why do we trust the bank?
35. The reason is very simple.
36. Because the bank has a very comprehensive procedure
37. and this procedure will be covered by the law,
38. so that's why we trust the bank to make sure that
39. all the transactions are valid and correct.
40. Now, but I want to remind you, in reality,
41. even if the bank has a comprehensive procedure
42. for every transaction, but then, some of its rules,
43. basically, it still relies on the staff to follow them.
44. So if the staff is cheating, in fact,
45. there's no 100% guarantee for the safety

46. or the security of the transactions.
47. Now, but right now, we have blockchain,
48. so we do not have a bank
49. and we do not have a centralised entity to do it for us.
50. Now one simple solution is we can just
51. put the transaction chain on the internet,
52. so everybody can get a copy and everybody can check.
53. Okay, so this is one simple solution.
54. So instead of keeping all the transactions in the bank,
55. what we do is we put all the transactions,
56. the transaction chain, into the internet.
57. Now, in this case, we actually have the property
58. of transparency, so anybody can do the audit
59. for all the transactions.
60. But the problem is if everybody can get a hold
61. of all the transactions, the first question we need
62. to worry about is,
63. can anybody modify the transactions easily?
64. The second question is, in reality,
65. if you are using a bank,
66. the bank is the one who maintains all the transactions,
67. the ledger, the transaction book.
68. But right now, the transaction chain is in the internet,
69. so the problem is who is going to maintain the chain?
70. And if you have new transactions,
71. who is going to append
72. or put the new transactions into this chain?
73. So these two questions are what we are going to study
74. and see how the cryptographic elements
75. are going to help in this blockchain construction.

Video: 2.2.2 Who can Modify Transactions?

1. Now, let me recall the cryptographic elements
2. we just learned.
3. For example, if we want to send a contract C from Alex
4. to the company X, remember, what we have to do is
5. we will send the contract C, the hash of the contract C,
6. together with the signature on the hash value.
7. And in this case, then the
8. contract C will not be tampered.
9. It cannot be changed by anyone easily,
10. so we try to make use of this idea
11. to construct our first blockchain.
12. Now, in the diagram, you can see that transaction one
13. is basically A, a person, A, tries to transfer $10
14. or 10 coins to B, and he also creates a hash value,

15. which is called h1, and he followed exactly
16. what we have learned, so he tried to sign on this h1,
17. so you can see the signature is signed by A.
18. So A authorised the transaction, $10 transferred to B
19. and he has created a hash and signed on the hash.
20. And then, the second transaction
21. is B is going to transfer $5 to C.
22. And at the same time, B also followed the rules,
23. so B has constructed a hash value, h2,
24. for transaction two and as well as signed on
25. the hash value h2.
26. And then, you can see the signature, basically,
27. is signed by B who also authorised
28. the transfer of $5 from his own pocket to C.
29. And you can see the last transaction is also from A.
30. So the transaction three is A tried to transfer $5 to D
31. and he also creates a hash value, h3,
32. for transaction three
33. and also signed on the hash value, h3.
34. Now, assuming that all these transactions
35. are on the internet right now, so I'm one of the users.
36. I can actually get this transaction chain
37. and verify whether every transaction is valid or not.
38. And also, I can also check the signature
39. because the signature can be checked by anybody
40. using the corresponding public key of the person.
41. So that's why I can see transaction one,
42. whether it's valid or not,
43. or transaction two and transaction three as well.
44. So this is my first construction of a blockchain.
45. But if you look at this carefully,
46. then you can see that actually A can do something
47. on the transaction even after it's put on the internet.
48. Now if you look at the diagram,
49. let's focus on transaction three.
50. Right now, A changes his mind.
51. "I do not want to transfer $5 to D."
52. So what he can do is he can
53. get a hold of all the transactions,
54. download a copy to his own computer.
55. Then what he wants to do is change transaction three
56. into only transferring $1 to D.
57. Now, then what can we do?
58. Recall that hash can make things difficult to change.
59. So once you change one bit, the hash won't match.
60. But in our problem is the text, I mean, the transaction
61. and also the signature basically

are created by the same person.
So that's why the same person can also change the text,
the signature, the hash together,
using his own private key.
Now, so, what we want to do is I want to make sure that
the transaction, every transaction,
cannot be changed by a single owner.
Now this is actually what blockchain is doing.
Now we have a modified version.
Transaction one stays the same.
So A tries to transfer $10 to B
and transaction two, the same.
B tries to transfer $5 to C.
The main difference is, assuming transaction one
is the first transaction of the whole chain,
then we will say that this is D1.
And if you look at transaction two,
when B tries to create a hash of transaction two,
in the original version, the hash is only created
on transaction two, but right now,
if you look at my modified version,
the hash is basically created on transaction two
together with D1.
So we'll try to use the whole transaction
in the previous block
and into the document before you create a hash.
Then, if A wants to change a transaction,
for example, he wants to change transaction D3,
then transaction four will rely on transaction three,
so that's why he needs to change
all the subsequent records
in order to make sure that all
the hash values will stay consistent.
So you can see that these are the key issue, key points,
that make the blockchain immutable.
So only people use this term, immutability,
to describe this property of the blockchain.
It means that the record is
permanent and tamper-proof.
So once a transaction is put in the blockchain,
it cannot be altered or deleted.
It becomes a permanent record.
Otherwise, if you want to change
something in a transaction,
you need to change all the
subsequent transactions
together in order not to be discovered.

109. Now, it's actually a very tedious work if you really want
110. to change something because
111. the chain may be very long.
112. Then, you are going to do a lot of changes
113. in the blockchain and I will talk about how to change,
114. how to create, how to append a new transactions
115. into the blockchain.
116. Then, you will understand
117. this is a huge amount of work.
118. Basically, it's not possible.
119. So you can see that, in a bank,
120. we try to guarantee the
121. immutability based on procedures
122. and the rules and hoping that the staff
123. will try to follow the rules.
124. Otherwise, they may go to jail.
125. But still, there's some staff may cheat,
126. so it's not 100% guarantee.
127. But on the other hand, in this blockchain,
128. we try to guarantee the property
129. of immutability base on the technology.
130. So we are using hash and signature to guarantee
131. this property, so it's not relying on human beings,
132. assuming that they will follow the rule.
133. So in some sense, you can say that it's safer
134. because the factor of human beings is eliminated.
135. It's guaranteed by the technology
136. you use in the blockchain.

Video: 2.2.3 Who Will Maintain Transactions?

1. Now, let's proceed to the next question.
2. Then who is going to maintain the chain
3. and try to append new transactions?
4. Then you know that in a bank,
5. the bank is going to do it.
6. We try to issue a new transaction
7. and the bank tries to validate our transaction,
8. if it's okay, we put it in the transaction book
9. but then in blockchain, everything is in the internet,
10. there's no centralised authority
11. to handle the maintenance,
12. handle the chain.
13. So who is going to do it?
14. In fact, it's very simple.
15. Everybody joining the scheme in the network
16. is able to do it.

17. Okay, now, how can we do it?
18. So everybody can have the authority to keep a copy
19. of the whole chain and when A has a new transaction,
20. he broadcasts this transaction
21. to everybody on the internet.
22. So everybody will receive a message
23. from A saying that, “I want to transfer my $10 to B.”
24. So this transaction will be seen by everybody
25. on the internet, if they are one of the users
26. of the blockchain.
27. And everybody is able to check it,
28. and if it’s valid, then he can try
29. to append this new transaction to the chain.
30. And the first one, usually who completes this will try
31. to broadcast the new chain to the internet.
32. So if I want to add a new transaction to the chain,
33. I send a message to everybody
34. so the first one who helps me verify the transaction,
35. will try to append a new transaction
36. on his own chain, and broadcast the new chain
37. to the internet, so somebody else would try
38. to get the new chain and work on other transactions.
39. The ones who help to check the transactions
40. are usually called miners in blockchain.
41. Everybody can be a miner depending
42. on whether you want to be a miner or not.
43. But you may have a question.
44. That may be chaos, right?
45. Because right now the internet may have many copies
46. of the blockchain, the transaction chain.
47. Now, assume at the beginning,
48. every miner got the same chain,
49. but after a while, we may have this situation.
50. Miner A appends a new transaction, and broadcasts it,
51. but due to the network congestion,
52. maybe B and C didn’t get it.
53. So only miner A has this new copy of the chain.
54. Or miner E who is not an honest person,
55. he’s an adversary, attacker,
56. tries to append a fake transaction
57. and broadcasts it.
58. And D didn’t know it, right?
59. So D would try to download E’s chain
60. and try to work on E’s chain.
61. And even worse, F can try to double spend
62. because F can initiate two transactions
63. even if his account may only have like $10,

64. he can say that I want to transfer $10
65. to Alex and another $10 to Bob.
66. And then sends out two transactions at the same time
67. and broadcasts it.
68. And based on the understanding that in the internet,
69. you can see there are some miners
70. who may get the first transaction,
71. and then some miners may get
72. the second transactions.
73. So in some sense, it seems like it
74. becomes chaos, right?
75. So if you imagine the situation is something like this,
76. there are many copies of the chain on the internet.
77. And maybe some of them are not the same.
78. The first chain is the corrent transaction chain,
79. and we assume that B right now,
80. the account has only $10.
81. And then, B is the attacker,
82. then you can see that B tried
83. to append a fake transaction
84. into the transaction chain.
85. B tried to transfer $15 to C and created a hash as well
86. and signed on a hash value as well.
87. But this is fake.
88. This is incorrect.
89. And another situation is,
90. B actually issued another transaction as well,
91. so B also wants to transfer $5 to D.
92. But then you know some miners
93. have been working on the first transaction
94. transferring $15
95. to C and another miner may work
96. on the transaction transferring $5 to D.
97. Then you can see that on the internet,
98. we may have these three chains.
99. And only one chain is correct.
100. So in a very complicated situation,
101. you can imagine that we have many, many chains.
102. Some are correct, some are incorrect,
103. some are the same, some are different.
104. Then how we can resolve the problem?
105. In fact, blockchain, the original idea,
106. you use a very simple rule.
107. Everybody when they discover that there is more
108. than one chain,
109. everybody will believe the longest chain.
110. And you may ask then why, is based on what kind

111. of principle, why only the valid transaction
112. can be added in this case?
113. And then why everybody eventually
114. will keep the correct chain?
115. Now, they have a very important assumption.
116. They assume that the majority of the users are honest.
117. Let me give you a concrete example
118. then you will understand
119. why we always follow the longest chain that is correct.
120. Now assuming that the existing chain
121. only has one transaction, transaction one there.
122. A transfers $10 to B and we are going
123. to have two transactions.
124. One is correct, the other is not correct.
125. So transaction two is correct,
126. we try to transfer $5 to C,
127. and transaction Tr2' is not correct.
128. B tries to transfer $15 to C
129. and you can see that if the miners try
130. to have to verify these two transactions,
131. most of the miners will say
132. that transaction Tr2 is correct
133. and transaction Tr2' is not correct.
134. So in other words, most of the miners will try
135. to append Tr2 onto Tr1 instead of Tr2'.
136. Now if you assume that the majority
137. of the miners are honest,
138. so even if there are some attackers,
139. the Tr1, Tr2' chain will only be agreed
140. by very few people.
141. And most of the honest miners will try
142. to continue adding transactions on the Tr1 to Tr2.
143. And very few attackers will take care
144. of the Tr1 to Tr2′.
145. Then you can imagine the correct chain
146. will get longer and longer if you give it enough time.
147. Because everybody knows that Tr2 is correct.
148. Tr2' is not correct.
149. So nobody is going to append new transactions
150. on the T2' chain.
151. So this is basically why the principle works.
152. Now, after resolving this issue,
153. my next question is why do people want to help?
154. Why do the miners want to help you?
155. Why do the miners want to validate the transaction
156. for you and then try to append the transaction
157. into the new blockchain?

158. The main reason is in the blockchain system,
159. we have this incentive for the miners.
160. So in return, if the miner is the one who validates
161. the transaction and appends the
162. new transaction successfully
163. into the blockchain,
164. he can create a new coin for himself.
165. He can get a bitcoin after doing the mining.
166. Because everybody wants to get this reward,
167. so what they want to do
168. is they want to make it fair to give all the miners more
169. or less an equal chance to get the reward.
170. So what they do is they will try to make the checking
171. of the transaction more difficult.
172. In fact, they have a concept called proof of work.
173. So you need to need to spend effort in it
174. in order to get the reward.
175. You can imagine,
176. that all the miners are trying to validate the transactions,
177. because after you validate
178. the transactions successfully,
179. you get a new bitcoin.
180. The system will try to ask miners
181. to compute a difficult
182. mathematical question using computers.
183. So in order to append a new transaction
184. on an existing chain, besides checking
185. whether the transaction is valid or not,
186. he needs to calculate an answer
187. for a mathematical question.
188. Now you can see that the transactions right now
189. are verified independently by multiple miners
190. and the decision is made by the majority of the miners.
191. There's no centralised decision-maker in the system.
192. And in fact, the one I just talked about
193. is one of the many trust models used in blockchain.
194. There are some others, we will also talk about them
195. in the later modules of the course.
196. And usually this consensus,
197. this trust model will come
198. with a consensus algorithm so different platforms
199. may use different trust models
200. and also use different consensus algorithms
201. to achieve the decisions.
202. Now let me summarise it first.
203. So roughly speaking, in a blockchain system,
204. the security and the integrity will be guaranteed

205. by using the cryptographic primitive,
206. like the hash, signatures, trust model,
207. the consensus algorithm, plus the incentive scheme.

Video 2.2.4 Cryptographic Technology: How to Protect Our Privacy?

1. And we still have one last question: privacy.
2. It seems like the privacy is even worse
3. than we have in the bank, because, in reality,
4. we have a bank,
5. then the privacy issue is limited to the bank.
6. The bank can look at your transaction,
7. but the others are not able to look at it.
8. But right now it seems like all the users in the internet
9. can see all the transactions.
10. So the privacy issue becomes a major problem.
11. Now, so how can blockchain handle it?
12. The answer is very simple.
13. Because remember how many
14. cryptographic primitives we have learned?
15. We have used hash, signature.
16. We haven't used the public key and private key pair.
17. So basically, blockchain will not ask you to use
18. real names in the transactions.
19. So we are going to use the public key
20. and private key to do it.
21. So for example, if A wants to transfer $10 to B,
22. B in order to receive this $10,
23. B will try to create a pair of public key and private key.
24. And everybody's public key will be used as his name.
25. So we are not trying to put the transaction
26. as "A transfers $10 to B", and instead,
27. this is what happens inside a blockchain:
28. Public key, basically, is only a bunch of numbers.
29. So we receive an address of a random number
30. transferring $10 to another account.
31. So basically we only have the account numbers
32. shown in the transactions without a real name.
33. And people are not able to map this account number
34. to the real person, because the number will be
35. generated by the user himself.
36. So this resolves the problem of privacy.

Meet Guest Speaker Prasanna Mathiannal (Co-Founder of MaGEHold)

2.2.5 Public-key Cryptography (Prasanna Mathiannal from MaGEhold)

1. Hello, everyone.
2. Hi, I'm Pras.
3. I'm the co-founder of MaGEHold,
4. an angel investment firm
5. in the blockchain space.
6. A brief about myself,
7. I'm a banker by the day,
8. technologist by night,
9. and a philosopher during the weekend,
10. but enough about me.
11. Let's dive into the hot topic, blockchain.
12. In cryptography,
13. there are a few unique concepts
14. and the one that is actually
15. most relevant for blockchain
16. is actually public key cryptography,
17. which is a form of asymmetric cryptography.
18. Now, what does that mean?
19. Let's say you have an account,
20. which is actually, in blockchain terms,
21. represented by a string of characters
22. and you're going to store a certain value,
23. and let us take bitcoin as an example
24. for easy illustration.
25. Then, you of course know that bitcoin
26. in current markets actually has some value.
27. Therefore, you want to be careful about
28. how you operate that account
29. and make sure it stays under your control.
30. So what gives you the control?
31. That control is given to you
32. by what is called a private key.
33. So you can kind of imagine
34. this whole account structure
35. and the private key that gives you control
36. and therefore, ownership of
37. that account in the same way
38. as you would see steel safes,
39. but with digital kind of keys
40. that you can key in to open it.
41. Then, how exactly does this cryptography work?
42. It is very simple.
43. You have a password or a secret key,
44. which you then undergo a process called hashing
45. and hashing just converts it

46. into a fixed length kind of output
47. and there's no other easy way
48. to actually replicate it
49. or kind of break it down backwards
50. to find out what was the password you initially use.
51. That's what is called hashing.
52. So as you might have guessed,
53. in controlling your account access in a blockchain,
54. especially public blockchains, like bitcoin,
55. private key and public key
56. is where hashing comes in.
57. So public key technically is a conversion /
58. a form of hash of the private key.
59. Second, whenever you have accounts,
60. you can automatically imagine transactions happen.
61. So for signing transactions
62. and proving that you initiated transaction
63. as a source to a destination
64. is another place in blockchain where
65. hashing is used.
66. Third, we talked about
67. securing the network by people.
68. This is where concepts called nodes,
69. which are actors within the blockchain network
70. that actually can validate your transactions,
71. pack them up into a block and then,
72. keep connecting them in a chain
73. as one block after another.
74. And in order to perform this action
75. and possibly get rewarded or incentivised,
76. you can actually use
77. certain consensus mechanisms,
78. like Proof-of-Work or Proof-of-Stake, etc.
79. So now, most public blockchains,
80. any data you store, either as logs
81. and databases inside the blockchain,
82. is open and free for all to read.
83. So blockchain is secure,
84. but the data you store,
85. you have to watch out
86. which blockchain you're on
87. and be sure that you're not compromised.

Module 2 Reference Reading

References and Suggestions for Further Reading in Module 2

(1) The original blockchain design paper by Satoshi Nakamoto:

- Bitcoin: A Peer-to-Peer Electronic Cash System (Source: Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org)

(2) Industry articles about the features of blockchain:

- 6 Key Features of Blockchain : This is what makes Blockchain so exciting! (Source: The Fintech Way)
- Key Characteristics of the Blockchain (Source: Deloitte)

Module 3 Blockchain Platforms

Welcome to Module 3

Dear Learners,

Welcome to Module 3 – Blockchain Platforms. In the last Module, you saw how cryptography works in blockchain using public-private key pairs, digital signatures and hash values.

In Module 3, we will continue to look at the technical aspects of blockchain including the characteristics of three major blockchain platforms, Bitcoin, Ethereum and Hyperledger. We will explore and compare these platforms under five perspectives including platform design objectives, public vs. private block chain, whether there's generation of cryptocurrencies on the platform, consensus algorithms, privacy and confidentiality.

In addition to hearing from chief instructor Dr. SM Yiu, later in the module, we will also have Charles d'Haussy (Director Strategic Initiatives ConsenSys) to share his expert opinions on consensus algorithm and trustlessness and immutability of blockchain technology.

Happy learning and have a great week.

HKU Blockchain and FinTech Course Team

Module 3 Learning Objectives

After completing Module 3, learners should be able to:

- classify blockchain platforms from five perspectives;
- compare three major blockchain platforms, namely Bitcoin, Ethereum and Hyperledger, in terms of five perspectives;
- understand more about tokenization and fund raising in blockchain projects.

3.1.1: Classification of Blockchain Platforms (Part 1) – An Overview of the 5 Key Perspectives

1. In the last module, we talked about
2. some cryptographic elements, like the digital signature,
3. public key / private key,
4. and also the hash function,
5. that form the basis of a blockchain.
6. And we also talked about how these elements
7. work together to form a basic blockchain.
8. Now, the original idea of blockchain
9. is to support Bitcoin.
10. But in fact, Bitcoin is not the only blockchain platform.
11. There are many available
12. blockchain platforms right now.
13. For example,
14. Hyperledger, Ethereum, Ripple, Corda, etc.
15. In this module, we're going to talk about the following.
16. First, we will talk about
17. the different classifications of these platforms.
18. And then we will try to compare three major platforms,
19. namely Bitcoin, Hyperledger and Ethereum.
20. Now, let's start with
21. the classifications of the blockchain platforms.
22. In fact, we can look at the blockchain platforms
23. from five perspectives.
24. The first one is whether the platform
25. is designed for generic applications or not.
26. And the second perspective is whether
27. the blockchain is a public blockchain or not.
28. And the third perspective is, we want to talk about
29. what kind of consensus models or algorithms it uses.
30. I hope you still remember we talked about
31. the Proof-of-Work in Module 2.
32. In fact this consensus model and
33. algorithm has big impact
34. on the performance of the blockchain platforms.
35. In particular, depending on
36. what kind of consensus model or algorithm you use,
37. it affects the efficiencies.
38. In other words, we worry about how many transactions
39. can be handled in a second by the platform,
40. or how many users can use the
41. platform at the same time.
42. And the fourth perspective is, we want to talk about
43. whether the platform provides smart contracts or not.
44. We'll talk about what are smart contracts later.
45. And finally, we want to know whether
46. the platform comes with a cyber token.
47. So we will try to look at

48. these five perspectives in detail.

Video 3.1.2: Classification of Blockchain Platforms (Part 2) – Perspectives No. 1 and 2

1. The first perspective is whether the blockchain platform
2. is designed for generic applications or not.
3. Sometimes the design of a platform
4. may only be for some particular industry
5. or the design of the platform may be generic.
6. In other words, you can actually use the platform
7. to develop applications in any industry.
8. Now let me give you some examples.
9. For example, Bitcoin actually is a very specific platform
10. because Bitcoin is only for the transactions,
11. the processing of the transactions
12. of this particular cybercurrency only.
13. So you cannot use Bitcoin to do anything else.
14. Or you cannot create any
15. applications in other domain areas.
16. If you look at Corda, basically the design of Corda
17. is specially for the financial industry.
18. And there are many others,
19. such as Openchain,
20. is basically created for digital asset management.
21. If the platform is specially designed
22. for a particular industry,
23. they will have specific features
24. only fit for that industry.
25. For example, in Corda, basically, they allow you
26. to write programs that you can incorporate
27. some of the legal expression,
28. because the financial industry worries a lot
29. about whether the transactions follow the law.
30. So that's why they have
31. particular features to allow users
32. to write programs that you
33. can embed legal expression
34. into the transactions.
35. But on the other hand, for the generic platforms,
36. then most likely
37. they will not have these kinds of features,
38. and then you can use it to design and implement
39. any applications in any domains.
40. So we'll try to look at whether the platform
41. is a generic one or is specially designed
42. for a particular industry.
43. Now, for the second perspective, we want to know

44. whether the blockchain is designed
45. for a public blockchain or not.
46. Now, if you look at the original design,
47. in Bitcoin, everyone can join Bitcoin
48. without being verified their identity.
49. In other words, I don't care who you are.
50. As long as you want to join, I will allow you
51. to join the blockchain easily.
52. They say that is permissionless,
53. meaning that you don't need to get permission
54. in order to get into the blockchain.
55. But however, think about it,
56. if blockchain is used by some big enterprises,
57. what they want to do is,
58. they might want to create blockchain for their business.
59. Now then they may have a concern.
60. If everybody in the public can join the blockchain,
61. then they worry that these members may be able
62. to see a lot of information about the company,
63. so they don't want to have this kind of situation
64. to happen in their blockchain.
65. Now so, what they want is,
66. they have other requirements
67. if they want to use blockchain
68. in their business.
69. First, they probably want
70. only the trusted parties
71. with certain identities can join.
72. Now this is very obvious, right?
73. If the parties are not trusted,
74. I do not want them
75. to look at the information of my company.
76. Or they even want to have a better control
77. on the members to let them
78. see what they want to see.
79. And on the other hand,
80. because they want the business
81. to be smooth, so that's why usually
82. they have a requirement for high scalability,
83. meaning that they want the
84. platform to incorporate
85. a large amount of users.
86. At the same time, they want the transaction speed
87. to be fast enough
88. to cope with the business.
89. So that's why people come up with another type
90. of blockchain platform, which is called a

permissioned blockchain.
Now in this type of permissioned blockchain,
the entities can only join the blockchain
if they can pass a verification process.
And of course, if you look at it this way,
it means that not everybody
can join the blockchain freely
without any verification,
so you can treat this kind of blockchain
as one which is not fully decentralized.
Let me give you an example.
For example, if my blockchain will allow a staff
from the insurance company to join,
so I need to have a verification process
to make sure that you are
one of the insurance company,
you are one of the staff on the authorised list
of companies before you can join a blockchain.
This kind of verification will be done
in this permissioned blockchain.
Now, so that's the second perspective
on how we can classify a blockchain platform.

3.1.3: Classification of Blockchain Platforms (Part 3) – Perspective No. 3

And the third perspective is we want to look
at what kind of consensus models or
what kind of algorithms the
blockchain platform is using.
In Proof of Work, they require the miners
to compute very hard mathematical problems
and they also introduce randomness into this problem.
Even if the miner has more computational power,
they may not be able to get the answer
faster than the other miners.
So that creates a fairness of the system.
In other words, we do not want some of the miners
who have lots of computational power
to take control of the whole blockchain.
And of course, if you still understand
what I talked about Module 2,
you can see in the Bitcoin platform system
it actually allows fake transactions to exist.
And then what we do is, we allow the transaction
to be put in the blockchain and then we can have
multiple blockchains; some with the real transactions

22. but some with the fake transactions.
23. But finally, we'll try to take the majority
24. to rule out the fake transactions.
25. And in other words, we depend
26. on the length of the chain.
27. We try to believe the longest chain is the correct one.
28. Because the basic principle behind is
29. most to the participants are honest.
30. So that's why, if most of the participants,
31. most of the miners are going
32. to append the transactions
33. in the longest chain,
34. then we would believe
35. that this chain is the correct
36. chain for all the transactions.
37. Now if you understand this
38. principle, this Proof of Work,
39. then probably you can
40. see some issues behind.
41. First, it takes time for the
42. miners to do the calculation.
43. In particular, to solve
44. the mathematical problem.
45. Then it affects the efficiency
46. of the whole blockchain
47. and also it's a waste of
48. resources, of computing resources
49. in order to calculate
50. meaningless math problems.
51. Now the second issue is at any time slot,
52. there can be different
53. versions of blockchains
54. existing in a system.
55. At any time or point, we still have
56. an issue to talk about when to confirm
57. if a transaction is really settled.
58. Now in the real Bitcoin system,
59. what they do is
60. they recommend the user to
61. wait a certain amount of time,
62. like, say 10 minutes or 20 minutes,
63. until the transactions get
64. stable in the longest blockchain.
65. Then they will confirm that this
66. transaction is really settled.
67. Otherwise, we cannot
68. guarantee the transaction

would be put in the
blockchain at that moment.
So you can see, this waiting also takes time
until the chain gets stable.
So the whole thing will slow down the performance
of the whole blockchain platform.
So in other words, on the blockchain platforms,
if you are using the Proof of Work as
the consensus model or the algorithm,
that means that the performance
of the platform must not be fast enough.
Now you can see that in many applications
this kind of performance is not acceptable.
So in the past few years, there were many, many
consensus models and algorithms
proposed by different people.
In fact, people are trying to use another concept
to work on this consensus algorithm,
which is called the Proof of Stake.
Now the basic idea behind is very simple.
Because you can see in the blockchain,
you know some people are holding
tokens or the cyber coins.
So we want to let the wealthy
people to make the decisions.
Now the rationale behind is very simple.
If I'm the one who holds a lot of cyber coins
in this blockchain platform, I do not want
to do anything illegal, I do not want the
fake transactions to be inputted
in the blockchain platform.
So that's why these kinds of
people will try to make sure
that the transactions are correct before
they are appended to the blockchain.
Now more precisely, what they are doing is
the one who holds more coins
will have a higher chance
to make the decision to append
a new block into the blockchain.
In this kind of Proof of Stake,
they usually will introduce
randomness into who will be the guy
who makes the next decision.
But then if you more coins
then you have a higher chance
to make the next decision to append

116. a block into the blockchain.
117. There are many variations
118. on this Proof of Stake.
119. For example, there is one variation that
120. they want to look at how long you've held the coins.
121. So in other words, in addition to seeing
122. how many coins you are holding,
123. they also want to know how long
124. you've held those coins.
125. They will combine these two factors together
126. in order to make a choice,
127. who is the next decision-maker
128. for appending a new block into the blockchain?
129. Now if you look at the existing blockchain platform,
130. there are many others.
131. For example, Ripple basically has
132. its own consensus algorithm, which they call
133. a Ripple Protocol Consensus Algorithm.
134. And there are some other platforms,
135. they try to use voting.
136. In other words, they will let the miners to vote
137. which transactions to be appended to the blockchain.
138. But what the main reason behind is, if you pick
139. a fast enough consensus algorithm,
140. actually can increase the efficiency of the platform a lot.
141. We want to make sure that this consensus model
142. is fair, secure, but at the same time
143. we want to increase the efficiency.

3.1.4: Classification of Blockchain Platforms (Part 4) – Perspectives No. 4 and 5

1. The fourth perspective is related to smart contracts.
2. If you look at the original design of blockchain,
3. for example, if you still remember
4. what I talked about in Module 2;
5. we actually talked about the original design
6. of blockchain for Bitcoin.
7. Now in this kind of blockchain platform,
8. it's not programmable.
9. In other words, people cannot write any programs,
10. any additional applications
11. on top of these blockchain platforms.
12. The only purpose of the blockchain
13. is to process the transactions
14. of the bitcoins of the users.
15. Now, but then in 2013,
16. smart contracts started to be proposed in Ethereum.

17. People usually mark this as Blockchain 2.0.
18. So from 2.0 onwards,
19. then we can actually use smart contracts
20. to write programs and create new applications.
21. Now, so you can see that smart contracts
22. are very important
23. in the development of blockchain platforms
24. because they open up the opportunities
25. for different developers
26. or different companies to
27. come up with new ideas,
28. to create new applications in
29. different disciplines.
30. Now but then having smart contracts,
31. of course is good for
32. application development
33. then we can have the chance
34. to develop different types
35. of applications for different disciplines.
36. But actually, it also brings
37. a lot of security problems
38. into the blockchain platforms.
39. And lastly, some of
40. the blockchain platforms
41. will come with a cyber currency,
42. and some of the platforms,
43. they may not have a cyber currency.
44. Basically, most of the cyber currencies
45. are created for money raising.
46. In particular the ICO we talked about.
47. Cyber currencies are also used as a token
48. to be spent or paid on a transaction.
49. Now in other words they have a platform,
50. they create a new cyber currency.
51. One of the main purposes is to
52. attract you to stay in the platform.
53. So you just get a hold of my
54. token and then the token
55. can only be spent on my platform,
56. so that's why you will stay in my platform
57. and try to pay for the
58. transactions in my platform.
59. Having this kind of token,
60. they hope that the price of
61. the token will be increased
62. so that the owner can make more money.
63. So that the people will try to invest

64. in your applications more
65. based on this new token.
66. You can see that this cyber currency
67. is not a necessary element
68. in the blockchain platform.
69. So not all the platforms
70. will have their own cyber currencies.
71. For example Hyperledger and Corda,
72. they do not have their
73. own cyber currencies.
74. And some of them may not
75. even have the capability
76. for you to create a new token.
77. But on the other hand,
78. it doesn't mean in this platform,
79. you cannot use any of the cyber currency
80. in the applications.
81. Actually, they can still
82. use Bitcoin, Ethereum,
83. to be embedded in their applications.

3.1.5: Highlights of Major Blockchain Platforms

1. Now, what I'm going to do next is try to talk about
2. the comparison between these three major platforms.
3. The first one of course, Bitcoin,
4. which is the original proposal
5. for using blockchain technology.
6. The second one I want to talk about
7. will be Ethereum.
8. We have an Ethereum enterprise alliance
9. formed by more than
10. 250 members, including
11. Microsoft, JP Morgan, Intel, etc.
12. And then, another major platform
13. for blockchain is called Hyperledger.
14. In fact, Hyperledger is formed
15. by the Linux foundation,
16. one of the open-source foundations,
17. and the aim of Hyperledger is to design
18. and develop enterprise blockchain.
19. So in other words,
20. they want to open up a framework,
21. so that different enterprises can actually create
22. their own versions of blockchain.
23. So let's try to compare these three
24. major blockchain platforms right now.

25. Recall that, we are going to evaluate
26. and compare this platforms from five perspectives.
27. The first one is whether this platform is generic or not.
28. The second is whether the blockchain produced
29. by this platform is a public blockchain,
30. namely, the permissionless blockchain
31. or if it is a permissioned blockchain.
32. And third dimension, is we want to know
33. what kind of consensus algorithm is being used
34. in the blockchain platform.
35. Next, then we'll see whether it supports
36. smart-contract programming or not.
37. And finally, we want to see whether there is a cyber currency
38. attached to the blockchain platform or not.
39. Now, if you look at the first dimension,
40. whether the platform is for
41. generic applications or not,
42. then everybody knows that
43. Bitcoin is not generic
44. because in the Bitcoin platform,
45. it is only tailor-made for the processing
46. of the Bitcoin transactions.
47. But on the other hand, Ethereum and Hyperledger,
48. they both can be considered as generic blockchains
49. because they are designed
50. for people who want to create
51. new applications, new projects
52. on the blockchain platform.
53. If you look at whether
54. the blockchain produced
55. by the platform is a permissionless
56. or permissioned blockchain,
57. both Bitcoin and Ethereum
58. are basically public
59. because they can allow users
60. to join the blockchain
61. without any verifications.
62. But on the other hand, if you
63. look at the design principle
64. for Hyperledger because you
65. want to help the enterprises
66. to create their own blockchain
67. for their applications,
68. so that's why they
69. put a criteria there,
70. only the trusted parties that can go through
71. a verification process can be allowed

72. to join the blockchain, so
73. that's why we will consider
74. Hyperledger is a permissioned blockchain.
75. Now in that case, then you can see that Hyperledger,
76. sometimes, people will consider that
77. it's not a fully decentralised blockchain.
78. If you look at the consensus algorithms or models,
79. then you can see that Bitcoin will,
80. of course, use the original design, proof of work,
81. and Ethereum, at the beginning, they also adopted
82. the proof of work as the consensus algorithm
83. for their system.
84. But however, they find it, right now,
85. the performance, that the efficiency is not good enough.
86. So right now, what they are doing is they try to move
87. from proof of work to proof of stake right now.
88. Hyperledger, the design principle is that they hoped to have
89. a framework so that different enterprises
90. can create their own blockchain systems.
91. So that's why, in this particular area,
92. in Hyperledger, it's very flexible.
93. You can pump your own consensus algorithms
94. into the blockchain design.
95. So basically, you can use proof of work, proof of stock,
96. and also, even other consensus algorithms
97. you can come up with that are applicable.
98. If you're looking at smart contract,
99. now Bitcoin is not designed
100. for people to write new applications.
101. They only process the Bitcoin transactions.
102. So that's why, in Bitcoin,
103. they will not support smart contracts.
104. But on the other hand, both Ethereum and Hyperledger,
105. they both support smart contracts.
106. And finally, if you look at the last criterium,
107. then, of course, Bitcoin has the cyber currency
108. as Bitcoin attached to the platform
109. and Ethereum also has its own
110. cyber currency called Ether.
111. But now, on the other hand,
112. Hyperledger does not want to stick
113. to any cyber currency or cyber tokens,
114. so that's why they don't have any
115. cyber currency attached to it.
116. Before we end the module,
117. I want to talk about a trilemma.
118. Now, you know that, actually,

119. what blockchain wants to do is
120. to achieve three properties:
121. the decentralisation, the security,
122. or people usually mentioned it
123. as consistency integrity issue,
124. and finally, if you want to put
125. it in real applications,
126. we want it to be scalable, scalability.
127. If you look at these three platforms,
128. then obviously, none of the platforms can achieve all
129. these three properties simultaneously at the same time.
130. Of course, the security or the integrity must be satisfied
131. by any blockchain platform,
132. otherwise it's not usable for any applications.
133. This is the original design principle for blockchain,
134. so that's why we want to make sure
135. that everyone there is consistent and secure.
136. If you look at Bitcoin, Ethereum, Hyperledger,
137. basically, all three can achieve this property.
138. If you look at the decentralisation, as I mentioned,
139. only Bitcoin and Ethereum are
140. permissionless blockchains.
141. So in other words, they are fully decentralised.
142. But on the other hand, if you look at Hyperledger,
143. they try to make a verification process there in order
144. to check whether the party can
145. join the blockchain or not,
146. so it's not fully decentralised.
147. But then, on the other hand, if you look at Bitcoin
148. and Ethereum, because they
149. use this proof of work to do
150. the consensus algorithm, so they slow down
151. the efficiency of the platform.
152. Hyperledger allows you to use
153. all kinds of consensus algorithms.
154. I hope you start to understand the trade-off between
155. a permissionless blockchain and the efficiency.
156. Now, if in a permissioned blockchain,
157. the parties that can join the blockchain
158. are actually trusted parties, so that's why you can see,
159. in the Hyperledger platform,
160. we actually can achieve a more scalable platform
161. than the Bitcoin and Ethereum.

3.2.1: What is Ethereum? (with Charles d'Haussy from ConsenSys)

1. Ethereum is the second generation of blockchain.

2. It really helps to programme and use smart contracts
3. and gets much more complex
4. in value adding propositions on a shared network.
5. You might have interacted on the Ethereum
6. through ERC20s
7. which helps to raise money
8. and support and fund different projects.
9. Some of you may have played with CryptoKitties,
10. for example. some other people
11. are using Ethereum blockchain without knowing.
12. Ethereum blockchain is used to take browser
13. by the United Nations
14. or the World Bank to help refugees.
15. The Ethereum blockchain is used for
16. creating digital identity
17. for people which don't have identity.
18. The Ethereum blockchain is used in financial services
19. to coordinate and
20. disintermediate financial services as well.
21. The Ethereum blockchain is used in the gaming industry
22. to play and work with different digital assets
23. which are created from the the digital games.
24. The Ethereum blockchain is
25. the second biggest blockchain in the world
26. which brings together
27. more than 300,000 developers today.
28. Ethereum is a shared platform, totally trustless,
29. with more than 10,000 different nodes.
30. More than 300,000 developers in the world
31. are developing open source software
32. on the open source platform, that is Ethereum.
33. Being open source, the Ethereum blockchain
34. allows anyone to benefit from the progress
35. of the world community.
36. The recipe of software on the Ethereum blockchain
37. is open source.
38. You can bring on your own ideas,
39. you can build on the ideas of someone else,
40. in a very affordable way.
41. The innovation on the Ethereum blockchain
42. is not only coming from one country or one city,
43. It's distributed all over the world.
44. Everyone benefits from the platform
45. and it's really the benefits of the open source software.
46. The Ethereum blockchain builds the Web 3.0.
47. It's an innovation for everyone, from everywhere.
48. It's not only Silicon Valley innovation

49. dominating the world,
50. it's everyone from Asia, Europe, US and Africa…
51. building a joint platform, a common platform
52. for innovation and entrepreneurs.

3.3.1: What is Ethereum's Place in Today's FinTech Ecosystem? (with Charles d'Haussy from ConsenSys)

1. So what is Ethereum and what is Ethereum's place
2. in today's blockchain and FinTech ecosystems?
3. The history of blockchain started more or less in 2009
4. with the Bitcoin blockchain,
5. which was the first experimentation
6. on distributed ledgers.
7. As this blockchain, Bitcoin, still exists.
8. It has demonstrated good value.
9. It has demonstrated long lasting performance
10. and securities and a lot of value has been created
11. around this Bitcoin blockchain.
12. But this blockchain is also so early and so old,
13. its technologies can only deliver so much.
14. So back in 2013-14, there were a lot of thought leaders
15. and technologies which thought
16. how they could improve
17. and basically go to the next step
18. building on the fundamentals
19. and building on the idea behind the Bitcoin blockchain
20. to build something which gets smarter in a way.
21. And that's where the Ethereum blockchain
22. started to arise
23. from different technologies working together,
24. among them, Vitalik Buterin, as well as Joseph Lubin,
25. the founder of ConsenSys later on,
26. and they work with different groups of people
27. to basically create a distributed computer.
28. And they created the first concept of "smart contracts",
29. where really, you get this technology
30. of coordination getting much smarter,
31. not only registering transactions.
32. You gave me something,
33. I put something in my wallet,
34. and the money is out of your wallet and in my wallet,
35. but getting something which
36. gets much more capacities,
37. with having some kind of a virtual machine
38. within the network
39. where you can really start to get "smart money".

40. You can get “smart contracts”
41. and you can start to have conditions
42. on all the distributions
43. and all the coordination works you want to do.
44. So to speak, to Ethereum’s smart contracts,
45. what are some useful Ethereum smart contracts
46. and actually what is a smart contract?
47. So a smart contract is basically a contract,
48. so it’s something which will work with
49. input and output.
50. If you want to have an online voting system
51. and you want this voting system to be decentralised,
52. you will design a contract which will
53. basically identify everyone around us,
54. all the people involved in this vote,
55. register their vote, and depending on the votes
56. which have been recorded by the smart contract
57. in a trustless manner,
58. the smart contract will issue the results of this vote.
59. You can also decide, for example,
60. that the smart contract will be
61. some kind of virtual entity
62. existing only on the network in a trustless manner,
63. or distributed manner.
64. And if we agree that I’m going to work for you
65. for a couple of days and you’re going to pay me
66. a couple of hundred dollars for that,
67. the smart contract will be basically doing the arbitration
68. and making sure that I did the work,
69. so I will document to the smart contract
70. I was working for you and I delivered the job.
71. And then, the smart contract
72. will order the money from you
73. and after you receive the proof that I was working,
74. the contract will give me the money,
75. for example, for some work.
76. It’s a kind of an escrow system, which is distributed.
77. But, from this escrow use case,
78. you can go with much more complex
79. kind of transactions
80. and much more complex kind of works.
81. So today, you see people building stock exchange,
82. for example, on the blockchains.
83. You see people building a full set of
84. contractual relationships between companies
85. and individuals on the blockchain also.
86. And what it brings, it’s a very low cost

and very inclusive technology,
and very inclusive way
to design interactions between people and companies
and/or companies to companies.
So what you will see in the coming years,
and it's already starting,
it's really like a lot of the non-digitalized
kind of relationships we have
and a lot of non-digitalized transactions we have,
moving in a digital world
and a lot of these interactions
will happen on the blockchain because it brings
a very low cost and trustless platform
for all these people to interact together.
So think of a working contract,
think of maybe the proof of you owning your apartment
or your piece of land, thinking of your identity.
Instead of having the data kind of owned and managed
by some big corporations,
you will very soon be able to own
all the data about your identity,
your behaviours online,
your different habits on the new internet,
and being able to share them with the people you want
and possibly, also monetize them.
So the blockchain in the context of the internet,
the blockchain technology and the Ethereum technology
is bringing what we call the Web 3.0.
So it's really an evolution
and a new layer of technology
on our internet experience.
So in the future, you will see in terms of blockchain
will not come to you in a very complex manner.
Most probably it's a blockchain
and we hope very soon will be totally invisible for you.
And the same way you send email today,
you don't really realise that there is so many encryptions
being done, there is so many different
stack of technology being used.
The Web 3.0 will bring you more value
and will appear to you as fairly similar
to what you're doing today,
but with a very new experience.

3.4.1: Trustlessness and Immutability of Blockchain Technology (with Charles d'Haussy from ConsenSys)

1. What we mean trustless technology is that,
2. if a rural bank away from Manila,
3. is confirming that they gave to you,
4. for example, a loan,
5. or they give to you a bit of cash
6. because you came to visit them,
7. we can basically document that
8. and this transaction is written in a trustless way
9. on the ledgers, which at the end of the day or every hour
10. can be basically rebalancing the ledgers.
11. So every transaction is documented and immutable.
12. So what do you mean by immutable?
13. So immutable means when you build
14. a blockchain infrastructure,
15. you build a coordination platform
16. between different parties.
17. And if one of the players, one of the bank for example
18. or one of the rural bank or one of the ATM, for example,
19. is claiming that $100 was given to someone,
20. so there is $100 less in this office,
21. the data will be recorded one time and shared
22. between all the different actors so everyone will know
23. that there is for example, in your branch $100 less,
24. and this cannot be changed anymore.
25. So there is no way for anyone to fake the information.
26. There is no way for anyone to play the system,
27. because the system is distributed
28. and the system is trustless.
29. So we share the same infrastructure.
30. If there is something happening in my branch,
31. it's recorded.
32. If there is something happening in your branch,
33. it's also recorded and I cannot change the records.
34. The records are immutable.
35. So I know exactly what has been happening
36. and I will trust what you will declare to me
37. because I will be able to cross check that
38. with the transactions from the blockchain.
39. So it's not only about building the trust,
40. but it's all about automating all the kind of book records
41. and audits and declarations between different parties.
42. All of this is automated on the blockchain
43. and also reports come to you automatically.
44. So are there any disadvantages to trustlessness,
45. to immutability on the blockchain?
46. There is no disadvantage to trustless in my opinion.
47. I think this is a very strong value proposition.

48. If we can work and collaborate at scale,
49. between so many people and entities,
50. it brings value, it brings access.
51. Now when they are immutable, there is always
52. a question mark, do you want to have always
53. on the blockchain a record of every transaction?
54. In this case, you will use encryption technologies
55. where we will be able to document each other
56. and trust each other about
57. some transactions being made
58. but without having all the transparency
59. about these transactions.
60. Maybe you don't want the world to know
61. that you've been taking $100 from your bank account.
62. So there is encryptions capabilities nowadays
63. in the blockchain solutions we deploy,
64. to allow you to still record a transaction,
65. so we know there is $100 less in your bank accounts,
66. but the world blockchain does not know about that.
67. This is where we are coming into the game
68. what we call the different layers in the blockchain.
69. So you might have a backbone
70. which is the Ethereum blockchain
71. and you build some applications on certain layers
72. on the top of this base layer
73. where you're going to run transactions.
74. And in case of any problem, you're going to come back
75. to the main net, is what we call the main net,
76. the backbone of the blockchain
77. to basically do the arbitration and realise,
78. was there transactions happening?
79. Yes or no?
80. But all of these transactions can happen
81. on what we call sidechain or layer two chains,
82. where you don't have to document to the world
83. about everything in your life.
84. So is everything on the main net public,
85. publicly accessible?
86. All the data is publicly accessible,
87. but you can treat this data also.
88. So you can possibly, for example, we can share
89. on the main net a hash about one transaction.
90. So we know the transaction is there,
91. but only you and me
92. we'll be able to understand
93. what is this transaction about.
94. For the rest of the network, people will just see a series

95. of encrypted numbers which are meaningless to them.

3.4.2: Proof of Work and Proof Stake (with Charles d'Haussy from ConsenSys)

1. When we talk about the Ethereum blockchain,
2. what is meant by it runs on a "proof of work" protocol?
3. So that's a very good question.
4. So Ethereum blockchain was launched in 2015, right?
5. And the way as a security of the network was designed
6. was by using some miners, which were basically
7. scanning all the transactions
8. and bringing them in blocks after blocks,
9. so this is why we call them a blockchain.
10. And this activity of scanning
11. and proving all of those different transactions
12. and putting them into blocks is called mining today,
13. and it's called a proof of work.
14. The Ethereum, what we call the Ethereum 2.0,
15. is around the corner.
16. This is being delivered right now.
17. And there will be a transition from proof of work,
18. where you're gonna use machine
19. and computers to look at all as the transactions
20. and validate these transactions on the network.
21. We got to move from machines doing it
22. to purely software
23. using a bonding system where people will be basically
24. using software to validate and
25. build validated transactions
26. and build the blocks,
27. and using a bond or so to make sure
28. that these don't validate the right transactions
29. or start to play with the system.
30. They might be losing their bond.
31. So we are moving from a proof of work system
32. to a proof of stake system, staking being a bond
33. and you put a little bit of Ether as a poof,
34. as a kind of a bond,
35. to guarantee that you will do a proper job.
36. So what happens when you don't do a proper job?
37. You lose your bond.
38. So you're incentivized to do a proper job.
39. And there is also a system that the job is being made
40. by different people at the same time
41. and the people are checking the job of each other,
42. so I cannot claim you're not doing a good job alone.
43. Different people need to basically, look at your work

44. and say, okay, he has been
45. basically faking the transactions
46. and a certain number of people all agree
47. that you are faking your transaction.
48. So the system will basically grab your bond
49. and you're losing your bond.
50. So who makes that distinction?
51. Who says user X is making bad transactions?
52. There will be thousands of miners
53. and thousands of validator in the new system,
54. so we will not call them miners anymore, but validators.
55. And these thousands of validators
56. have a system in place
57. where they're cross-checking each other
58. and it's purely mathematical
59. and purely organized by the network itself.
60. So everyone checks the work of everyone
61. and when there is certain number of people flagging
62. misbehaviors from someone, then there will be
63. an automated system where the bond
64. of this person will be just burned.
65. So instead of using thousands of computers,
66. you're using thousands of validators
67. which are much less impacting the environment.
68. So yes, it's beneficial.

3.5.1: Tokenizing (with Charles d'Haussy from ConsenSys)

1. So tokenizing is one of the
2. value propositions of blockchain.
3. And today, many people are looking at this way
4. to basically create digital shares
5. of many illiquid assets.
6. That's what tokenization is.
7. So if you think of a building,
8. today if you want to buy a building, you buy a building.
9. And you buy the full building.
10. And this can be very costly, and the building is a building
11. and there is one proof of ownership of this building.
12. If you want to digitalize this building,
13. how are you going to create shares?
14. And how will these digital shares
15. of the building be issued?
16. And what is the most efficient way to do it?
17. Some people are doing this for many, many years
18. by creating a very expensive fund,
19. using a lot of lawyers to create a fund,

20. which he presents a building, and then selling shares
21. of the fund which owns the building.
22. And this process is actually very paper-intensive
23. and extremely costly,
24. and not really affordable for many people,
25. and not easy to distribute after that.
26. So this movement of tokenization is thinking
27. all these illiquid assets which we are surrounded by,
28. should it be a real estate,
29. should it be company shares of non-listed companies.
30. So before an IPO company shares exist.
31. Maybe, your bakery is a company down the street,
32. and you can be a shareholder of this bakery.
33. Or you can be a shareholder of a project
34. which will be happening for a few weeks
35. and then fade out.
36. So when you go through the process of tokenization,
37. you create digital shares of something
38. which is not liquid,
39. or something which is not adding avenues to be exchanged.

3.5.2: What is a Token? (with Charles d'Haussy from ConsenSys)

1. What is a token?
2. So a token is a vehicle built on the blockchain
3. to create values
4. or to have some kind of specifications, right?
5. So the first token you've seen
6. on the Ethereum blockchain was the ERC-20.
7. So the ERC-20 was able to hold values,
8. to move value from one place to another,
9. from one contract to another,
10. from one user to another,
11. and just bring the whole value in it.
12. Since then, the technology keeps making progress,
13. so you've seen many different type of ERCs.
14. So you can think of many different kind of vehicle
15. and wrap you can put on this Ethereum blockchain.
16. So you have, nowadays, ERC-721, you've got ERC-1400,
17. you've got ERC, you've got plenty of ERCs,
18. which will all have very specific features
19. towards very specific properties.
20. So some ERCs, for example, as the 721,
21. is a type of ERC which cannot be cut.
22. So they exist in a very limited numbers of units
23. and you cannot cut an ERC-2071.
24. So if you think of an ERC-20, for example,

25. they are called fungible.
26. So fungible tokens means if I give you one token
27. and you want to share half of it with someone,
28. you can basically cut it in two and send 0.1 Ether,
29. for example, to someone and send 0.3 to someone else.
30. So they have the same, I will say, specificities as money.
31. Some of the tokens will be called non-fungible tokens.
32. So if I give you one non-fungible token,
33. it's one token only and this is the only one.
34. And then, it creates many different properties
35. and it brings many different use case for this one token.
36. Some other tokens will have properties that they will be
37. only exchangeable between accredited people.
38. So for example, if I want to sell company shares,
39. for example, you and me can exchange company shares
40. because we are adults
41. and because we qualify to buy and sell shares.
42. But maybe these shares should not be
43. in the hands of kids
44. or should not be in the hands of people
45. which are living in another country
46. with other regulations.
47. So we can start to really create some kind
48. of programmable money and programmable vehicles.
49. A token is a vehicle which moves in the blockchain
50. between the smart contracts
51. and lives in the blockchain.
52. You can own it, you can share it, and all of these vehicle
53. will have different specifications,
54. and these specifications gives them different properties
55. for different type of use.
56. So the most popular is the ERC-20,
57. but since the birth of the ERC-20,
58. there is probably hundreds of different type of tokens,
59. which comes with all different specifications.
60. So think of a token of a car, like a car.
61. Some cars are designed to transport families,
62. some cars are designed to be extremely fast,
63. some cars are designed to deliver mails and parcels.
64. Some cars are designed to move food all around the city.
65. So think of a blockchain of a big infrastructure
66. and you need to have different tokens for different uses.
67. And that's what a token is.

3.5.3 [Industry Guest Speaker] Tokenizing Shares and Fund Raising (with Charles d'Haussy from ConsenSys)

1. What do you think about the state of the ICO?
2. Is the ICO dead or is it still a valid way
3. to raise money for a blockchain project?
4. So when the ERC-20 and the Ethereum was launched,
5. many people realized that there were many ways
6. to use this technology.
7. And one use of this technology
8. was raising funds for projects,
9. what we call an ICO.
10. So a project would at the time create a token
11. which will be sold to investors
12. to basically fund them and help them
13. to start to bring people together
14. and build the product.
15. So this ICO phenomena has been very popular back
16. in 2017 and 2018, and then now has kind of faded out
17. because many of these projects
18. have not always been delivering
19. what they were promising.
20. Some of them have been doing fantastic,
21. some them have been doing poorly
22. and I think the market has been kind of maturing.
23. So you will probably not see as many ICOs as before.
24. You will see them much more structured,
25. maybe they will not be named ICOs,
26. but the mechanism of funding projects
27. using the blockchain will remain,
28. but will come in different ways now using
29. more complex types of tokens or complex types
30. of relationships or mechanism of raising funds,
31. which will give more guarantee to the investors
32. and also more guarantees to the people raising money.
33. But there is always a need to raise money,
34. there is always a need to digitalize things around us.
35. So the new mechanism are coming up.
36. Maybe not they will not be called ICO anymore,
37. maybe STOs there are many different ways to use
38. and benefit from the technology to fund projects.

3.6 What is Hyperledger?

1. Before we start, let's talk about one important point
2. about the differences between
3. Ethereum and Hyperledger.
4. Basically, Ethereum and Bitcoin are very similar.
5. They are designed as a single platform,
6. but on the other hand,

7. Hyperledger basically is a family
8. of multiple platforms developed for different types
9. of applications for enterprises.
10. In fact, these platforms are very flexible
11. and they have different characteristics,
12. they can fit into different types
13. of applications for the enterprises.
14. So therefore it is more flexible for the developer
15. to develop appropriate applications
16. using different platforms.
17. The audience, if you are interested in Hyperledger,
18. can try to learn more on the
19. differences of these platforms,
20. so that you can always pick the right platform
21. to develop your own applications.
22. Now let's start to compare Hyperledger and Ethereum.
23. Now basically all these five categories,
24. or five perspectives, are interrelated.
25. So we need to first look at their design objectives first.
26. For Hyperledger, it's mainly designed for enterprise,
27. so mainly for B2B applications,
28. but on the other hand,
29. for Ethereum, they aim at B2C applications.
30. Now in this case, then you can see that Ethereum
31. will allow users to join the chain on their own.
32. So therefore, Ethereum will provide a public chain
33. for the applications.
34. But on the other hand,
35. because Hyperledger aims at enterprises applications,
36. though they are supposed to
37. be a permissioned blockchain
38. so only registered or permitted users are allowed
39. to join the chain, the blockchain.
40. Now if you understand this,
41. I hope you still remember the differences
42. between a public chain and a permissioned chain.
43. Now for public chain,
44. we actually require some incentives
45. for miners to work on the chain.
46. So therefore,
47. in Ethereum, we need to give
48. the miners incentive rewards
49. in order for the miners to work on it.
50. But on the other hand,
51. a permissioned chain of the Hyperledger
52. is basically for the consortium.
53. So basically they are willing to contribute

to the blockchain and they are registered users.
So in other words, we do not really need
to give them incentives for the miners to work on it.
Now this also explains why,
if you look at the built-in cryptocurrency,
then Ethereum has its own Ether.
But on the other hand, actually,
Hyperledger does not require such a cryptocurrency,
for the reward of the miners.
Now, if you look at it carefully
and you understand everything I just talked about,
then you can see that Ethereum will allow users
to join the chain freely.
But on the other hand,
Hyperledger has more restrictions
on who can join the chain.
Basically all the users, alone users or registered users.
So in other words, the behaviour
of the users in Hyperledger
are in a controlled manner.
But on the other hand for Ethereum,
because the platform may not know
the real identity of the user,
so the behaviour of the users
is more difficult to control.
Now this also explains why,
when we look at the consensus algorithm,
then Ethereum basically is using the proof of work
in order to guarantee the security of the whole system
and therefore you will take a longer time
in order to process each transaction.
But on the other hand for Hyperledger,
then the user or the developer can have a choice,
more flexible to choose an
appropriate consensus algorithm
for their applications.
In other words,
the consensus algorithm
used by the Hyperledger,
can run faster and require
less resources, less storage
and can be more flexible.
And in fact Hyperledger
even has an option for you
to pick that you do not
require a consensus algorithm
to work on the chain.

101. And so if you really understand this,
102. then you can quickly imply
103. that Hyperledger is more scalable.
104. And if you look at the number
105. of transactions per second,
106. actually Hyperledger can go up
107. to thousands while Ethereum,
108. at most is like 15 to 20
109. transactions per second.
110. So you can see the differences.
111. Basically it's because of
112. the consensus algorithm
113. and also Hyperledger is under
114. a controlled envoronment,
115. but on the other hand, Ethereum is not.
116. Then we come to the final perspective.
117. How about privacy and confidentiality?
118. For Ethereum, it's similar to Bitcoin.
119. For the identity,
120. we basically use the public key
121. as the address of the of your account.
122. So, in other words, we
123. are using the pseudonyms
124. and therefore, the identity
125. off the sender or the receiver
126. may be hidden.
127. But on the other hand, as
128. we talked about before,
129. the transaction may still be traceable.
130. And in the basic design, of course,
131. for the transaction content,
132. everybody can see the actual content,
133. so it's publicly viewable.
134. Now if you look at Hyperledger,
135. for example, one of the platforms is called Fabric,
136. the identity is basically
137. anonymous and only the authority,
138. when they do the registration,
139. can reveal the real identity of the sender
140. and the receiver.
141. Otherwise, you know the identity is protected.
142. And for the transaction content,
143. in Hyperledger, they have better access control.
144. so that transaction content can be encrypted.
145. And the access control can be applied
146. to allow some of the users to look at it,
147. while the others may not be able

148. to access the transaction details.
149. Now this is actually one of the characteristics
150. decided in Hyperledger.
151. The main reason is that,
152. they enable the company to do business
153. with different partners.
154. Even for the same product,
155. they can have different discounts or different prices.
156. So only some of the users can see these transactions,
157. while the others may only see their own transactions.
158. So let me summarise.
159. One thing I talked about,
160. Hyperledger is not for the public.
161. It's mainly for consortium.
162. And Hyperledger has well controlled users
163. and fly-granted access control for transactions.
164. So therefore there's no need
165. to have a very secure consensus protocol
166. and the trade-off is we can have a faster
167. and lighter consensus algorithm.
168. So that's why Hyperledger can actually run faster
169. and can be more scalable.

3.7.1 Hyperledger Blockchain Technologies (An Interview with Brian Behlendorf from The Linux Foundation)

1. How about we start with, "What is Hyperledger?"
2. To talk about Hyperledger,
3. first I want to talk about the Linux Foundation
4. and the Linux Foundation is a non-profit consortium
5. of over a thousand different companies
6. started about 17 years ago to help figure out
7. how do we make open source projects sustainable.
8. And how do you build
9. a vibrant, healthy commercial
10. technology ecosystem around things
11. like the Linux operating system, initially.
12. And the trick there was to figure out
13. the right balancing act between organizing
14. and supporting all of the open-source developers
15. who want to contribute code to a common platform,
16. but also, giving their employers
17. and other companies in that space enough room
18. and enough support to build commercial activities
19. on top of the common code.
20. So having both that developer hat and a company hat,
21. and organizing the companies to help support

22. kind of a small team of funded staff
23. at the Linux Foundation
24. to coordinate those efforts,
25. kind of like an air traffic control tower.
26. They figured out how to make that work
27. for the Linux operating system.
28. And then, it quickly became
29. clear that you could apply
30. that model to other technology domains,
31. things that are immediately adjacent
32. to the operating system, such as using Linux
33. inside of telco hardware or inside of automobiles,
34. things like security libraries, like OpenSSO,
35. and then, two-cloud computing,
36. like the Cloud Native Computing Foundation,
37. which is the home for Kubernetes,
38. and all of these additional projects the model was,
39. companies that are members
40. of the Linux Foundation also
41. become members of these
42. projects and contribute funds
43. and help those kinds of projects take off.
44. And so, in December 2015, the Hyperledger project
45. was announced with 30 initial members.
46. And some of those were the
47. names that you would expect,
48. like IBM and Intel.
49. Others were unusual, like J.P. Morgan
50. and a company called Digital Asset,
51. who you'd not heard of in an
52. open-source context before,
53. but it was really a coming together of companies
54. who realised there was something interesting about
55. distributed ledgers, about blockchain technology,
56. that was distinct from all the
57. cryptocurrency applications,
58. that really deserved a place
59. to be able to be explored,
60. to develop some underlying technology,
61. explore those use cases,
62. and figure out, can we grow these technologies
63. to be production-ready and enterprise-ready?
64. So I joined in June of 2016 as Executive Director.
65. I used the term "nerd diplomat"
66. to, kind of, better describe what I do.
67. I am a Linux Foundation employee,
68. as are 10 of my staff report, as well as four people

69. based here in Hong Kong, actually.
70. We do two different things.
71. We help organize the open-source developers.
72. We don't write the code ourselves.
73. We just try to make sure that there is enough process,
74. enough structure, enough common elements,
75. like the same open source licence
76. is used across all the code,
77. which is the Apache Licence, but really,
78. helping them figure out how
79. do they focus their efforts
80. on what is a portfolio of technology projects.
81. Some that you've heard, like Fabric, Hyperledger Fabric,
82. which is very widely used,
83. and some of them brand-new projects,
84. like Hyperledger Transact or Besu,
85. which I can talk about in a bit.
86. But really, the idea is that there's this conveyor belt
87. that we put software projects on
88. to get them to the point where
89. enterprises can use them.
90. And then, the second thing we do at Hyperledger
91. is help encourage companies
92. to build on top of this code
93. and help them understand how to build
94. support models around it or incorporate it
95. into their products or services,
96. or simply be more effective end users of the technology.
97. And that's really the main benefit we give to companies
98. that pay money to support it,
99. is helping them with marketing, doing events.
100. But there are things we do that really will help
101. even the broader ecosystem,
102. even people who aren't members of ours,
103. so that's kind of, in a nutshell, what Hyperledger does.

What Are the Differences Between Hyperledger and Other Blockchain Technologies? (Brian Behlendorf from The Linux Foundation)

1. So, what do you think are
2. the differences between Hyperledger
3. and other platforms,
4. other blockchain platforms?
5. What the major difference is?
6. So, we have a number of platforms, actually,
7. within the Hyperledger greenhouse,
8. as we call it.

9. And we use the greenhouse metaphor to try
10. to help people understand we have some technologies
11. that are very mature, some technologies
12. that are still starting out,
13. but they share the same oxygen,
14. the same airspace.
15. They sometimes will cross pollinate each other.
16. And so, to talk specifically about
17. some of the frameworks that
18. we have, Hyperledger Fabric
19. was designed to be a high-performance
20. distributed ledger system that is highly programmable.
21. So you can use it for digital assets.
22. You can use it for tracing of supply chain processes.
23. You can use it for all sorts
24. of complex business orchestration purposes.
25. It was certainly built for enterprise use cases,
26. which means it has a lot of power.
27. It also has a lot of complexity to it at times,
28. but it's now running on every
29. major cloud provider in the world.
30. It offers Fabric as a service and lots
31. and lots of companies are providing products
32. that incorporate it and provide support for it.
33. One of the differences between it
34. and say, some of the public ledger technologies,
35. one of those is performance.
36. In the lab, it can do 3,000 transactions a second,
37. kind of under ideal conditions, admittedly,
38. but that's a much better number
39. than you'll see in most others
40. and there's work underway
41. to get that up to 20,000 transactions per second.
42. There are lots of parameters that you can tune
43. when different things are important to you,
44. like supporting a larger
45. network might be more important
46. than a higher transaction rate,
47. so you can adjust certain things about it.
48. And really, it's the standard now out there
49. in the financial services space
50. in supply chain traceability.
51. Its deployment is pretty widespread at this point.
52. Hyperledger Sawtooth was kind of our second project
53. and it's a little bit more of an experimental platform.
54. It in some ways is more true to Nakamoto Consensus
55. of kinda probabilistic finality.

56. And it has some novel consensus mechanisms,
57. like proof of elapsed time,
58. and it has better abstraction layer between
59. the smart contract layer
60. and the ledger layer that has made it easier
61. to bring in other smart contract languages,
62. like Ethereum or Solidity or DAML,
63. which is the Digital Assets Markup Language,
64. and support those kind of on top of Sawtooth.
65. And what we find actually is the nature of competition
66. in an open-source space isn't
67. the same as Beta versus VHS.
68. The nature of competition in open-source,
69. especially when they're under the same roof,
70. like they are at Hyperledger,
71. is people want to learn from each other.
72. They wanna understand what have you built
73. that is cooler than what I've got.
74. And we can bring down a bit of the ego
75. and certainly, bring down kind of the financial incentives
76. for parties to split.
77. And in fact, there's one part of Sawtooth
78. that has been broken out
79. and is being put over to Fabric,
80. which is that ability to run
81. different smart contract systems.

The Rapid Growth of Blockchain in Meeting Industry Demand in Asia Pacific Region (Julian Gordon from The Linux Foundation)

1. Hyperledger is the blockchain project
2. of the Linux Foundation.
3. We are open-source with over
4. 270 companies around the world
5. as our members and a thriving open-source community
6. of developers working together
7. on blockchain applications for business.
8. So, we are very well placed to see
9. and to nurture the rapid growth of blockchain
10. in meeting industry demand in Asia Pacific
11. and around the world.
12. It is exciting times
13. in the world of blockchain for business.
14. Blockchain applications are evolving from pilots
15. to real world platforms,
16. and we see a lot of interest and development
17. in Asia Pacific markets,

18. from Australia to India, Japan,
19. Singapore, Thailand, all across the region
20. and most especially I would say in China.
21. Projects are going into production in many industries
22. and bringing benefits including
23. substantial cost reductions,
24. dramatic increases in efficiency, transparency,
25. and security, and the development
26. of new business models and opportunities.
27. At Hyperledger, we host a greenhouse
28. for blockchain projects.
29. We provide expertise, infrastructure,
30. and support so that developers and companies
31. can collaborate in an open-source environment
32. on blockchain technologies for business.
33. Our projects have
34. a broad collaborative software community around them.
35. Everyone is welcome to participate.
36. Some are in incubation,
37. and others are active being used in hundreds of POCs
38. and implementations globally.
39. Six of the projects are distributed ledgers.
40. They are in different stages of development.
41. Hyperledger Fabric, Hyperledger Sawtooth,
42. Hyperledger Row and Indy,
43. which is for self-sovereign identity,
44. are already active being used
45. in live business applications globally today.
46. Hyperledger Besu is an Ethereum client
47. that runs on both private networks
48. and the Ethereum public network.
49. We have four software libraries
50. including Hyperledger Quilt
51. for blockchain interoperability and Ursa,
52. which is a cryptography library.
53. We have tools such as Hyperledger Calliper,
54. which is a benchmarking tool for blockchains.
55. We have also domain specific projects
56. such as Hyperledger Grid,
57. which is for supply chain applications.
58. So, what are the main industries
59. where we see blockchain having a real business impact
60. in Asia Pacific?
61. Hyperledger technologies are being developed
62. for business solutions across virtually all industries,
63. including energy, manufacturing, telecom, education,
64. transport, and in the public sector.

65. But in Asia Pacific and globally,
66. we see the most activity
67. in financial services, supply chain, and healthcare.
68. In these industries, we already
69. see Hyperledger platforms
70. being used in live real world solutions.
71. In financial services, in areas such as capital markets,
72. equity trading, mortgage underwriting,
73. KYC, and anti-money laundering, corporate banking,
74. insurance, and particularly in trade finance.
75. For supply chain, we have areas
76. such as provenance tracking,
77. cutting bureaucracy at ports and customs,
78. IoT devices to detect poor shipping conditions
79. and title tracking for high value goods.
80. For healthcare, we have areas
81. including provider directories
82. and certification, patient-driven healthcare records,
83. insurance claims processes,
84. and the whole pharmaceutical supply chain.

Module 3 Reference Reading

References and Suggestions for Further Reading in Module 3

NOTE: We may come across information about comparisons of different blockchain platforms (note that those may not be based on the same 5 perspectives discussed in Module 3. Quite often we'll consider the comparisons from the domain of applications.

(1) Academic paper for reference

- Blockchain platforms: A compendium (Chinmay Saraf et al.)
- A comprehensive reference model for blockchain-based distributed ledger technology (Andreas Ellervee et al.)
- Taxonomy development of blockchain platforms: Information systems perspectives (Shehu M. Sarkintudu et al.)
- Comparison of blockchain platforms: a systematic review and healthcare examples (Tsung-Ting Kuo et al.)
- BLOCKBENCH: A framework for analyzing private blockchains (Tien Tuan Anh Dinh et al.)

(2) Information of some popular blockchain platforms

- Ethereum platform: https://www.ethereum.org
- Hyperledger platform: https://www.hyperledger.org
- Bitcoin: https://bitcoin.org/en/
- Corda: https://www.corda.net

- Ripple: https://www.ripple.com

(3) Industry articles and information on: tokenization, fund raising, and differences of ICO and STO

Will Asset Tokenization Revolutionize Fundraising and IPOs?

The Difference Between ICO and STO

5th ICO STO Report

Module 4 Blockchain Applications

Welcome to Module 4

Dear Learners,

Welcome to Module 4 – Blockchain Applications. In the last Module, we looked at the characteristics of three major blockchain platforms, Bitcoin, Ethereum and Hyperledger.

In Module 4, you will first be introduced to key selection criteria for blockchain applications by chief instructor Dr. SM Yiu. Then you will hear from our guest speakers, Dr. Paul Sin (Consulting Partner from Deloitte, China) and Anil Kudalkar (MD, MaGESpire Partners) w will share with us some real world use cases in enterprise blockchain including: trade finance, supply chain financing, cross-border connectivity, capital markets and government services.

Furthermore, our guest speaker Charles d'Haussy (Director Strategic Initiatives ConsenSys) will talk about how to deploy an application on Ethereum and some interesting use cases of ConsenSys on Ethereum.

Happy learning.

HKU Blockchain and FinTech Course Team

Module 4 Learning Objectives

After completing Module 4, learners should be able to:

- **understand the selection criteria for using blockchain for an application;**
- **list some use cases in real applications that use blockchain and why these use cases are good fits for the blockchain platform.**

4.1.1 Selection Criteria for Blockchain Applications (Part 1) Key Factors 1, 2, 3

1. Welcome to Module 4 of our Blockchain course.

2. Now in this module,
3. what we are going to do is,
4. we want to look at Blockchain
5. from the application point of view.
6. So we want to look at what applications
7. can make the model of Blockchain better.
8. Okay, let's review:
9. what are the characteristics of Blockchain?
10. Basically, Blockchain is a ledger.
11. A ledger means that it's a database of transactions.
12. So it's trying to store the transactions into the database.
13. And the second characteristic
14. is decentralised properties.
15. In other words we do not have a centralised
16. trust authority for the whole system.
17. And the third characteristic is immutable,
18. meaning if you put a transaction in the Blockchain,
19. you can never change or even delete it.
20. And of course it's transparent,
21. so that all the users can see the transactions.
22. Now all these are the good points of Blockchain
23. but Blockchain does have some limitations,
24. we also talked about in earlier sections.
25. For example, the scalability and
26. also the complicated trust or
27. decision-making model
28. based on some kind of assumptions.
29. So these are the characteristics
30. of a Blockchain system.
31. And on the other hand,
32. I also want to review with you
33. the limitation of having a centralised ledger,
34. meaning that we do have a trusted authority
35. to handle the system.
36. And we do have at least three disadvantages.
37. First of all, it might incur high transaction fee,
38. and the privacy issue because the trust authority
39. is able to look at all the transactions of yours
40. and of course the last one is the processing time.
41. When we talk about transaction processing time,
42. we refer to the case that maybe we need to involve
43. multiple parties in the transaction.
44. For example,
45. if you want to transfer money from one bank
46. to another bank overseas,
47. then you might involve
48. at least two banks or sometimes intermediary parties.

49. Or for similar tasks,
50. for example, if you want to open
51. a bank account in different banks,
52. or try to locate a product from multiple suppliers,
53. then we need to repeat the same procedures for
54. multiple times so it incurs a long processing time for it.
55. Now, we understand the advantages and disadvantages
56. of a decentralized and centralized ledger.
57. Then based on these pros and cons,
58. we want to make a good decision,
59. to see whether the application is good
60. for Blockchain platforms.
61. Now I hope you still remember the first characteristic of Blockchain:
62. Blockchain basically is a ledger.
63. Now, so the first question you should ask yourself is,
64. does your application require the system to
65. store, retrieve, or process transactions?
66. In other words,
67. does your application require a database?
68. Now if the answer is no, it means that you don't actually
69. need to store a database, then in this case, usually,
70. we will not go for Blockchain.
71. Okay, let me give you some examples,
72. then you will understand what I'm talking about.
73. For example, a bank may want to provide a service
74. to help the customer to calculate the interest
75. for a mortgage loan.
76. This service usually is anonymous, right?
77. Because they do not want to
78. remember or store any details
79. of the input given by their customers
80. and usually, their service is free.
81. Then, in that case, we do not need to store anything,
82. and the service just wants to calculate the interest
83. for a particular mortgage loan.
84. Then in that case,
85. we usually will not use Blockchain.
86. There are many, many similar examples.
87. For example, the audit department may want to provide
88. free services for people to calculate the tax,
89. or you can provide a website to help students
90. or professionals to calculate the answer
91. for some math problems, etc.
92. All these cases you are not going to
93. store all the transactions.
94. You just provide a service for calculations.
95. Then, in that case, we will not go for Blockchain.

So, first of all, you need to ask yourself
whether you need a database in the application.
Okay, the second one, also, we refer to
a characteristic of Blockchain.
You should ask yourself, do you have
a trusted centralized authority?
In other words, in the whole application,
do you have a party that you trust,
and he can actually control the system for you?
Now, if your answer is yes, then again,
you don't need to use Blockchain.
Let me give you a common example.
I think we all trust the immigration department
or the government, to maintain our traveling records
for going in and out of the country.
And also, they actually have
the authority to know about it
and in this case, you can see that the privacy issue
is not a major concern,
and in fact, we will believe that the authority
will handle it properly.
So in that case, we do have a trusted authority
that can handle our records.
Then, in that case, we do not need to use Blockchain.
There are many other examples, for example,
if we are talking about the
ownership information of properties,
the purchase records of the apartments,
we always trust the government,
and all this information
will be stored in the government database.
In that case, we do have a trust authority
to handle the information.
In other words,
there's no need for us to go for Blockchain.
Now the third question you should ask yourself
is about the transaction fees.
Now even though you might have a trusted authority,
for example the bank, who can handle
the transaction for you, but if the transaction fee
is too high, then you need to think about whether
you should go for Blockchain platform or not.
Okay, let me give you some examples.
If you want to transfer the money between banks
or you try to trade data, buy and sell data,
or you try to rent the apartment,
you will see that the agent in between

143. may charge you a high transactions fee.
144. Then, in that case, you may think about whether
145. we can go for Blockchain platform
146. in order to eliminate the centralized authority
147. to handle all these transactions
148. so that you can enjoy a lower transaction fee.
149. Now of course, usually the trust authority
150. will try to provide additional services
151. or add on services to you in this kind of services.
152. So you need to evaluate whether this service is worth
153. the high transaction fees, or will this service
154. be so critical that a Blockchain platform
155. may not be able to provide a similar service to you.

4.1.2 Selection Criteria for Blockchain Applications (Part 2) Key Factors 4, 5, 6

1. Question number four,
2. you also need to consider
3. whether your application
4. will involve multiple parties.
5. When I say multiple parties
6. I mean that the number
7. of parties is at least three.
8. Now, if the number of parties involved in the application
9. is less than three, then in that case,
10. we also do not recommend you to use blockchain.
11. Now, a major characteristic of blockchain
12. is this decentralised trust model.
13. In other words, we try to let the entities
14. who participate in the blockchain to make the decision.
15. But if the application only involves two companies
16. or even one company,
17. then if you try to use blockchain,
18. then you need to go for
19. a more complicated trust model.
20. Then, I think this is not necessary.
21. Okay, now let me give you another example.
22. Now, if two companies, they decide to join forces
23. to market a product, it's easy for them to compromise
24. how to store the transaction,
25. how to handle all the transaction process
26. for the transaction.
27. Then, in that case, I don't think we need to go
28. for the complicated trust model in the blockchain,
29. but I want to make a remark here.
30. When I say company,
31. I just used this term to refer to an entity.

32. Sometimes, even in one company,
33. they might try to put some
34. of the applications into blockchain.
35. If the company actually involves many departments
36. and the departments, they don't trust each other
37. or they do not want others to looks at their data easily,
38. then in that case,
39. we still consider this case a multiple-entity case.
40. Then, sometimes, we still try to
41. use blockchain to implement
42. some of the application in just one company.
43. For example, if a company has different branches,
44. one in Hong Kong, one in UK, one in US,
45. maybe they want to combine
46. their data to do something,
47. then, in that case,
48. they might not want others
49. to look at their data,
50. but they want to compile their data
51. to do some, for example, marketing purpose.
52. Then, in that case, they may try to put the application
53. on the blockchain.
54. And then, the next question
55. you should ask yourself is,
56. does your application involve
57. high frequency of transactions?
58. Now, if your answer is yes,
59. then again,
60. we do not recommend you to use blockchain.
61. The main reason is,
62. if you still remember our earlier sections,
63. we talk about the transaction rate of blockchain.
64. Now, the slowest blockchain transaction rate is like this.
65. They can only handle seven or
66. eight transactions per second.
67. Now, for comparison, if you look at Visa,
68. basically, they can handle
69. 2,000 transaction per seconds.
70. Now, then, in this case, if you try to put an application
71. with a very high frequency
72. of transactions into blockchain,
73. basically, blockchain cannot handle this kind of volume.
74. Then, it would be a disaster.
75. If you look at the internet,
76. people start to talk about new design of blockchain
77. and some of the blockchain platforms
78. that they claim that

79. they are able to handle 1,000
80. to 2,000 transactions per second.
81. Now, that may be the case,
82. but we do need more evaluation
83. in order to confirm whether
84. the performance is that good.
85. In other words, at this moment, I still think that
86. if your applications involve
87. high frequency of transactions,
88. maybe you need to think twice
89. before you go for the blockchain platform.
90. So, another example is if you're talking about
91. high frequency trading in stock market.
92. Basically, they are talking about almost a million
93. transactions per second, then definitely,
94. you are not able to use blockchain platform
95. to handle this kind of transaction volume.
96. The last question you need to ask yourself
97. before you really go for blockchain,
98. you need to think about whether you have
99. enough entities to maintain the blockchain.
100. In particular, one type of blockchain
101. is called permissionless.
102. Basically, it's a public blockchain,
103. so everybody can join the blockchain.
104. In this kind of blockchain, the trust scheme,
105. for example, if you're talking about proof of work,
106. actually requires quite a number of entities
107. to help to maintain the fairness of the decisions.
108. Otherwise, someone maybe able to cheat.
109. I give you a very simple example;
110. if your blockchain has a voting system to vote on,
111. which chain we wouldn't want to follow.
112. Now, if your chain only has 10 entities,
113. if six of them actually collude together
114. and then, they are able to, so in that case,
115. if you are not sure whether you
116. have enough users or entities
117. to maintain the blockchain,
118. then you also need to think carefully
119. before you actually move
120. to the blockchain platform.

Selection Criteria for Blockchain Applications (Part 3) Best Fit Applications

1. Now, on the other hand,
2. there are other characteristics

of the applications that fit very well
in a blockchain platform.
Now, let me try to illustrate some of them.
Now, the first one is
if the application will emphasize
on the chain of custody alone.
For example, I worry about
the origin of the medicine,
the food, or the wine, etc.,
then you know that
one of the big characteristics
of blockchain is once you
certify or verify something
and then, you put it in the blockchain
then, people cannot modify or change it,
so that integrity can be maintained.
So basically, what they are doing right now
is they will try to keep this chain of custody
in the blockchain platform,
so whenever the customer tries to buy a product,
they may just use the QR code.
Then, they can retrieve the whole chain of custody
of the product and then, they see
where the medicines come from
or the food comes from.
So this is one of the good characteristics
of the applications that will try
to use blockchain as one of the platforms.
The second characteristic is if the application
actually involves tedious procedures.
For example, they might involve repeated renovation.
For example, if you need to do job hunting,
then you know that the company usually asks
for your graduation certificate
or if you go for further study, they will again ask
for your certified graduate certificates.
And then, right now, what people are doing
is they will try to apply to the university
and pay the money and then, wait for the university
to send a certified copy to the companies
or to the universities
in order to verify your qualifications.
Or, for example, if you're trying to open a bank account,
then you need to show your identity proof,
address proof, in order to open a bank account.
If you go to another bank,
you have to repeat the same procedures.

50. Usually, it always takes time.
51. Now, think about it.
52. If we try to put all these in the blockchain,
53. for example, if the universities basically
54. will try to certify your certificate
55. and the certified certificate is already
56. put on the blockchain system
57. and then, what you need to do is
58. you just need to inform the university
59. that you're going to apply for this job
60. or apply to another university.
61. And the company can actually
62. get the certificate information
63. directly from the blockchain without any delay
64. as long as you pay for it of course.
65. And the payment actually can also
66. be done in the blockchain as well,
67. based on the smart contract procedure
68. we talked about in earlier sections.
69. So in this case, this kind of application,
70. if they involve tedious procedures, repeated validation,
71. is also very good for blockchain platforms.
72. My final example is about the applications that involve
73. multiple suppliers and multiple buyers,
74. kind of like many-to-many relationship.
75. For example, if you're looking for a product
76. from multiple suppliers or the love matching example
77. I used in an earlier section,
78. so if we do not have blockchain,
79. so what we need to do is
80. we need to register yourself
81. to every company separately
82. and then, pay the membership fees separately.
83. And then, you need to look at all the results
84. from the individual companies.
85. Then, it is basically a waste of time
86. and you need to look for these kind of suppliers yourself.
87. Now, on the other hand,
88. if we can create a common marketplace
89. or a better data trading place using blockchain platform,
90. then what we need to do is
91. we just can issue one request
92. for a particular product
93. and the suppliers in the
94. blockchain platform can basically
95. provide you all the information you require,
96. and then, you just pay for what you want.

97. So this is basically the three particular characteristics
98. of an application that fits very well
99. into the blockchain systems.
100. Now, finally, there is another key issue.
101. Now, if the application involves multiple parties
102. to join to participate in the blockchain system,
103. now you need to make sure that almost all the entities
104. will join the blockchain system.
105. Otherwise, for example, in a supply chain management
106. or in a mortgage loan evaluation,
107. if some party, they do not join the blockchain,
108. then this party will become
109. the bottleneck of the procedure.
110. Or basically, they will break the chain of custody.
111. In other words, you cannot retrieve everything instantly
112. from the blockchain
113. and then, it will delay the whole procedure.

Selection Criteria for Blockchain Applications (Part 4) Decision Making

1. What I'm talking about today
2. is kind of like a guideline for you to consider
3. whether an application should go for blockchain or not.
4. Now, before I end my section.
5. Now let me go through this flowchart.
6. After doing this flowchart you should be able
7. to give some indication
8. whether you need to consider blockchain
9. as the platform for your application or not.
10. The first question is whether you need a database
11. in the application?
12. Now if you don't need a database,
13. basically, we do not need a blockchain.
14. Now, if your answer is yes,
15. then your next question is,
16. do you have a trusted authority in the application?
17. For example, will the government handle the data
18. that you trust the government?
19. Now if yes, then you still need to ask another question,
20. whether the transaction fee is too high.
21. Now, if the transaction fee is not high,
22. it's acceptable to you and
23. you do have a trusted authority
24. to maintain the database
25. and to handle the transaction for you,
26. then again, don't go for blockchain.
27. Now, then, on the other hand,

28. if you do not have a trusted party,
29. trusted authority, or even if you have a trusted authority
30. like the bank but the transaction fee is too high,
31. then you may still consider using blockchain
32. for your application.
33. Then the next question you should ask yourself
34. is whether the application
35. involves more than two entities.
36. If the answer is no
37. because there are only two entities
38. then in the application
39. you can actually compromise everything easily.
40. Then, in that case, we do not use blockchain.
41. But if your answer is yes,
42. in other words, we need a database,
43. we do not have a trusted authority or
44. the transaction fee is too high,
45. and the application actually involves more
46. than two entities.
47. Then you need to ask another question,
48. will all the entities join the blockchain platform?
49. You need to have an understanding
50. whether these parties are willing to work together
51. in the blockchain platform.
52. If your answer is no, I'm not sure maybe only a few
53. of the entities will join the blockchain platform.
54. Now in that case, maybe you still consider not
55. to use blockchain because otherwise,
56. as I mentioned before then these entities
57. will become the bottleneck of the whole procedure.
58. Only in the case when you are quite sure
59. that the majority or even all of the entities
60. will try to join the blockchain platform,
61. then you start to consider
62. whether the blockchain platform
63. is a good infrastructure
64. for the application.
65. Then the next question you should ask
66. is whether the application involves
67. high-frequency transactions.
68. At the time of the course actually most
69. of the platform might not be able to deal
70. with high-frequency transactions.
71. If your answer is yes,
72. my application involves high-frequencies transactions,
73. then in that case I also recommend you
74. not to use the blockchain platform.

75. But on the other hand, if the answer is no,
76. you have a database to maintain
77. but you do not have a trusted party,
78. trusted central authority or the transaction fee
79. is too high and the transaction involves more
80. than two entities and you know that most
81. of the entities or all the entities
82. will join the blockchain platform
83. and the application will not involve
84. very high-frequency transactions,
85. then, in that case, we can actually consider
86. using blockchain as your platform.
87. But then you still need to
88. evaluate one more characteristic
89. because after all, we will need to see
90. whether the blockchain can
91. actually helps you to save money,
92. save time, etc.
93. In other words, I will need to look at the characteristics
94. of the application to see if they actually emphasize
95. the chain of custody,
96. or will the blockchain platform help you
97. to save the processing time
98. or will the blockchain platform help you
99. to locate the product or service you like
100. in a many-to-many relationship?
101. Now that in that case,
102. I think we should go for the blockchain.
103. I hope the flow chart is clear enough
104. for you to have a brief idea
105. when you have tried to consider an application,
106. whether it's good for blockchain or not.
107. My final remark is that, even if you think
108. that your application should go for blockchain,
109. I hope you still remember in the earlier section
110. we talked about how we can also classify blockchain
111. into public blockchain, private blockchain
112. or even you can in the middle
113. have a hybrid blockchain.
114. If that's the case,
115. then we still need to choose what type of blockchain
116. you're going to implement for your application.
117. Now, which type of blockchain you need to pick,
118. actually, depends on two factors.
119. Now, because public blockchain relies on all the entities
120. in the blockchain to make the final decision
121. of the blockchain,

so the trust model will rely on all the entities
and these entities are allowed to freely
to join the blockchain
without any verifications, validations or authentications.
In other words, if you use a public blockchain
you need to trust the entity who will make
the fair decisions.
Now on the other hand, if you do not trust all the users
in the blockchain, you may go for a private blockchain.
In other words, the user will be authenticated
before you allow them to use your blockchain,
or you can pick a middle model.
For example, the miners are all the authenticated users
but the other users can freely join the blockchain,
so this will be the hybrid model we talked about.
So which blockchain you need to pick depends
on how much you trust the entities
and to what level you want your application
to release the decision-making to the entities.

4.2.0 Blockchain and Enterprise – A Technology of Coordination (Charles d'Haussy from ConsenSys)

1. So when it comes to enterprise blockchain,
2. it really comes back to this first definition
3. we shared earlier on, that blockchain offers
4. a technology stack to coordinate things.
5. And the way enterprises identify value
6. in the blockchain's value proposition is
7. that many companies are working
8. with many different stakeholders.
9. So think, for example, of the supply chain industry.
10. In the supply chain industry, your job is basically
11. to pick up goods, which are ready out of a factory,
12. put them on the trucks, the truck goes to the boats,
13. the boats go to the other side of the world
14. and it involves so many different players,
15. so many different actors.
16. And that's where the technology of coordination
17. that is blockchain really helps to build
18. an infrastructure where you can coordinate
19. the work for all these people
20. and you don't depend only on one player.
21. So this is one of the core value propositions
22. of blockchain enterprise.
23. Where we find a lot of traction right now is
24. in financial services again

because the financial services
industry is a very big industry involving
a lot of different players and a lot
of different actors, which work together
and blockchain is a way for them to work
together much more efficiently.
So if you think, for example, of the way
you distribute today a financial product,
there is usually an issuer of an insurance,
for example, and then there is insurance workers
and then there is insurance agents.
And all this work and all this information
they share together by promoting, selling,
distributing insurance contracts involve
a lot of information to be
shared in a very trusted manner
because if you lose information on the way,
you put some people life at stake basically.
So in a way, you want to disintermediate.
But the way to disintermediate if you don't have
the right technologies, not every company is ready
to take over the job of intermediaries, right,
unless you've got the right technologies.
And this is where people are building
a lot of blockchain enterprise solutions
to get more direct access with their customers
in a very organised way, and very transparent way,
and automated way using smart contracts
and using blockchain infrastructure.
Another way enterprises, I will say have as a benefit
of blockchain is by building consortiums.
So if you think of different banks
or if you think about different actors
of any stock market, there is many different actors,
in a way they are happy to transact together
but they are also competing, maybe, in some ways.
Or they don't always give so much trust
to each other for some reason.
So in this case, you want to build a consortium.
A consortium is basically a
group of companies bringing
together, they are working on the same market
on different part of this market for different industries
and they create a consortium to decide,
we want to build together, what infrastructure,
which would be trustless, which would help us
to coordinate things.

72. And this infrastructure, we don't want it to be
73. kind of managed, or led, by a single party.
74. We want to have this platform,
75. built and co-managed by everyone, so we all trust
76. and we know it's not a platform belonging
77. to one player only.
78. So we don't have to trust one player only,
79. anyone can take, I would say the leadership
80. or decision on this platform.
81. And the way to design today consortiums
82. around one technology using
83. blockchains really makes sense
84. because all these players build a consortium,
85. builds the rules of how they want to interact together,
86. and basically apply these rules on blockchain
87. and then they all co-own the infrastructure.
88. They all cooperate in this infrastructure.
89. And the technology of blockchain has been designed
90. exactly for that, so it's a very excellent way
91. for enterprise to work together using
92. the technology which has been designed for them

4.3.1: Why Permissioned Blockchains are used in Enterprise Network? (Dr. Paul Sin, Consulting Partner from Deloitte, China)

1. Hello everyone, I am Paul Sin.
2. I am the FinTech partner for Deloitte
3. as well as the leader
4. of the Asia Pacific Blockchain Lab in Deloitte.
5. In Deloitte, we have three blockchain centers,
6. one in Hong Kong looking after Asia Pacific,
7. one in Dublin look after EMEA,
8. and one in New York looking after America
9. and we work very closely together.
10. So today, what I'm going to do is
11. to share some of the use cases,
12. especially global use cases,
13. which we have deployed not just as a proof of concept,
14. but also in production environment,
15. and they are already serving
16. real business problems and scenarios.
17. So maybe I will start with defining
18. what is enterprise grade blockchain?
19. A lot of people associate blockchain with Bitcoins,
20. and/or Ether or other crypto assets.
21. But in a lot of enterprise applications,
22. we do not use that kind of blockchain.

23. Those blockchains are called public blockchains.
24. And in public blockchains, all the users are anonymous.
25. And we're trying to create an immutable ledger
26. for anonymous user to transact with each other.
27. While we are–
28. While this is a very idealistic platform,
29. it has some limitations that enterprise find it difficult
30. to put in real application.
31. One of them is the
32. the slow performance.
33. For example, in Bitcoin, it takes maybe 10 minutes
34. to complete a transaction.
35. Ethereum, maybe a few seconds to 12 seconds.
36. This kind of network is far from sufficient
37. to support all these enterprise application.
38. There is also another reason
39. why we do not use public blockchain,
40. because it consumes a lot of computing power.
41. So, if I need to install supercomputers
42. to have the network up and running,
43. it will be too costly for enterprise.
44. What we use in enterprise environment
45. is usually permissioned blockchains.
46. In permissioned blockchains,
47. we do not have anonymous users.
48. All the people that are using the blockchain
49. have gone through an onboarding process.
50. And they are issued with digital signatures,
51. so we know who these people are
52. and when they are committing a transaction,
53. we can trace it back
54. to the original initiator of the transaction.
55. So, there will be no risk of like money laundering
56. in this kind of network.
57. And the performance is very fast
58. because I do not need anonymous users to do mining
59. to prove that they are legitimate users.
60. They already have a digital signature.
61. So we know these guys are legitimate users already.
62. Because of that, the transaction speed is very fast.
63. Usually we can have few thousands
64. like five to six thousands transactions per second.
65. Some networks that are running today
66. in production can go up to
67. 20,000 transaction per second.
68. And this is the speed we need
69. for enterprise applications.

70. Now, when we come back to the use cases,
71. why do we need blockchain?
72. Blockchain is a data layer in technology.
73. And we have technology for
74. sharing data since the beginning
75. of the computer science technology.
76. So in the past, if I need to share data, for example,
77. within an organisation across different departments,
78. I can create a centralised database
79. and everyone put their data in,
80. and we can share the data effectively.
81. And those systems now become
82. the ERP system for traders
83. and corporates or maybe core
84. banking system for banks.
85. But when we are exchanging data,
86. real-time between corporations or between businesses,
87. then this kind of technology will not be applicable.
88. If I'm a bank, for example,
89. and I want to exchange the customer information
90. with the insurance company,
91. I'm not going to open the insurance company system
92. and enter the customer information in their system.
93. Vice versa, the insurance company will not use
94. the bank system to enter the
95. data in my core banking system.
96. And because of that,
97. we need another way to exchange data effectively
98. between two enterprises,
99. who both own large enterprise systems already
100. in their own environment.
101. We develop something called API,
102. application programme interface,
103. which connect these two systems together,
104. and these two systems can then
105. exchange data automatically
106. real-time without human intervention.
107. API works very well,
108. except that when we are transferring
109. sensitive customer information
110. across organization boundaries.
111. Then we are going to violate a lot of data privacy laws.
112. Like, in Hong Kong, we have PDPO.
113. In China, we have Cyber Security Law,
114. and a lot of these kinds of law.
115. And globally, we have GDPR,
116. and this law will forbid us from

117. exchanging sensitive customer information.
118. This is one of the reasons why we use blockchain,
119. or to be more precise, distributed ledger technology.
120. There is also another reason why we need blockchain.
121. If in an ecosystem, there's only one data producer.
122. Let's say, if I'm a credit rating agency,
123. I provide credit rating of different enterprises
124. to the financial institute.
125. And in that scenario, there's only one data producer.
126. All the people in the ecosystem are data consumers.
127. And in that case, we can use OpenAPI,
128. and we call that utility model.
129. So as a credit agency,
130. I let people subscribe my API
131. to obtain credit ratings,
132. and that is an effective model.
133. The other way around,
134. if there are many data producers
135. and only one data consumer, like a regulator,
136. a regulator will collect all these regulator reports
137. from all the financial institutes in the ecosystem.
138. And in that case, I can also use OpenAPI,
139. I can ask all the financial institutes
140. to submit their regulatory reporting through OpenAPI.
141. And that also works very effectively.
142. The only situation where API does not work well is
143. when everyone can be a data producer and consumer.
144. So let's say if this is a KYC network,
145. Know Your Customer network,
146. and I am a bank,
147. if a customer come to my bank to open an account,
148. they may probably spend like
149. one or two hours to go through
150. all these customer due diligence process.
151. And after they have done all that
152. and I open an account for him or her,
153. when this customer go to another bank,
154. they need to spend another one and two hours
155. to do the same thing.
156. So it doesn't make a lot of sense for the ecosystem
157. because every bank will follow the same procedure
158. to do this customer due diligence.
159. Why do we need to repeat that again and again?
160. So, a better way to do that is,
161. if the first bank have already done the KYC process,
162. I will put that results on a network
163. where the result will be

164. synchronised to all the other banks
165. in the ecosystem.
166. And when the customer go to another bank,
167. then immediately within a few minutes,
168. they can open account for this customer.
169. And that sounds very perfect,
170. except that there are data privacy issues
171. on sharing KYC information.
172. So, due to the hashing algorithm and encryption engine
173. in distributor ledger or blockchain,
174. we can now synchronise this
175. sensitive customer information
176. without violating the privacy ordinance.
177. That's for the first thing.
178. Second is that, in this ecosystem,
179. every bank is a data producer and data consumer.
180. And if I use API to do this,
181. I need to create point to point integration among all
182. the combination of these banks.
183. That means, if I have like seven banks,
184. I may have 42 integration points.
185. And that is very hard to build and maintain.
186. If one bank changes their API interface,
187. six other banks will need to re-build their interface again
188. and test the whole thing again.
189. So this is not a very effective way to distribute data
190. and synchronise data.
191. Blockchain provide a mechanism
192. which all this KYC information will then be broadcast
193. to everyone and without exposing the identity
194. of the customer.
195. Only when the customer goes to
196. another bank, give consent,
197. and then provide their identity,
198. the second bank can then retrieve the KYC information
199. from this KYC network.
200. And this is exactly how we apply
201. distributor ledger or blockchain.
202. So, this just illustrates why we use blockchain
203. instead of traditional data base
204. and the OpenAPI technology.
205. If you are trying to solve a problem,
206. what we define as real-time,
207. secured B2B synchronisation
208. of data, especially sensitive data.
209. In an ecosystem with multiple
210. data producers and consumers

211. then distributor ledger will be
212. the best technology available at the moment
213. for you to solve that business problem.

4.3.2 Use Case: Blockchains for Trade Finance (Dr. Paul Sin, Consulting Partner from Deloitte, China)

1. Let me give you a simple example.
2. If I am a bicycle manufacturer in China
3. and I am exporting bicycles overseas.
4. One day I suddenly receive a purchase order
5. from the States as an ordering of a thousand bicycle.
6. If I can get the bank to finance me
7. in working capital and produce those bicycles,
8. I can produce those bicycles, ship it over,
9. collect the payment, pay the bank back
10. with the principal and the interest.
11. And the bank makes money, I make money,
12. the customer is happy so this is a perfect scenario.
13. The challenge is, at the moment,
14. a bicycle manufacturer like me,
15. goes to a bank to apply for financing.
16. Four out of five cases will be rejected.
17. And there are three reasons why
18. the bank does not finance me.
19. The first is that they know me
20. but they do not know the buyer in the States.
21. So if they finance me, they don't know whether
22. even if I deliver the bicycles, they don't know
23. whether the buyer's going to pay the invoice or not.
24. Secondly, they are afraid that the P.O. has been tampered.
25. So if the U.S. buyer is maybe like ordering 100 bicycles
26. but then I add a zero and become 1000 and get
27. a much larger amount of financing,
28. the bank cannot tell.
29. The third issue is duplicate financing
30. and which is very common.
31. Banks can lose like 200 million U.S. in one transaction
32. because of duplicate financing.
33. The idea is like this, if I am the bicycle producer
34. I can take that purchase order,
35. go to 10 different banks and apply for financing.
36. And the bank will not know that they
37. are the competitor or the other bank
38. has already financed this SME.
39. So everyone of them will finance me based on that P.O.
40. That piece of paper and there's no way

41. we can detect duplication.
42. If you want to solve that with traditional technology,
43. what you can do is you put,
44. ask all the bank to put all the purchase order
45. they received as a collateral
46. in a centralised database and
47. de-duplicate all of this P.O.
48. But this will expose all the bank's customer information
49. as well as their sensitive business
50. turnover information, etc.
51. So no bank is willing to do that and therefore
52. in the past centuries, said trade finances
53. has a lot of fraud which we cannot resolve.
54. Now, with the blockchain technology, we can scramble
55. all the data of the purchase order and all these trade
56. documents, bill of lending, invoice, etc.
57. And put in their – in every bank's own data centre
58. what we call a data node.
59. And this data node will then synchronise
60. all the data with all the other bank's data nodes.
61. And these data cannot be reverse-engineered
62. in the original data form.
63. But when the same P.O. is presented
64. to two different banks,
65. the way blockchain scrambles the data,
66. we call that hash algorithm.
67. The way we hash the same P.O. are the same.
68. So the resulting hash will always be the same.
69. And when we compare these two hashes,
70. we know there is a duplicate financing.
71. Similarly, when I provide the buyer's identity
72. and the Hong Kong or the Chinese banks
73. do not know whether this buyer exists or not,
74. they can check the KYC hash
75. created by the American bank.
76. And if the hash is the same as the hash I created
77. based on the buyer ID the seller provided,
78. then I know this buyer is a legitimate buyer
79. based in the US and with the bank I can
80. go on for all the KYC of the US bank
81. and they have good credibility.
82. So this is very important and that allows
83. the whole ecosystem payers to
84. share this sensitive information
85. without worrying about breaching data privacy.
86. And with that, people like the buyers, sellers,
87. the shipping companies, the banks,

88. the insurance companies,
89. they all feel comfortable
90. using the data on blockchain as a trusted source
91. of trade information that allows them to do,
92. reduce the risk of the whole ecosystem.
93. There's no duplicate financing risk for the bank.
94. There's no forged document
95. risk in the financing process.
96. There's no forged document for the insurance.

4.3.3 Use Case: Blockchains for Supply Chain Financing (Dr. Paul Sin, Consulting Partner from Deloitte, China)

1. If you think about financial services,
2. what they do in essence is to price risk.
3. If the risk of an ecosystem is lower,
4. then the financial charge and the financial cost
5. of doing business will be lower also.
6. I was told that when insurers
7. insure a container of goods,
8. being in transit,
9. they actually do not know what is contained
10. in the container.
11. You can ship a container of
12. glass or a container of diamonds.
13. They will charge the same premium,
14. because they don't have the information.
15. With Blockchain you have transparency
16. of all this information.
17. And insurance can charge you
18. a much more reasonable premium.
19. And that also means a lower cost for SMEs.
20. With all this transparency,
21. SME will have a much higher financing rate.
22. With that they will have a higher
23. production capacity.
24. SMEs represent almost 70 to 80 percent
25. of the GDP of developing countries.
26. That's why governments are very keen
27. to adopt, issue with ledger,
28. to help SME to obtain financial services.
29. So that a whole economy can thrive better.
30. So this… Some of the top use cases of
31. Blockchain in the world now
32. are trade finance and supply chain financing.
33. The second biggest use case is
34. supply chain traceability.

35. So traceability has two angles.
36. One angle is fighting counterfeit products.
37. The other one is to prove that your products
38. are sustainable.
39. Or from sustainable sources.
40. At the moment, there are a lot of
41. counterfeit products everywhere in the world.
42. Official statistics are like seven percent
43. of the global trade are counterfeit products.
44. But in some developing countries
45. this figure is much higher.
46. There is a lot of effort in trying to trace
47. the product back to the origin.
48. One of the famous cases will be diamond.
49. We do not want diamonds from the conflict zones,
50. what we call black diamond,
51. to be circulated in the economy.
52. Because of that,
53. we want to know where those diamonds come from.
54. If I can have the miner, the polisher, the wholesaler,
55. the retail, everyone to put the record on the Blockchain,
56. then we can trace the diamond
57. from the hands of the customer
58. all the way back to the mine.
59. We can feel pretty assured that this diamond
60. is not a blood diamond.
61. And also with that,
62. you can also prove diamonds are not stolen
63. or from gangsters or criminals.
64. You can then obtain financing, insurance,
65. and other kinds of financial services
66. around your product.
67. So this becomes a very important use case.
68. We have seen people tracing
69. not just diamonds but wine.
70. A lot of wines are fake wines at the moment.
71. People trace Wagyu beef,
72. because those are luxurious products.
73. People trace palm oil.
74. Because we want to know whether the palm oil
75. is coming from deforestated area.
76. Otherwise we cannot import any into Europe.
77. We also want to see
78. if some of the vaccines are from
79. real pharmaceutical companies
80. or they are fake vaccines.
81. You probably have heard that there are

82. food-safety centers established
83. by large supermarkets
84. to make sure all the food are safe
85. when they are being put on the shelf.
86. This is probably the second biggest use case
87. in Blockchain applications.

Use Case: Cross Border Connectivity – Trusted Data Transfer (Dr. Paul Sin, Consulting Partner from Deloitte, China)

1. There are many other kinds of blockchain applications.
2. I will mention the last one
3. which explains the value of blockchain.
4. So at the moment, there are a lot of discussions
5. about Greater Bay Area in south China.
6. And compared to all the other bay areas
7. like San Francisco or Tokyo,
8. our Chinese greater bay area is quite special.
9. Because we are talking about one country, two systems,
10. three jurisdictions and three different currencies,
11. and also controls on people flow and capital flow, etc.
12. So one thing we need to solve is if we want to facilitate
13. products, people and capital flowing cross-border,
14. we need to allow information to flow first.
15. Let's say if a citizen wants to move from Hong Kong
16. and to China and work there.
17. Then you need to move all the employment records,
18. pension records, your identity information,
19. tax equalisation information.
20. There is a lot of information we need to synchronize.
21. Before we can let that person settle down
22. smoothly in a new place.
23. So in order to do that we need a way to send
24. sensitive customer information,
25. sensitive individual information cross-border.
26. And this is something a lot of people are working on.
27. In the financial services world we see that people
28. like credit bureaus trying to synchronise credit reports.
29. So that if I'm an SME in Hong Kong,
30. I have a good credit report,
31. I can go to China to do business and I can borrow
32. from the bank in China who is inquiring
33. the credit bureau in China to see my credit report,
34. which is already synchronized
35. from Hong Kong to China.
36. We also see that in the past
37. when insurance companies in China try to sell

38. their product through the bank in Hong Kong or Macau.
39. And the policy information
40. cannot be synchronised cross-border.
41. And because of that there are a lot of inefficiencies.
42. So for example, if I am a insurance customer.
43. I bought the insurance policy from a bank in Macau,
44. but the insurance provider is in China.
45. And I go to the branch to pay the premium.
46. The bank actually does not know
47. how much premium is outstanding.
48. So they will accept whatever I pay them.
49. They ship the premium back to China.
50. They do the reconciliation and then they find discrepancies.
51. They inform the bank, the bank calls the customer
52. chase for the discrepancy.
53. And then they will settle all these payments
54. like 20 days later.
55. So this is a very inefficient process.
56. With the ability to synchronise the data cross-border,
57. we can shorten all these turnaround times and reduce
58. manual efforts and also the errors in the process.
59. All the processes in this kind of collaboration,
60. we call that bank assurance partnership,
61. can be streamlined through a distributed ledger.
62. And we find that almost 86% of manual efforts
63. can be reduced in this kind of partnership.
64. So if you have a B2B partnership
65. and you have a lot of these sensitive
66. customer information being synchronised.
67. Blockchain will be a very effective tool to do that.
68. Looking forward with all these successful cases
69. already in production,
70. I would say that we are already way past
71. the proof-of-concept stage,
72. which is what people have been doing back in 2016.
73. So 2016, 2017 are the years of proof-of-concept.
74. A lot of press releases on different kind of POC.
75. But in 2018 we start to see a lot of platforms
76. going to production.
77. You probably heard of the
78. Hong Kong Monetary Authority
79. with 12 banks, they have eTradeConnect in production
80. announced in Fintech Week.
81. We have we.trade in Europe now based
82. in Dublin launched in production.
83. We have Voltron, Marco Polo…
84. There're a lot of trade finance platforms

85. now being launched in production.

How to Deploy an Application on the Ethereum Blockchain? (Charles D'Haussy from ConSenSys)

1. So if I want to deploy a smart contract
2. or an application on the Ethereum blockchain,
3. what do I need?
4. Do I need an account on
5. let's say, Google platform or something like that?
6. How do I actually build something
7. on the Ethereum blockchain?
8. The Ethereum blockchain is an open-source blockchain.
9. So a lot of the tools to interact with the blockchain
10. and build on the Ethereum blockchains
11. are available free of charge.
12. So you will start by creating yourself an account
13. on Ethereum which is something
14. which is totally free of charge,
15. and then you will get yourself familiar
16. with how we code smart contracts, for example,
17. and you're going to be able to basically launch
18. and host your contract on the Ethereum platform.
19. Then when you want to run this program
20. there will be a few costs involved such as gas,
21. what we call gas, is a little bit like the same way
22. you put gasoline in your car,
23. there is gas also to basically run your program
24. on the blockchain.
25. So the same way
26. if you host your website on a server for your blog,
27. for example, you will need to pay every month
28. a monthly fee to basically rent this space on a server.
29. You will also rent some space on the blockchain,
30. on the Ethereum blockchain to run your program.
31. So once it's up on the Ethereum blockchain,
32. once a program is up on the Ethereum blockchain,
33. could ConsenSys or could Ethereum just decide
34. to take something down?
35. The beauty of the blockchain
36. and the beauty of Ethereum
37. are that things happening on the blockchain
38. are totally transparent and they are immutable.
39. So every single transaction, every single activity
40. is recorded by the whole network itself.
41. So today you find about 10,000+ different nodes
42. within the Ethereum blockchains

43. which really guarantees you
44. that it's recording in a very distributed way
45. and also an immutable way.
46. So it's a platform which belongs to everyone
47. and everyone can build on it and no one has the right
48. or the capacity to remove something.
49. So a lot of people know about CryptoKitties,
50. a very famous Ethereum decentralized application.
51. Besides CryptoKitties,
52. are there any Ethereum applications
53. that have reached mainstream adoption?
54. So it's still early for the Ethereum ecosystem.
55. But we see some very strong signals that the growth
56. of the ecosystem is really coming very strong.
57. So you have for example, in Switzerland, parts
58. and certain cities in Switzerland such as the city
59. of Zug, which is I think an online identity,
60. blockchain identity system
61. and blockchain-based voting system for their citizens.
62. You see a lot of use cases which are live
63. in production right now,
64. which involves the supply chains.
65. So when you want to basically record the journey
66. of goods and journey of raw materials
67. to really understand where they are coming from
68. and how they bring together a product.
69. If you really want to understand the provenance
70. and the product journey.
71. There are many use cases
72. which relate to payment, for example.
73. So instead of using the traditional legacy system
74. to send money cross border,
75. you're going to use the blockchain
76. to basically move money
77. between one country to another.
78. And this can be done with Crypto money
79. or this can be done also with a Crypto Vacuum
80. for traditional Fiat money.
81. So there are many use cases happening right now.
82. This is the beauty of this technology
83. and why so many people are excited
84. about the Ethereum blockchain is,
85. it's an ecosystem of talents.
86. It's an ecosystem of more than 300,000 developers,
87. all building their own products,
88. their own infrastructure on the core layer
89. that is the Ethereum blockchain.

90. So it's really, I would say, a very large playground
91. for technologists, for creators,
92. for entrepreneurs to build
93. use cases related to identity,
94. related to a change of money cross border,
95. for example, on the supply chain side,
96. whenever you want to document
97. or get your online identity and
98. give ownership to the users,
99. this is a playground which is really fantastic.

4.4.2 Use Case: Bounties Award Ethereum for Cleaning Beaches (Charles D'Haussy from ConSenSys)

1. One use case of blockchain which really illustrates
2. this coordination capability
3. of the blockchain technology,
4. there is one initiative
5. which is called Ethereum Bounties.
6. So you can basically coordinate an action from a group
7. of people in a decentralized manner
8. and decide to give rewards to
9. people for doing something.
10. So for example, one very concrete and
11. very original example here in Asia, a few weeks ago
12. in the Philippines, some people volunteer
13. to clean up a beach.
14. And they said we are really
15. happy to clean up this beach,
16. but we would love to have some rewards to organize
17. as a logistics for us for these
18. 50 people to go to the beach
19. and to basically bring back, also, all the waste
20. they collect from the beach back to a proper place.
21. So they wanted also to find
22. some reward enough for a day job
23. for some people who are ready to do these activities.
24. So all of these has been coordinated using
25. the Ethereum Bounty systems, which is decentralized,
26. where people were saying, I love this project
27. and I'm happy to contribute maybe $1, maybe $5, $10,
28. and people basically crowdfunded
29. using the Ethereum blockchain rewards,
30. an event of cleaning a beach.
31. But you can think the same
32. thing for giving some lessons
33. or doing all kind of activities in our everyday life

34. using decentralized technology.
35. So the people were able to get rewarded,
36. have a guarantee of reward to be paid to them,
37. and being brought together just by a technology
38. which is very optimized for this kind of coordination.

4.4.3 ConsensSys and the Ethereum Platform (Charles D'Haussy from ConSenSys)

1. So ConsenSys is a group of
2. technologies and entrepreneurs.
3. We were founded by Joseph Lubin in 2015.
4. Today we represent about 1,000 people,
5. which are all working on mostly
6. on the Ethereum blockchain.
7. And we developed technologies
8. which are low layer technologies.
9. So we do a lot of research and tools for people
10. to interact with the Ethereum blockchain,
11. but we also built different companies
12. and kind of organisations
13. which are focusing on different use cases on the blockchain.
14. So some people within ConsenSys are working
15. and doing research for Ethereum.
16. Some of the group of people are working
17. on the use cases around finance.
18. We have a group of people working on social impact
19. of the blockchain, developing applications
20. with different stakeholders
21. to really create an impact,
22. using the technology of blockchain.
23. We are also an accelerator for
24. all blockchain entrepreneurs
25. to help them really get the idea together
26. and kick off the projects.
27. And we also do all kinds of activities related
28. to the community engagement to make sure
29. that the people will capture the potentials
30. of the Ethereum technology
31. and one more vertical we have within ConsenSys
32. is what we call ConsenSys academy,
33. where we help the executive, we help developers
34. to really understand the potentials
35. of the Ethereum blockchain and
36. give them very practical
37. and concrete trainings to get their hands on,
38. starting to code, starting to build businesses,
39. but starting to build projects

40. on the Ethereum blockchain.

4.4.4 ConsesSys Use Case: Project i2i(Charles D'Haussy from ConSenSys)

1. ConsenSys has here in Asia one project
2. which is really I will say a milestone for us
3. and a marquee project.
4. It's called a Project i2i.
5. So i2i means individual to individual
6. and infrastructure to infrastructure.
7. So what i2i is about,
8. it's about connecting the rural banks in the Philippines,
9. to the core banking system of
10. the Philippines in the cities.
11. So the Philippines is a country
12. which is made of many different islands
13. and you can imagine that
14. building infrastructure over there
15. is very costly and extremely complex.
16. So what's happening is there is some remote villages,
17. which do not have access to the same banking services
18. you will get in the traditional larger urban cities,
19. in the Philippines.
20. And what we've been building over there together
21. with Union Bank, one of the
22. main banks in the Philippines,
23. is really extending the network of services
24. and the infrastructure extending from the core cities
25. to the rural banks using blockchain technologies.
26. Why we choose blockchain technologies in this case
27. is because it was the easiest way
28. to connect all these different rural banks.
29. There're hundreds of them
30. spread all over the Philippines
31. and connect them back to the existing system.
32. And if the existing system was to be built to reach them,
33. it will be extremely costly
34. and basically possibly never happen.
35. So the way was really to kind of bridge the gap
36. in a trustless manner, in a cost-efficient manner,
37. to help all these rural banks to provide cash services,
38. to provide loans, to provide all the services of a bank,
39. but connecting them back to the main bank
40. using the blockchain technologies.

4.5.1: Use Case: Trade Finance and Supply Chain (Anil Kudalkar, MD, MaGESpire Partners)

1. I'm Anil Kudalkar, managing director
2. and co-founder of MaGESpire Partners.
3. Today I'm going to speak about some of blockchain's
4. most used cases and the best fits.
5. The first one I want to speak about
6. is trade finance and supply chain.
7. Automated smart contracts and blockchains
8. can transform how business
9. processes of supply chain and trade finance works.
10. Since supply chains are
11. complex and distributed involving many parties
12. across the globe, there's a lack
13. of trust between one another,
14. leading towards the need for trusted third parties
15. like banks or intermediaries.
16. With blockchain, smart contracts can be
17. executed automatically to transfer any
18. goods and money without the need for
19. middlemen such as a bank and their exorbitant fees.
20. This will not only help in building a trusted network
21. but also ensures authenticity and origin of
22. product being supplied.
23. Trade finance it has heavily been a paper-based
24. industry as of 2017 it was like about
25. 9 trillion transactions worth when done.
26. Typically the steps involved are
27. creating a purchase order then the
28. exporter creates an invoice to the importer,
29. the importer requests the LC, the bank then
30. approves and publishes the LC,
31. and exporter creates a packaging list.
32. Then, the carrier creates and publishes the bill of lading
33. and then it's the exporter
34. submitting the invoice.
35. So there's a lot of procedures involved, and lastly the
36. issuing banks endorses the released documents.
37. One good example which is from
38. Hong Kong is about HSBC late in 2018
39. successfully completed the first batch
40. of a live pilot trade finance
41. transaction on eTradeConnect.
42. This is a newly launched blockchain platform
43. co-founded by seven banks and
44. facilitated by HKMA which is the
45. regulating body. The platform enhances
46. efficiency and transparency by digitizing
47. trade documents and automated

48. trade finance processing,
49. leveraging the unique features of blockchain.
50. The key benefits we saw in the pilot were
51. digitized trade loan applications,
52. application to approval times in the life of transactions
53. reduced from one and a half days to just four hours
54. and increased efficiency and transparency of
55. trade finance transactions.
56. Among the first batch, there was also a purchase of
57. supplies by a furniture and household
58. retailer from its supplier.
59. The transaction involved a purchase order
60. and invoice as well as a proof of delivery
61. which has created exchange and
62. confirmed on the eTradeConnect platform.
63. The counterparty was able to
64. submit a trade finance request directly to the bank
65. based on the documents uploaded on the platform.
66. eTradeConnect is yet another
67. milestone in the evolution of commercializing
68. blockchain globally.
69. What are the most important benefits
70. of the technology of blockchain in trade finance?
71. One, is the traceability – tracking goods
72. and trade assets where they are
73. currently residing, then, related asset information
74. can be relayed, again, real-time.
75. Transparency – increased commercial transparency
76. can reduce delays in financing trade and
77. details of the transactions against commercial and
78. agreements improve further trust.
79. The other important point is auditability.
80. Each trade finance transaction is
81. recorded sequentially and indefinitely.
82. So this provides an audit trail for the life of the
83. trade asset between parties.
84. And the next big aspect is security.
85. Each trade transaction is verified within the network
86. using independently verified complex cryptography.
87. Authenticity of the trade-related information
88. can be assured.
89. Then, obviously there is collaboration
90. which allows each party to share easily
91. and securely trade finance-related data.
92. Fragmented internal systems are
93. centralized, allowing interoperability.
94. Again, now coming to efficiency.

95. Transactions are completed within
96. a shorter amount of time.
97. This ability to operate smart contracts
98. which automatically trigger commercial transaction.
99. The supply chain management is the next example
100. I would highlight.
101. I would like to take one
102. example from the pharma industry.
103. Product tracking refers to tracing of
104. unit levels the drugs and medicine
105. across end-to-end supply chain using blockchain.
106. All stakeholders in the ecosystem can
107. access the provenance,
108. authenticate items and prove compliance.
109. This is enabled by
110. the real-time capability and distributed features
111. associated with the platform.
112. For example, tracking drugs on the blockchain
113. throughout the life cycle from manufacturing
114. to patients could facilitate counterfeit-free
115. drug identification or assist drug recall management.

4.5.2 Use Case: Capital Markets (Anil Kudalkar, MD, Magespire Partners)

1. Next example I would like to highlight is from
2. capital markets and settlements.
3. For example, the Swiss exchange SIX expects its
4. traditional trading platform to be overtaken
5. within a decade by an alternative
6. platform using only blockchain technology.
7. SIX digital exchange, which is the SDX,
8. is due to launch in mid-2019, and initially there will be
9. a parallel run to the existing
10. platform of a purchase and sale of securities
11. on a blockchain on a distributed ledger.
12. The transactions can be
13. completed in a fraction of a second.
14. Another example is the Australian exchange.
15. ASX has become the first major board to announce
16. an adoption of blockchain technology to record
17. shareholding and manage the clearing and
18. settlements of equity transactions.
19. Blockchain or DLT uses shared ledger to
20. permanently record transactions in a way that is
21. practically impossible to tamper with.
22. The ASX said it will soon be scrapping its old
23. clearinghouse system, which is Chess.

24. In the 90s, that was the state of the art, right?
25. But the new testing of the new DLT technology
26. over the last two years has gone better.
27. Now, coming on to the Hong Kong exchange.
28. The Hong Kong exchange is entering an open-ended
29. period of consulting where it wants to use
30. DLT for the stock connect program.
31. Once this is sort of done it will try to implement it
32. into other areas within the exchange.
33. So this will be real-time and transparent synchronization
34. of communications to move away
35. from sequence-driven,
36. one step at a time processing.
37. The stock connect is one area
38. which they are doing a pilot and then they will be
39. applying it to other areas of the exchange.
40. Away from securities, some of the other compelling
41. applications of DLT in the capital
42. markets include payments.
43. For payments, the DLT can streamline end-to-end value
44. transfers, reducing cost,
45. and operational risk settlement process.
46. For example, Ripple's XRP ledger provides real-time
47. cross-border settlements using
48. tokens that represent central bank currencies.
49. In foreign exchange, HSBC's FX Everywhere protocol
50. processed more than three million
51. intercompany FX transactions worth
52. 250 billion in the first year.
53. Syndicating, lending trade finance and other forms
54. of bank finance still rely on paper documents
55. and manual processes.
56. DLT could transform this by providing a shared record of
57. shipments, ownership, financing, and insurance.
58. The we.trade platform built by 20 European banks
59. including HSBC and hosted on the IBM's blockchain
60. conducted its first open account trades in July 2018.
61. Then it will be fund administration as an application.
62. A DLT ledger recording the creation, redemption and
63. transfer of funds units would eliminate many of the
64. current complexities of fund administration.
65. It could unify cross-border sales processing
66. and transfer agency.
67. There are two large platforms,
68. Fundsquare and Calastone,
69. are both developing a new DLT
70. infrastructure based on blockchain.

71. The other important application is
72. customer identification.
73. An industry-wide distributed ledger could host
74. a shared record of beneficial owners
75. such as a utility that would give appropriate
76. permissioned access to market participants
77. allowing them immediate KYC and AML checks,
78. assisting with client onboarding
79. and enhancing tax reporting.
80. DLT can deliver many potential transformative
81. applications in the capital markets,
82. especially the post trade arena
83. offers the most compelling opportunities.
84. DLT could also reshape the practice
85. in other areas of the markets, especially
86. as interoperability between ledger starts to take shape.

4.5.3 Use Cases on General Government Services & Sustainable Livelihood (Anil Kudalkar, MD, Magespire Partners)

1. We've seen that blockchain technology has been hailed
2. as a revolutionary means to secure
3. and transparent record keeping and data sharing
4. with seemingly endless potential uses
5. in the wide variety of sectors.
6. Today government agencies
7. around the world are looking
8. for blockchain to help their services be more efficient.
9. First, I would like to highlight the identity
10. as one of the biggest applications.
11. Perhaps the most essential and enabling use case
12. for a blockchain in government services
13. is the realm of digital identity.
14. Governments are not only the source
15. of key identity information for citizens,
16. but from official registration from our births to demise,
17. issues of death certificates, they need to also enable
18. this in a digital format.
19. As this has proven difficult to achieve
20. in the traditional centralised technologies,
21. some governments are looking
22. to use blockchain to realise this idea.
23. The second is title and asset registrations.
24. The same process can, of course,
25. be used to secure information
26. about almost any kind of registration,
27. for example, businesses, automobiles.

28. Some of these used cases could have
29. significant social impact,
30. such as registration of firearms
31. and ammunition to track their usage or abuse.
32. Blockchain has been long proposed
33. for use in land registries, for instance,
34. this was initially the case
35. in all developing countries looking
36. to fight corruption by local officials.
37. The third would be healthcare.
38. Another important use case
39. for blockchain is in publicly provided healthcare.
40. There are two main areas.
41. First, the blockchain can potentially improve the
42. securing and sharing of patient medical records.
43. Today medical records are typically kept separately
44. in doctors' offices, hospital databases.
45. They are still often shared manually and not always
46. in a very secure way.
47. This is a problem, considering the sensitive nature
48. of the data.
49. It can also get complicated in multi-provider system,
50. where various people and institutions
51. have to make input to a patients data.
52. Blockchains are very good for such scenarios
53. providing a clear audit trail of inputs
54. by multiple sources and ensuring the data
55. is not manipulated or corrupted once it is saved.
56. Estonia, which has established
57. a national electronic health record is contemplating
58. using a blockchain based registry
59. to ensure the correct handling of sensitive health data
60. by securing the entry of new data into the record
61. and providing an immutable audit trail
62. of how the data has been used.
63. In Sweden there is an initiative
64. to develop a national blockchain for healthcare records
65. to give citizens more control of their data.
66. Blockchain technology offers a possibility
67. to radically streamline such processes.
68. In Sweden recently they've carried out
69. a first successful test transaction
70. of a fully blockchain-based transfer of title.
71. In the UK HM Land Registry is testing blockchain
72. in its bid to become the world's leading land registry
73. for speed, simplicity, and an open approach to data.
74. Health data is not just important for patients.

Anonymized, it can be a great source of information
for researchers and authorities.
In Europe, My Health My Data, which is being funded
under the EU Horizon 2020 programme,
aims to use blockchain to create
the world's first open biomedical information network.
Among other things it would encourage hospitals
to make anonymized data available to open research
and make it easier for citizens
to take control of their health records.
In the above use cases what is proposed
is generally not storage of data itself
in a blockchain network, rather the blockchain
is used to store proof that off-chain data is genuine
or to store a record of who has access to what data.
This allows data owners to store their personal
and medical data in secure locations of their choice,
rather than allowing large number of health providers
to store the same data, sometimes in antique
and poor IT systems.
Education certification is another area
where important personal data
tends to be kept in silo databases.
Typically the universities,
or schools that issue the diplomas.
Getting access to the information
in order to prove credentials
can be a laborious undertaking.
Degrees can also be relatively easy to falsify,
causing problems for those who are trying
to verify these credentials.
Blockchain-based systems can help here
on both sides of the equation.
As with the health records they can allow individuals
to take control of the education credentials
through possession of verified records,
which they can use as needed.
Because such credentials can be easily verified,
employers, or others who rely on them,
can have more trust in their veracity.
The potential of such an approach
has been widely recognised,
and many projects have already started.
The University of Nicosia, for instance,
already issues academic certificates
that have been verified online by a blockchain.
In Malta the government is teaming up with a

122. startup to build a prototype system to do the same.
123. A consortium of Malaysian universities
124. is building a blockchain-based platform
125. to combat fake degrees, while a French startup
126. is looking to use blockchain network for the issuance
127. of sharing of university and other degrees.
128. The European Blockchain Partnership
129. has selected diploma sharing on blockchain
130. as one of the promising use cases to be deployed
131. over the European Blockchain Services Infrastructure,
132. a use case that is backed by several member states.
133. The last one is e-voting.
134. Voting is another important use case dependent
135. on transmission of private but verifiable data.
136. And e-voting has long been
137. a great prospect for e-government.
138. If citizens could easily and securely vote
139. from any location, for example, using smartphones
140. or your personal computers, we could in theory develop
141. more participatory democracies,
142. voting more often on more issues.
143. With verified data on the blockchain
144. it may be possible to design e-voting systems
145. that are much more transparent and trustworthy,
146. while preserving confidentiality.
147. In such systems election authorities
148. would issue voting credentials to users directly
149. that could be used to cast anonymous ballots.
150. Through various techniques it could then be possible
151. to automatically count those ballots,
152. ensure that no votes were cast more than once,
153. and prove the validity of the count
154. without revealing the identity of those who voted.
155. The example here is citizens of Zug, in Switzerland,
156. used their blockchain IDs earlier this year
157. to conduct the cities first blockchain-enabled e-vote.
158. While only consultative in nature, it
159. may be one harbinger of other things to come.
160. Similar blockchain based e-voting projects are
161. underway in areas far-flung
162. as West Virginia and Moscow.
163. E-voting is also mentioned as a possible use case
164. in European Parliament's blockchain resolution
165. of October 2018.

4.6.1 Use of Hyperledger Blockchain Technology in Trade Finance, Supply Chain and Digital Identity (Brian Behlendorf from The Linux Foundation)

1. You know, people talk about applications a lot
2. in blockchain, Hyperledger.
3. Can you share with us some interesting applications
4. using Hyperledger?
5. Well the most common ones tend to be in Fabric.
6. And actually, this is true for Sawtooth as well,
7. tend to be in trade finance and supply chain traceability.
8. So in trade finance, we have examples now of networks
9. that've been set up in Singapore
10. by a company called DLT
11. Ledgers working with DBS Bank
12. and others who've done hundreds
13. of millions of dollars worth
14. of extensions of letters of credit.
15. In China, a bunch of the banks there
16. have formed a consortium as well.
17. Here in Hong Kong, they've launched something called
18. eTradeConnect, a partnership with HKMA
19. and a number of the Hong Kong banks.
20. And another one called we.trade.
21. So all of these different networks are
22. springing up around trade finance,
23. and not all of them are in production yet,
24. but they are certainly growing in traction and I,
25. this is not just like an experiment
26. that will be thrown away.
27. This is actually like creating real value.
28. 'Cause trade finance has some of these
29. unique characteristics that
30. I think blockchain technology
31. is particularly well-suited for in terms of being
32. cross-jurisdictional, international by nature,
33. that sort of thing.
34. And then, supply chain traceability
35. is obviously very related to that.
36. And part of the value there is being able to know,
37. "Hey, I bought this electric vehicle.
38. The battery has a lot of cobalt in it."
39. Cobalt only comes from a few countries in the world.
40. Some of those have mines that are well-regulated
41. and they keep child labour out,
42. others do not have such good regulation.
43. And so being able to trace-ably know that your cobalt
44. comes from a known good mine,
45. or the diamond in that diamond ring?
46. Comes from a diamond mine that actually has
47. appropriate controls to prevent child labour.

48. Or even rice.
49. I mean, at the other end of the spectrum
50. from diamonds, right?
51. There's a big problem out there
52. with fraudulent rice, you know.
53. Fake rice, actually, in the supply chain.
54. And also different qualities of rice, different varietals.
55. You want to know that you're getting the right one.
56. But I think the largest meta use case kind of group
57. that I like is back to digital identity.
58. Digital identity is so essential to every digital process
59. we have now, and we're really
60. behind where we should be.
61. Your ability to prove that you have
62. a visa to travel somewhere,
63. your ability to prove that you have a diploma,
64. is bound up in systems that are locked in
65. and different standards, different protocols,
66. even when they're digital.
67. And for many people around the world,
68. they're still not digital, right?
69. And you can sense this in populations
70. that cross international borders quite a bit,
71. or in particular in populations that are refugees,
72. that are leaving behind kind of a failed country,
73. failed system.
74. And so, a lot of interesting applications out there
75. for the use of digital identity systems,
76. distributed digitalized identity systems
77. in the developing world,
78. to give people a greater sense of participation
79. in the global economic system,
80. financial inclusion, and greater dignity.
81. So I'm really excited about that.
82. And we're seeing, with Hyperledger
83. Indy deployments now,
84. in the United States and Canada, in the Netherlands,
85. but also a project to bring a national digital ID system
86. to the country of Sierra Leone.
87. And I think we'll even see countries like India,
88. that have invested a lot in a centralised digital ID model,
89. move to a self-sovereign or a kind of
90. distributed digital ID model, because that's the only way
91. you can support migrant populations
92. and some of the greater
93. resiliency that that model brings.

4.6.2 To Use Or Not To Use Blockchain

1. We also know that not all the applications
2. fit blockchain platform, right?
3. Have you come across any failure cases
4. in applying Hyperledger in some use cases?
5. In 2019, we know better how to build agile systems,
6. how to start small,
7. how to do POCs,
8. how to grow them.
9. All this technology is about trust, all right.
10. Some markets have a big trust gap
11. especially if you're crossing international borders,
12. especially if you have weak institutions,
13. that's going to matter,
14. but in a single country,
15. if you have parties that regulations are solid,
16. and the court systems are efficient and all that,
17. you might not need a blockchain right,
18. and so the relative value of that
19. differs use case to use case,
20. and that's where I have seen
21. some projects get launched and people realise
22. it's not worth the extra cost because
23. no blockchain solution is going to be faster
24. than a centralised database.
25. A centralised database is going to be
26. faster and cheaper,
27. easier to upgrade
28. almost better by every measure
29. except you have to figure out
30. somebody to run that who you trust,
31. and that's when you want to use a blockchain
32. is when you don't want to give
33. somebody that much power.

4.7.1 Use Case: How Walmart Brought Unprecedented Transparency to the Food Supply Chain with Hyperledger Fabric (Julian Gordon from The Linux Foundation)

1. Supply chain is one of the hottest areas
2. for blockchain solutions,
3. with many use cases in production today.
4. Two great examples are from Walmart
5. and a start up from the UK called Circulor.
6. At Walmart, they face the challenge
7. that when an outbreak of foodborne disease happens,
8. it can take days, even weeks, to find it's source.

9. Better traceability could help save lives
10. by allowing companies to act faster
11. and protect the livelihoods of farmers
12. by only discarding produce from affected farms.
13. Walmart thought that blockchain technology
14. might be a good fit for the
15. decentralised food supply ecosystem.
16. To test this idea,
17. the company created a food traceability system
18. based on Hyperledger Fabric.
19. Walmart, with it's technology partner, IBM,
20. ran two proof-of-concept projects to test the system.
21. One project was tracing mangoes
22. sold in Walmart's U.S. stores,
23. and the other aimed to trace
24. pork sold in it's China stores.
25. The food traceability system
26. built for the two products worked.
27. For pork in China,
28. it allowed uploading certificates of authenticity
29. to the blockchain,
30. bringing more trust to system
31. where trust used to be a serious issue.
32. And for mangoes in the U.S.,
33. the time needed to trace their provenance
34. went from seven days to 2.2 seconds.
35. Walmart can now trace the origin of over 25 products
36. from five different suppliers,
37. using a system powered by Hyperledger Fabric.
38. The company plans to roll out the system to
39. more products and categories in the near future.
40. It has announced that it will start requiring
41. all of it's suppliers of fresh, leafy greens
42. to trace their products using the system.

4.7.2 Use Case: How Circulor Achieves Traceability of Tantalem Using Hyperledger Fabric (Julian Gordon from The Linux Foundation)

1. Another great supply chain case study
2. comes from Hyperledger member, Circulor.
3. Rwanda is the worlds biggest supplier of tantalum,
4. a rare mineral used to make capacitors
5. found in devices like smart phones and laptops.
6. But tantalum is sometimes smuggled in
7. from conflict-ridden Congo,
8. where it is mined by children
9. or workers enslaved by warlords.

10. This led the OECD, US and the EU
11. to name tantalum a conflict mineral
12. and pass regulations to improve its traceability.
13. Despite these rules, no one had a fool proof way
14. to prove where tantalum came from, until now.
15. The Rwandan government and mine operator,
16. Power Resources Group,
17. wanted to prove that every bag of tantalum ore
18. from Rwanda was mined, transported, and processed
19. under OECD approved conditions.
20. UK based technology company,
21. Circulor, created a system
22. that ensures tantalum is mined, transported,
23. and processed under approved conditions
24. with an unbroken chain of custody.
25. They engaged stakeholders across the supply chain,
26. mapped the tantalum supply chain,
27. and created fool proof new processes
28. to build the blockchain.
29. Powered by permissioned blockchain,
30. built on Hyperledger Fabric,
31. the system uses facial recognition and QR codes
32. to deliver a real world first,
33. mine to manufacturer traceability of this vital resource.
34. And the results,
35. the blockchain based system to trace tantalum
36. went live in three mines
37. and an ore sorting facility in Rwanda
38. in the autumn of 2018.
39. The system is designed to slash today's
40. high cost for compliance, satisfy regulators,
41. reassure consumers, and build revenues for Rwanda.

Module 4 Reference Reading

References and Suggestions for Further Reading in Module 4

NOTE: There are many published information on blockchain applications and use cases, the following are some examples:

- 17 Blockchain Applications That Are Transforming Society (Industry news article)
- Top 10 Real-world Applications of Blockchain Technology (Industry news article)
- 5 Applications for Blockchain in Your Business (Industry news article)

Module 5 The Limitations, Opportunities and Challenges of Blockchain

Welcome to Module 5

Dear Learners,

Welcome to Module 5 – The Limitations, Opportunities and Challenges of Blockchain. In the last Module, we looked at the key selection criteria for blockchain applications and some best fit use cases in public and enterprise blockchains from guest speakers from different industry sectors.

In Module 5, we are happy to introduce six guest speakers to you, among others, Malcolm Wright (Chief Compliance Officer at Diginex) who will discuss the Privacy and Security risks of blockchain and Jon Rout (Head of Product for APAC, Digital Asset) will share his expertise on Applied Smart Contracts. Then we will hear from Alan Cheung (Director, Advanced Digital Systems of Astri) who will share the opportunities of blockchain for health insurance, and Johnny Cheung (General Counsel of B.C. Technology Group) will discuss the benefits of blockchain in banking. Also, our key instructor from Introduction to FinTech course, Henri Arslanian (FinTech & Crypto Leader for Asia, PwC) will talk about the institutional opportunities in the digital asset space.

Furthermore, our other key FinTech instructor, Brian Tang will talk about Understanding Facebook's Libra – in the Context of Wechat Pay, Bitcoin and Hedera in a series of short videos.

This is a pretty exciting week. May you enjoy the great contents from our guest speakers.

HKU Blockchain and FinTech Course Team

Module 5 Learning Objectives

After completing Module 5, learners should be able to:

- **understand the security and privacy concerns of a blockchain platform;**
- **have a brief understanding of possible risks in different components of a blockchain platform;**
- **learn more the benefits of using blockchain in various applications and industries.**

5.1.1 Five Modules in Blockchain Systems

1. I hope you still remember
2. that we have three properties
3. that we want to satisfy for the blockchain platform.
4. The first one is decentralization,
5. that is we do not want to
6. have a centralized management

7. to overlook the system.
8. The second one, of course,
9. we want to guarantee the
10. security and privacy, as well.
11. The third property is scalability.
12. We want to make sure that the blockchain
13. is still efficient, even if you have lots of users
14. and lots of transactions.
15. And we all know that no existing cryptocurrencies
16. or blockchain platforms can
17. satisfy all the three properties.
18. So we have talked about the
19. scalability issue before,
20. so in this module, we mainly will focus
21. on the security and privacy issues.
22. Now, in fact, we have experienced two stages
23. of blockchain already.
24. People usually name it Blockchain 1.0
25. and also Blockchain 2.0.
26. Now, for Blockchain 1.0,
27. the blockchain is mainly used for cryptocurrencies
28. but then in about 2013,
29. Ethereum started to introduce smart contracts.
30. Simply speaking, it's an embedded program
31. inside a blockchain that can be executed automatically
32. and this marked Blockchain 2.0.
33. Now smart contracts basically can enable the developers
34. to write new applications on blockchain
35. and then at the moment,
36. people started to expand blockchain
37. into other areas
38. such as health care, supply chain,
39. charity, journalism, music industry, etc.
40. but then on the other hand,
41. these smart contracts also introduced a lot
42. of security problems.
43. In this module, we will try to look
44. at the security and privacy issues.
45. If we want to take a closer look
46. at a real blockchain system,
47. we can divide the blockchain system
48. into the following modules.
49. The first one is the lowest level.
50. We usually call it system level.
51. It's about its overall system architecture
52. and how you put the transactions into the system.
53. It's about data structures, etc.

54. And of course, because we need
55. to write the smart contract,
56. we need programming languages,
57. so the language design will be an issue,
58. whether the language design is secure or not.
59. So the second module is the programming.
60. The third one is the crypto scheme.
61. I hope you still remember that blockchain actually uses
62. quite a number of cryptographic elements
63. in order to make sure that the
64. blockchain is secure and safe.
65. For example, the public key, private key
66. cryptography,
67. digital signature as well as the hash functions.
68. And on the other hand,
69. we also need a trust model
70. in order to get a consensus among of users
71. because there's no centralized management,
72. so all the decisions will be made
73. by all the users in the system,
74. so we need a protocol
75. or a consensus protocol
76. to make the final decisions for the blockchain.
77. And finally, of course,
78. if the developers are going to
79. write different applications,
80. then we have an application layer
81. which may also introduce security
82. and privacy issues.
83. Now, based on these five modules
84. in a real blockchain system,
85. actually the researchers have done a recent survey
86. in 2017 – the conclusion is that blockchain
87. is not 100% secure
88. and is not 100% privacy-preserving.
89. Now, they actually located at least nine risks
90. inside these blockchain systems.
91. We are not going to go over all of them.
92. We will try to pick some of them
93. so that you can understand the risks
94. if you are going to use a blockchain system.
95. And these nine risks
96. can be mapped into the five modules we talk about.
97. In other words, some of the security risks
98. are introduced by the system design,
99. some by the programming language
100. to be used for the smart contracts,

some are introduced in the applications,
some are actually introduced
by using inappropriate crypto schemes
and some may be introduced in the consensus protocol.
So we will try to take a closer look
into some of these risks today.

5.1.2 Limitations of Blockchains (Part 1)

Now, you probably have heard
about this 51% vulnerability
in the internet, but what does it mean?
Now, before we talk about
this 51% vulnerability,
let's do some review first.
So I hope you still remember blockchain
has no single centralized administration,
so who is going to help to add
new transactions into the chain
and how to guarantee
these chains are valid?
In fact, if you still remember,
in the public chain,
everybody joining the scheme in the network
is going to decide which new transaction
is going to be added into the chain
and how to guarantee the validity of these transactions.
So, everybody will try to keep a copy of the chain
and when A has a new transaction,
he will try to broadcast this transaction to everybody
and everybody can help to track it.
In fact, this "everybody",
usually, people call them the miners.
Okay, the miners will have to
check whether this transaction
is valid according to the history
of the blockchain, the transactions,
and then, try to append this into the chain.
And of course, the first one who can complete this
will broadcast the new chain.
And I hope you still remember
we do have some chaos, right?
At the beginning, we assume that every miner
has the same blockchain, but after a while,
miner A may append a new block
and broadcast, but B and C may not get it
because they are in the network.

39. Or for example, miner E, who
40. may be an adversary, okay,
41. a bad guy, may try to append
42. a fake block and broadcast it,
43. and D does not know it, may
44. work on E's blockchain.
45. So even worse, F may try
46. to double spend his money,
47. send out two transactions
48. giving the same amount of money
49. to two different users and broadcast it.
50. So in other words, even if we
51. start with a correct blockchain
52. and eventually, then we might
53. have some fake blocks appended
54. to the blockchain
55. and also, there may be
56. some double-spending cases
57. in the blockchain.
58. Then what we are going to do,
59. if you still remember,
60. all the miners will try to
61. validate all the transactions.
62. So a very simple rule that blockchain follows
63. is everybody will try to follow the longest chain.
64. Now, the rationale behind is
65. very simple because we assume
66. that the majority of the miners are honest.
67. So what does it mean?
68. It means that every miner will try to look
69. at the transactions
70. and they will try to pick the chain
71. with the valid transactions there.
72. So, therefore, more people will vote on the correct chain
73. and the chain will get longer and longer.
74. For example, the existing chain
75. only has one transaction,
76. Tr1, and then, we have a
77. correct transaction, Tr2,
78. and a fake transaction, Tr2′,
79. and most miners will
80. check both transactions,
81. Tr2 and Tr2′,
82. and they will agree that the
83. correct chain should produce
84. Tr1 to Tr2 instead of Tr1 to Tr2′.
85. So in other words, more

86. miners will keep the copy
87. of the correct chain
88. and further work on it, so it
89. will become longer and longer.
90. And I hope you still remember
91. why the miners want to help.
92. Because of the incentive.
93. So in return, they have
94. the blockchain system
95. to validate the transactions
96. and put the transactions into the blockchain,
97. append it to the blockchain.
98. Then, he can receive a new coin for himself
99. and sometimes, also get the transaction fee
100. depending on the owner.
101. The validation process only involves
102. checking the account balance
103. and seeing whether the transaction is valid or not,
104. so it can be done very quickly.
105. So, in order to make it difficult,
106. we are trying to use the Proof of Work concept.
107. I hope you still remember this.
108. We talked about it in the previous module.
109. So what you do is they need
110. to solve a difficult problem
111. in order to append a new
112. transaction to an existing chain.
113. Let me summarise the scenario first.
114. So if a new transaction is broadcast,
115. the miners will try to work on
116. the validity of the transactions
117. and at the same time, they will spend
118. their computational power to solve a problem.
119. So, after they solve the problem, get the solution,
120. and after the validation process,
121. then they can broadcast a new chain with
122. the new transaction appended
123. to the original chain.
124. Now, so in other words, who can control
125. which new transactions to be appended to the chain
126. actually depends on whether
127. he can solve the problem quickly.
128. Also it would depend on the majority of the miners
129. because they are the ones who
130. validate the transactions
131. and decide which transaction
132. to be appended to the new chain.

133. Now, so I hope you now will understand
134. what is the 51% vulnerability.
135. In other words, the principle
136. behind is to go for the majority.
137. If you are powerful enough
138. to control more than 50%
139. of the computational power,
140. you are able to control
141. more than 50% of the miners,
142. then you can control the miners
143. to add which transactions to the new blockchain.
144. Then you can ensure that your chain is the longest
145. and then, you can control how the chains look like.
146. And basically, you can append fake transactions,
147. double spending transactions into the blockchain,
148. and nobody can object this
149. because you already control
150. over 50% of the miners
151. and have more than 50% of
152. the computational power.
153. So in other words, if you are going to use the blockchain
154. with a pure PoW consensus algorithm,
155. then you need to be very careful who are the miners
156. and whether there's somebody actually controlling
157. more than 50% of the computational power
158. and also control more than 50% of the miners.
159. Now, I hope you also understand why the throughput
160. is not high because we need
161. to give the miners some time
162. to solve the difficult problems
163. and also, we need to wait a
164. certain amount of time in order
165. to distinguish which blockchain is longer
166. in order to take the blockchain
167. as the valid blockchain.
168. So therefore, you can see that if you use
169. a pure PoW consensus algorithm,
170. the transaction throughput
171. of the design of the blockchain system
172. is only about seven or eight
173. transactions per second.
174. This is also one of the scalability issues
175. we need to resolve.

5.1.3 Limitations of Blockchains (Part 2)

1. Now I'm going to give you more examples

2. why we say that the blockchain system platform
3. is not 100% secure.
4. Now, my next issue is about the private key security.
5. I hope you still remember
6. that we are not using our real names
7. when we are trying to create an account
8. or a wallet in a blockchain.
9. So do you still remember what we used
10. to create a account or blockchain wallet?
11. Basically we are using public keys
12. and private keys in order to access the account
13. and usually the private key is the key
14. in order to access the account.
15. Now, if the private key is being stolen,
16. your money will be gone
17. and there's no way to trace the money
18. because we do not have a centralised management
19. to look over all the wallets and the accounts.
20. Now, some researchers actually
21. discovered a vulnerability
22. in a crypto scheme which is called ECDSA.
23. They use it in blockchain
24. and they find that the private key they generate
25. is not random enough.
26. So in other words, an attacker has a chance
27. to recover a user's private key.
28. Now, once the private key is being recovered,
29. the attacker can actually access to the wallet
30. and transfer the money to his own account
31. and there's no way to trace
32. where the money will be going.
33. So this is another example showing that sometimes
34. if the developer did not use a correct
35. or an appropriate crypto scheme
36. in the blockchain system,
37. we may also have a security issue there.
38. Now, let's turn to look at the security
39. of smart contracts.
40. As I mentioned,
41. from blockchain 2.0,
42. the smart contracts actually enabled developers
43. to write a lot of new applications.
44. Now, according to a study
45. by the Black Hat USA in 2018,
46. there are already 1.5 million
47. Ethereum smart contracts that
48. have been created in the blockchain

49. but unfortunately, based on another survey
50. by IBM and IIT,
51. based on the amount of smart contracts they studied,
52. they have indicated that 94.6%
53. of the contracts which contain
54. cryptocurrencies worth more
55. than $0.5 billion are vulnerable.
56. In other words,
57. these smart contracts are not safe.
58. According to a survey,
59. they also listed a lot of smart contract securities,
60. for example, in particular,
61. they have identified some security issues
62. on the programming languages
63. for smart contracts in Ethereum
64. which is called Solidity.
65. In other words, people use Solidity
66. as a programming language
67. to write smart contracts in Ethereum
68. but then they find that they require a number
69. of security issues there.
70. Now, in this module, I'm going
71. to tell to you some of them.
72. There were also major incidents that happened before.
73. Okay, let me just give you some idea
74. about what had happened before.
75. A DAO attack happened in June 2016.
76. DAO actually is a smart contract
77. written for crowd funding.
78. So people tried to give funding to the projects based
79. on this smart contract
80. and in fact, it's very successful.
81. In 20 days, they raised about US $150 million.
82. However, the attackers exploited the vulnerability
83. of Solidity, they found a loophole
84. in the programming language of Solidity,
85. so they found a security hole in the smart contract
86. and about US $16 million was stolen.
87. And another major instance
88. happened in a Bitcoin exchange
89. in March 2014.
90. Actually this Bitcoin exchange
91. was one of the world's largest Bitcoin exchanges.
92. It handles over 70%
93. of all the Bitcoin transactions
94. and they also exploited a security hole
95. in Bitcoin which is called the transaction mutability.

96. And US $450 million Bitcoins were stolen.
97. If I remember correctly,
98. actually the company went bankrupt
99. after this amount of Bitcoins had been stolen.
100. Now let me just give you a very, very rough idea
101. what the transaction mutability is about.
102. It's very easy to understand.
103. I hope you still remember,
104. every transaction, for example,
105. the details about how much money from which owner
106. to give which receiver
107. will be digitally signed
108. and then usually the transaction ID
109. will be the hash of the transactions.
110. Now, in earlier implementations
111. because it was in 2014,
112. there's no standard for appending data.
113. In other words, when they create a hash,
114. what they do is they would try to put the content
115. of the transaction together with a padding string
116. at the end, a 01, a random 01 at the end
117. in order to create a hash.
118. Now, because this hash is the transaction ID,
119. so if the attacker is able to change the padding string,
120. then the ID will change
121. and then what they are trying to do is they claim
122. that the transaction is being lost.
123. In fact, the transaction has been transferred
124. into their account
125. but they changed the padding string
126. so the ID changes so the owner
127. cannot trace the transaction
128. where it has been gone.
129. So basically the owner
130. will try to issue another transaction again
131. and transfer the money again,
132. so they try to do this – retry, and retry
133. and then transfer the money
134. out from a single account.
135. So this is basically how they
136. could steal 450 million Bitcoins
137. from the account.
138. So the platform realized this security hole,
139. so they fixed it already
140. but then on the other hand,
141. we still have a lot more security issues
142. in smart contracts.

143. I wanna give you some more examples,
144. so that you can be aware that while using smart contracts,
145. one needs to be very careful.

5.1.4 Limitations of Blockchains (Part 3)

1. Now the famous one is called
2. the under-priced DoS Attack.
3. DoS is the Denial-of-Services attack.
4. So what they are trying to do is the attacker tries
5. to create some smart contract
6. in order to slow down the performance
7. of the blockchain system.
8. Let me give you some basic idea first.
9. Now, smart contracts, as we mentioned,
10. will enable the developer
11. to write programs to be executed
12. in the blockchain
13. but it doesn't come for free,
14. so in Ethereum, they have a charging scheme.
15. So every user, if they want
16. to execute a smart contract,
17. they need to pay for it
18. and then every operation in that smart contract
19. will be assigned a certain amount of units
20. to be charged.
21. Usually they call this gas units in Ethereum
22. so the user can specify the price per gas unit
23. and the limit and the miner
24. who helps to execute the code
25. will get the execution fee,
26. so that's why the miner is willing to help
27. because they can get the reward
28. from helping to execute the smart contracts.
29. So the attack idea is very simple.
30. They will look for the operations
31. that are under priced,
32. in other words, you can just pay a little bit amount
33. of money or gas units,
34. then you can execute the operations
35. and then what they do
36. is they repeatedly execute these operations
37. in order to slow down the operation
38. of the whole blockchain.
39. Now, there were two real attacks in 2016.
40. One is called EXTCODESIZE,
41. the other is called SUICIDE.

42. Now let me talk about them one by one.
43. Now, there's an attacker,
44. they deploy a smart contract
45. involving many EXTCODESIZE operations
46. and it's about 50,000 per block
47. and then you can imagine
48. that because we still need to execute these operations,
49. so the clients will spend
50. a long time processing these transactions.
51. Actually, he try to slow down the whole blockchain
52. and the throughput drops quickly at that moment.
53. So it becomes a DoS attack.
54. The reason is when the designer
55. tried to decide the gas cost for this operation,
56. they set a very low cost, only 20 units
57. but on the other hand,
58. this operation involves expensive
59. input/output operations.
60. So in other words, every node in Ethereum
61. will try to maintain the same copy of the blockchain.
62. Now, in the old days, they only need
63. to download all the transactions
64. of the whole blockchain
65. but because of a smart contract,
66. so if they want to get a copy
67. of the whole blockchain,
68. what they need to do is they need
69. to download all the transactions
70. and also download all the smart contracts
71. in the blockchain
72. and also, execute all the historical transactions
73. in order to synchronise the blockchain
74. with the other one to which the same state.
75. So in other words, for every smart contract
76. inside the blockchain,
77. the miner has to execute it, all of them
78. in order to achieve the same state as the others.
79. So if you think about it,
80. if you have many of these operations to be executed,
81. then you can see that every miner
82. has to download a lot of smart contracts
83. and try to spend a lot of time in
84. executing all the smart contracts before they start to
85. validate new transactions to append to the blockchain.
86. So that's why we call it's a DoS attack.
87. It means we try to make the service unavailable
88. to the users.

89. Now the solution at that moment
90. is they've realised that this operation,
91. the gas cost is too low,
92. so what they do is they increase it
93. from 20 to 700.
94. It's about like US $.0042
95. in order to stop this kind of DoS attack.
96. Now another one,
97. we usually call it the SUICIDE attack.
98. Now, this is very similar.
99. The attacker tries to deploy a lot
100. of smart contracts and these smart contracts,
101. they execute a particular command
102. and this command, this operation is called the SUICIDE
103. and the SUICIDE command is very simple.
104. What they do is they try
105. to stop the executable smart contracts
106. and try to send the remaining money,
107. the Bitcoin or token into the designated account.
108. So in other words, SUICIDE means
109. that I realize that I need to stop this contract
110. and put the remaining balance
111. of the money into a designated account.
112. Now, in the original design,
113. if the SUICIDE cannot find the target account,
114. it will create a new one
115. and to create a new account is time-consuming
116. and the consequence of this attack
117. is they find that 19 million of new accounts
118. were created for nothing.
119. So you can see that it's the time,
120. the disc space also wasted
121. and if you look at the reason for this,
122. it's because the original designer set the gas cost
123. of this operation to be zero,
124. so in other words,
125. I can write a smart contract
126. with lots of SUICIDE operations
127. in it without paying anything
128. but then the system has
129. to execute this operation
130. in order to create new accounts
131. and execute the SUICIDE operations.
132. Then right now the solution is they try
133. to increase the gas cost
134. of the operation from zero to 5,000
135. and if you need to create a new account,

136. you need to pay another 25,000 gas units
137. in order to stop this kind of attack.
138. Now you can see that there are solutions proposed
139. like increasing the gas cost of under-priced operations,
140. there are still a lot of possible attacks
141. and actually the attacks have been stated
142. in one or two survey papers already.

5.1.5 Limitations of Blockchains (Part 4)

1. Now so you can see that security
2. is an issue in the blockchain platform,
3. it's not a 100% secure system,
4. so when we are using blockchain system,
5. you need to pay attention to the security issues.
6. Now, on the other hand,
7. privacy is also an issue.
8. Now, I hope you still remember
9. that all the transactions in the original design
10. of the blockchain are transparent
11. meaning that everybody can
12. look at all the transactions.
13. Now, although we do not use real names
14. but people can still look at the details
15. of the transactions, for example,
16. I can check from which wallet to which wallet,
17. how much money has been transferred.
18. In fact, people have done analysis
19. on this wallet relationship
20. and have identified some of the transactions
21. and I will talk about this in the next lecture
22. but on the other hand,
23. then you can see that we cannot expect 100% privacy
24. in a blockchain system.
25. Now let me elaborate a little bit more.
26. Usually we are talking about three types of privacy.
27. One is the sender privacy,
28. the identity of the sender
29. and also the identity of the recipient.
30. Of course, we want to hide these two identities.
31. We do not want people to know
32. who is going to pay money to the other person
33. but on the other hand, the amount,
34. the information inside a transaction
35. should also be kept confidential.
36. So we do have another privacy,
37. the privacy of the details of the transactions.

38. At this moment, none of the existing schemes
39. can achieve all three types of privacy
40. and at the same time can make the platform scalable.
41. So in other words,
42. we do not have a perfect system
43. that can protect the privacy of the sender,
44. the identity of the recipient
45. as well as the information inside the transaction
46. as well as making the blockchain system scalable.
47. Many researchers and practitioners,
48. they realized this problem,
49. so they started to address this issue.
50. Let me give you some examples.
51. Zcash, they basically tried
52. to leverage a cryptographic technique
53. which is called zero knowledge proof
54. in order to hide the identity of the sender, recipient,
55. as well as the information
56. inside a transaction.
57. The other cryptocurrency, Monero,
58. actually use a linkable ring signature.
59. There are many, many others
60. but at this moment,
61. we will cannot see a blockchain platform
62. that can actually achieve all these three types
63. of privacy and they are scalable.
64. So do not expect 100% privacy protection yet.
65. Now I hope I have given you enough examples
66. to show that there are security
67. and privacy issues in blockchain systems.
68. Now although blockchain is a great platform
69. with lots of potential and implications,
70. but on the other hand,
71. I hope people could be aware the security,
72. privacy, scalability issues.
73. All these issues are not yet completely resolved.
74. So in this module, we mainly talk about some
75. of the security and privacy issues.
76. In the next week,
77. we will talk about some evil sides
78. of blockchain and Bitcoins.

5.2.1 Risks and Limitations of Blockchain: Privacy (Malcolm Wright from Diginex)

1. Today I'm going to discuss two topics
2. around the risks and limitations of Blockchain.
3. First, I'll discuss privacy considerations that developers

4. and firms that use Blockchain should be aware of.
5. I'll then discuss some key security risks
6. and what can be done to mitigate them.
7. In the context of privacy then.
8. I will use the European Union's General Data Protection
9. regulation, or GDPR, as the baseline for this discussion.
10. The GDPR came into effect on
11. 25 May 2018 and is generally
12. regarded as the benchmark data privacy standard.
13. With Blockchain projects often
14. spanning different countries,
15. it is appropriate to take
16. the highest benchmark
17. as we consider privacy issues.
18. So what do we mean by personal data?
19. Personal data means any information relating directly
20. or indirectly to a living natural person,
21. where it identifies them or makes them identifiable.
22. Processing personal data means any operation
23. or set of operations performed
24. upon the data, for example,
25. collection, recording, organisation,
26. structuring, storage,
27. adaptation and alteration.
28. The nature of blockchain
29. means that every transaction
30. taking place will be published and linked to a public key
31. that represents a particular user.
32. The public key is encrypted
33. to prevent anyone who views
34. the blockchain from being
35. able to identify the user.
36. However, the re-use of the
37. public key enables individuals
38. to be singled out by
39. reference to their public key,
40. even if they cannot be directly identified.
41. The public key, when associated with an individual,
42. will likely qualify as personal data
43. for the purposes of the GDPR.
44. However, there are some blockchain technologies
45. that permit the public key not to be published,
46. which may change how we view this.
47. When the public key is visible,
48. it could be possible to attain information
49. that enables an individual to be identified,
50. either because it is held by the service provider

or because somebody is able to connect
a public key to the individual.
At that point, all transactions that the relevant
individual has made are then publicly available.
So you may ask, can we not just anonymize the data?
The European Union Working Party on Data Protection
provided guidance on the difference
between pseudonymized and anonymized data.
This distinction is important in relation to blockchain
as data protection rules do
not apply to anonymized data;
as such data cannot be traced
back to a living individual.
However, the threshold for data
to qualify as anonymized is very high.
Encrypted personal data can often be traced back
to a person if enough effort is put in by experts
or someone who holds the key to decryption.
Therefore, encrypted data will often qualify
as personal data and not as anonymized data.
This means that in most instances the privacy rules
will be applicable to at least some of the data
involved in blockchain systems.
Blockchain technology relies on hashing,
which consists of generating a code of a fixed length
for a given piece of digital information,
regardless of its length.
Hashing is important because
it permits somebody to verify,
by recalculating the hash that a given piece
of information is identical to the digital
information that was originally hashed.
A hash cannot be reverse-engineered
to discover the original information.
The process only works in one direction,
from the original document to the hash.
Yet in spite of this, the European Union Working Party
on Data Protection stated that hashing
is a technique of pseudonymisation, not anonymisation.
According to the working party, it is sufficient
for a hash to permit records to be linked for a piece
of information to constitute personal data.
Therefore, a hash that represents a person's ID card
would likely be considered personal data
even though the hash itself is impossible to reverse
engineer into the personal information.
Finally on privacy, one of the design features

of blockchain architecture is that transaction records
cannot be changed or deleted.
The GDPR recognises a right to deletion.
The broad principle underpinning
this is the right to enable
an individual to request the deletion or removal
of personal data where there is no compelling
reason for its continued processing.
Clearly this is at odds with Blockchain architecture
and it is for this reason that it is advisable
for personal data to be kept off-chain.

5.2.2 Risks and Limitations of Blockchain: Security (Malcolm Wright from Diginex)

Moving on to our second topic then.
Blockchain security.
Here, I'm going to focus on three areas of risk.
First, the 51% attack.
This is where bad actors gain 51%
of blockchain mining power
on a particular blockchain network.
51% attacks are one of the most recognised
blockchain security flaws.
Once 51% of the mining power, or hashrate,
has been achieved, bad actors
can reverse transactions
to perform double-spends
and prevent other miners
on the network from confirming blocks.
A double spend is an attack where a given set
of coins is spent more than once in a single transaction.
In 2018, several notable
cryptocurrencies such as ZenCash,
Verge, and Ethereum Classic fell victim to 51% attacks.
The attackers walked away with
over 20 million US dollars
due to the blockchain security issue.
Where a blockchain utilises a Proof-of-Work
consensus mechanism it will need mitigations in place
to prevent this type of attack.
Such mitigations might include being vigilant
of mining pools on the network,
implementing merged mining on a blockchain
with a higher hashrate, or switching
to a different consensus mechanism.
The second security issue we'll cover are software
or smart contract flaws.

34. Most of the larger blockchains such as Bitcoin
35. and Ethereum have proven their resilience to attack.
36. However, the apps built on top of them are still
37. susceptible to bugs as well as malicious coding.
38. Last year, software bugs alone in wallets
39. and decentralised apps, or dApps,
40. led to over 24 million US dollars in damages.
41. It is important that any software using blockchain
42. undergoes rigorous testing and review.
43. This process should include
44. independent code reviews,
45. penetration testing, and smart contract audits.
46. Additionally, any reputable application should have
47. redundant security measures in place.
48. And finally, private key security.
49. If someone's private key is accessed
50. by an unauthorised individual, their transactions are
51. no longer considered reliable
52. as the encryption can be broken.
53. To prevent this, controls should be in place
54. to safeguard the private key used to protect
55. an individual's transactions.
56. Where a user is holding self-custody of their private key,
57. they should ensure that access to it is controlled
58. and a strong private key is used to secure it.
59. Early in 2019 researchers uncovered
60. that a blockchain bandit had made off
61. with over $50 million US dollars where they were able
62. to guess simple private keys,
63. find the associated public key,
64. and then clear the address of funds.
65. Where the private key is being held by a custodian
66. or an exchange, the responsibility is
67. then with the custodian or the exchange to ensure
68. they have taken appropriate steps
69. to secure the private keys.
70. One of the weakness that has
71. been noted in the past here is
72. that the users themselves very often do not know
73. what to ask of a third-party custodian or exchange
74. to verify that their keys will be held safely.
75. This then, is where the industry can help to educate
76. and where courses such as this one are important.

5.2.3 The Five Security Risks of Blockchain (Alan Cheung from Hong Kong Applied Science and Technology Research Institute (Astri))

1. I think many people have already explained
2. the basic concepts of blockchain.
3. But still, up to today, many still have concerns about
4. the potential issues of blockchain.
5. I will spend a little time to share our points of view.
6. The first topic is about 51% vulnerability.
7. This is caused by the mechanism
8. of the block mining consensus operation.
9. It happens in public blockchains,
10. particularly cryptocurrency,
11. when using proof of work consensus
12. that requires computation by blockchain node.
13. Hackers often stage concerted attack
14. by using hardware-assisted miners
15. to become the fastest winner in the mining process.
16. Since the winning miner can
17. build new transaction blocks,
18. the hacker will essentially
19. take over blockchain operations.
20. However, it depends on how easy it is to own
21. the majority mining power of
22. such a blockchain network.
23. The setup costs of miners could be very high
24. to achieve this attack.
25. For permissioned blockchain,
26. the issue could be less of a concern
27. because the consensus algorithm is different
28. and the participating parties would agree
29. on certain legal and governance terms
30. and therefore will be better protected
31. when operating such a network.
32. About private key security.
33. As of today, most blockchains
34. employ public key cryptography
35. for identification.
36. It's usually in a blockchain host private key.
37. Ideally, the private key should
38. be only known to the user.
39. However many cryptocurrency exchanges
40. store the private keys of the users in online wallets.
41. There have been cases where users' private keys
42. in online wallets has been stolen by hackers.
43. And as a result, lots of funds had been stolen.
44. The keys in the online wallet must be protected
45. with some kind of multifactor authentication
46. to avoid being stolen.
47. In a permissioned system, however,

48. standard IT security guidelines needs to be followed
49. to minimise identity fraud.
50. Permissioned blockchains also
51. use certificates of authority
52. to manage certificates of private keys.
53. Therefore, user access can be rerouted
54. if the keys are stolen.
55. About criminal activity.
56. Bitcoin, because of its anonymous transaction nature,
57. is often used for criminal activities
58. such as money laundering,
59. blackmailing, and ransomware.
60. To deter money laundering,
61. some governments require cryptocurrency exchanges
62. to collect customer's personal information
63. and contact KYC procedures.
64. Permissioned blockchains usually are subject
65. to periodical audit to detect illegal activities
66. and to comply with regulatory requirements.
67. About double spending.
68. Professional hackers can exploit
69. the infrastructure of blockchain to make it possible
70. to double spend the cryptocurrency.
71. They can perform so called DDOS attack
72. on the blockchains nodes
73. and break the blockchain P2P network
74. into multiple fragments,
75. and then they can spend the cryptocurrency
76. on each of the network fragments.
77. They can also use hardware mining chips
78. in the set of money nodes
79. to dictate the transaction in the blockchain.
80. There are efforts in the public blockchain platforms
81. to make their mining algorithm hardware-resistant.
82. While many permissioned blockchains
83. do not issue cryptocurrency and
84. the money nodes are trusted.
85. However, they still need to ensure the network
86. has sufficient redundancy to
87. prevent network fragmentation.
88. About the vulnerabilities in smart contracts.
89. Smart contract is a string of blockchain.
90. It allows blockchain to execute
91. complicated business logic.
92. However, a misconstructed smart contract
93. can be used by hackers to
94. perform destructive operations.

95. An example is the Ethereum DAO,
96. distributed autonomous organisations smart contract.
97. It's just originally used to allow people
98. to fund blockchain projects with their own crypto coins.
99. However, there's a program flaw
100. in the initial version of the smart contract.
101. An attack on it was staged in June, 2016.
102. The attacker managed to retrieve approximately
103. 3.6 million Ether from the DAO fund.
104. For the permissioned blockchain platform
105. they should also take precaution
106. to prevent the presence of vulnerabilities
107. in the smart contract.
108. They should conduct security code scanning
109. on smart contracts to remove code susceptible
110. to hacker attacks.
111. They should also conduct thorough testing
112. to avoid misuse of the smart contracts.

5.3.1 Applied Smart Contracts: Opportunities, Risks, and Applications for Enterprise (Jon Rout from Digital Asset)

1. Good day, my name is Jon Rout.
2. I work for Digital Asset, the creators of DAML,
3. an intuitive open-source smart contract language
4. that runs across a growing
5. number of distributed ledgers.
6. Enterprises use DAML to model
7. programmable digital assets
8. and to automate complex
9. multi-party business workflows.
10. You can get started programming
11. your own smart contracts
12. for free at DAML.com.
13. By the end of our session today,
14. you'll understand a little bit
15. about what smart contracts are,
16. the opportunities they bring,
17. and the risks that need to
18. be considered and managed.
19. We'll review also how DAML smart
20. contracts are being applied
21. to create real business value around the world.
22. Okay, let's get started with some clear problems.
23. Today enterprise infrastructure is siloed,
24. as you can see in the graphic here.
25. We've got a number of different cogs

26. representing the different technology stacks
27. at each institution,
28. and a number of different database types.
29. What this represents is that each institution today
30. keeps independent and duplicated records
31. of the same information.
32. Usually they run asynchronous message-based systems
33. with large teams of people
34. performing manual reconciliation
35. in order to keep the data in alignment
36. across several different firms.
37. This creates a number of challenges.
38. Firstly, technology costs are unnecessarily duplicated,
39. and upgrades become quite difficult
40. when you need to get everybody on the same page
41. at the same time.
42. Secondly, because every firm
43. is using different technologies,
44. reflected by the different cogs in the graphic,
45. there is inconsistent processing across different firms,
46. which creates the need for operational cost
47. or manual reconciliation in the first place.
48. Thirdly, there's no real-time shared state.
49. There's no guarantee that what I see is what you see,
50. between these companies on the page,
51. and this makes coordination quite tricky.
52. Finally, a distributed ledger, or blockchain,
53. that the smart contracts are running upon,
54. guarantees that each firm sees the same information
55. at the same time,
56. provided, of course, that they're entitled to do so.
57. This solves for the shared state problem
58. that we were talking about.
59. DAML smart contracts are being used
60. to upgrade the post-trade functionality
61. offered to all 120 members of the Australian market,
62. delivering for the first time
63. real-time access to GoldenSource
64. clearing and settlement data to members,
65. and significant future potential benefits
66. to all of the market such as, for example,
67. through corporate actions automation,
68. or by enabling market places for ASX
69. and third-party DAML applications
70. that can be leveraged by members of the network
71. to rapidly add new functionality
72. and create new value for their own customers.

Okay, so what advantages can smart contracts bring
to this problem statement?
Smart contracts are small pieces of executable code
designed to be shared between different participants
in a distributed ledger network,
as you can see in the picture here,
and they can really help us address
some of those problems at the very core.
Firstly, smart contracts reduce
duplicated technology costs
by shifting common business logic into shared code
that can be deployed to all of the firms
in a distributed network.
Upgrades also become easier
as new products and workflows
can be modelled as smart contracts too
and deployed to each member's distributed ledger node,
much like installing a new app
or upgrading an old one on your phone.
Secondly, because we're now
leveraging smart shared code
across all of those participants in the network,
you can also guarantee consistent processing
by each of the firms with the necessary implication
that less manual reconciliation is required
to keep everybody in sync.
Third, and finally, our distributed ledger or blockchain
that sits underneath it all,
these smart contracts run upon it in such a way
that you can guarantee that each of the firms
sees the same information at the same time,
provided of course that they're entitled to do so.
This solves for our shared state problem.
Importantly, smart contracts don't need to replace
the paper contracts that enterprises
rely so heavily on today to be valuable in the enterprise.
Really, what they can do is augment
those existing paper documents
by creating automatable versions
that can be shared between different counterparties
and used to ensure that the downstream processing
of the agreements that are being made
is consistent and quick.
Okay, so smart contracts make a lot of sense,
but what should our requirements be
as we choose our smart
contract programming language,

120. before we use it to create
121. enterprise grade smart contracts?
122. First, our key requirement is
123. that we need to be able to model what it means
124. to own different types of assets.
125. Let's think about a simple example.
126. What does it mean to own a house?
127. As an owner, for example, you have the right
128. to exclude other people from your property,
129. the right to charge a rent to your tenants
130. when they occupy the place,
131. but you also have the obligation
132. to pay property taxes to the government.
133. Your ownership then, when you think about it,
134. can really be modelled as this bundle
135. of rights and obligations that collectively represents
136. what it means to own your house.
137. This concept is extremely powerful
138. and can really be extended to basically any asset class,
139. from simple real property
140. like the one we're talking about now,
141. to complex derivative products like interest rate swaps.
142. Secondly, if we're thinking about the requirements
143. for our smart contract language,
144. you need to think about how supply chains work,
145. how business workflows work.
146. Fundamentally, these are complex processes
147. that require sequential
148. communication and orchestration
149. between multiple different firms
150. as they perform different actions in sequence
151. to create value for their end customers.
152. Successful automation in this space
153. means guaranteeing that all firms
154. that are participating in a workflow
155. are in sync on the order and status
156. of the task to be completed by each firm.
157. Our smart contract language needs to support this.
158. Third, determining which participants,
159. customers, or perhaps even regulators
160. need to be able to act upon or have visibility
161. over contracts, assets, or workflows
162. is critically important.
163. In the enterprise, it's never okay
164. to share all of the information with everybody,
165. even when the network is permissioned,
166. so we need to get intelligent here.

167. Accordingly, a well-designed smart contract language
168. needs to offer developers a simple means
169. of defining the participants
170. who may enter into agreements,
171. the capacity to successfully express
172. the bundles of rights and obligations
173. like a home ownership that we talked about before
174. that allows us to model clearly different asset classes,
175. and also to offer built-in access control.
176. Fortunately, DAML, the smart contract language
177. that we're learning about today,
178. gives you all of these features out of the box.
179. Okay, so let's think about this
180. more from a risk lens here.
181. Some of you may be more familiar with major bugs
182. in the Ethereum distributed ledger,
183. such as those in the smart contracts
184. that established the distributed
185. autonomous organisation,
186. or more recently the Parity wallet,
187. which have led to tens of millions of dollars of losses
188. for people that were affected by those contracts.
189. Most importantly, these bugs have shown the world
190. the potential cost of bad code in distributed systems.
191. Although the impact of bugs
192. can be much better mitigated
193. in permissioned enterprise DLT networks
194. than on public blockchains,
195. the potential impact of bugs
196. is still higher in distributed networks
197. than in isolated infrastructure status quo.
198. How can a smart contract language selection
199. mitigate this risk, and what are our options?
200. As you can see in the graphic,
201. general purpose programming languages
202. are generally our starting point.
203. These are languages like C++, Kotlin, and even Solidity.
204. These languages are fully featured
205. and enable experienced developers
206. to produce sophisticated functionality.
207. However, the complexity and lack of safeguards
208. inherent in those languages
209. means that the risk of unintentionally creating
210. high-impact buggy code is quite significant.
211. Next in the order of risk
212. is functional programming languages.
213. This is the family of languages

214. that include examples like Haskell and Clojure,
215. and they offer the benefit that code
216. always returns the same results given the same inputs.
217. This makes testing them,
218. or testing smart contracts that are written with them,
219. easier and lowers risk.
220. Lowest risk of all though
221. for enterprise smart contract development
222. are domain-specific languages that are purpose-built
223. to model distributed workflows across firms, like DAML.
224. Those languages leverage restriction
225. to enhance developer usability
226. and reduce the risk of errors,
227. kind of like the reason why
228. you choose to do maths problems
229. on a calculator rather than a laptop.
230. Sometimes, usability is enhanced
231. by restricting the features that are available.
232. It's really about the right tool for the job.
233. Okay, so now we've learned a bit about the theory,
234. what are some real examples of this technology
235. creating true value for the enterprise?
236. First, Digital Asset was fortunate to be selected
237. in January of 2016
238. to partner with the Australian Securities Exchange
239. to deliver a DAML-driven replacement
240. for the cash equities clearing and settlements system
241. known as CHESS.
242. This system manages all of the post-trade operations
243. for the $2 trillion Australian share market.
244. DAML smart contracts are being used
245. to upgrade the post-trade functionality
246. offered to all of the 120
247. members of the Australian market,
248. delivering for the first time real-time access
249. to GoldenSource clearing and settlement data
250. direct from the CSD
251. to members and significant future benefits
252. through, for example, corporate actions automation
253. and also by enabling a marketplace for ASX
254. and third-party DAML applications
255. that can be leveraged by members of the ASX network
256. to rapidly add new functionality
257. and create new value for their own customers.
258. Second example, right here in Hong Kong in 2018,
259. we successfully completed a prototype
260. with the Hong Kong stock exchange

261. to bring the power of DAML
262. to its post-trade allocation and processing platform
263. for northbound stock connect trading.
264. The solution helps market participants cope
265. with the very tight settlement timeframe
266. for mainland China A-shares
267. by delivering visibility of processing status
268. across all of the parties in the network,
269. significantly improving workflow
270. and accelerating troubleshooting
271. when breaks occur.
272. We're excited to continue working with HKX
273. as we look to bring those benefits to production.
274. A final example, in 2019,
275. the International Swaps and Derivatives Association,
276. or ISDA,
277. announced that they are partnering together
278. with Digital Asset
279. to build an event specification module in DAML
280. to compliment the ISDA common domain model,
281. their industry-wide blueprint
282. for how derivatives are traded and managed
283. across the trade life cycle.
284. This is designed to enhance consistency
285. and facilitate interoperability
286. across firms and platforms.
287. In this case, a DAML-driven event specification module
288. empowers front-office developers
289. to unambiguously construct the life cycle events
290. of complex derivative products
291. with machine-executable DAML code,
292. ensuring consistency across firms
293. as the life cycle of a complex
294. derivative asset progresses.
295. So, what have we learned?
296. Smart contracts can offer efficiencies to the enterprise
297. as common workflows get mutualized,
298. reducing the challenge of upgrades,
299. guaranteeing consistent processing across firms,
300. and minimising the ongoing operational cost
301. of reconciliation.
302. Second, because the potential impact of bugs
303. in distributed systems can be high,
304. it matters which language you choose
305. to write your smart contracts in.
306. Domain-specific languages like DAML
307. use restriction to enhance usability for developers

and minimise risk by giving
them the right tool for the job.
Last, we have explored some real-world applications
of smart contracts creating real value for the enterprise
around the world.

5.3.2 Applied Smart Contracts (DAML): Step-by-Step Example (Jon Rout from Digital Asset)

Okay so enough theory,
let's look at a real example smart contract
written in DAML.
On the screen now, you can see the DAML code
for a simple layer use Smart Contract template.
In DAML, we create templates like this
to describe the rights and obligations
created by a particular type
of digital asset, agreement or workflow.
These templates can be shared
by all parties in a network
and instantiated as needed on
a shared ledger as contracts.
There are a couple of key parts to the code here
and don't worry it's not scary.
Firstly, signatories, these are the parties
to an agreement who need to sign off
in order for the contract to be created in the first place.
This is important because it means
that with DAML,
a party can never be required to do something
without having first agreed to it as a signatory.
This is quite in keeping with
common law around the world.
Observers, the next thing, are the parties
who receive the notification
when a contract is changed or modified
throughout its life-cycle.
This is particularly useful
if you need to give visibility to a regulator.
Work is in done in our contract
when a choice is exercised by a controller
as you can see here.
Our IOU contract has three
simple choices modelled for us.
Different controllers in each case.
The Lender, for example, is the controller
of the Split Choice which enables them
to carve up their right to be paid back by a Borrower

40. into two different parts.
41. The Lender is also the controller of the Transfer Choice
42. which give them the capacity to request
43. to transfer their right to be repaid by the Borrower
44. to a new Lender.
45. One bank to another for example,
46. who can then choose to accept or reject their request.
47. Finally, the Borrower is the controller
48. of the Payback Choice,
49. which is their right to pay back a portion
50. of the amount outstanding on the IOU
51. and simultaneously reduce the Lender's total claim
52. to repayment by the amount they've just paid back.
53. Choices are by default are what we call Consuming
54. in our Distributed Ledger,
55. after Choice Execution takes place,
56. the old contract is archived
57. and new contracts are created in its place
58. to reflect the new state of the world,
59. the new rights and obligations
60. of each of our participants.
61. Let's look at how that works in practise
62. when our DAML Smart Contract is deployed
63. to a Distributed Ledger.
64. Let's assume for starters that
65. a loan has been established
66. and our Borrower needs to
67. pay $100 back to Lender One.
68. First, our Borrower exercises her right
69. to pay back $30 of the $100 outstanding on her loan.
70. In a single atomic transaction
71. on our Distributed Ledger,
72. the old IOU Smart Contract is archived,
73. a new IOU Smart Contract
74. with a balance outstanding of
75. $70 is created in its place.
76. The cash contract representing
77. the borrowed $100 is archived
78. and two new cash contracts are created
79. to represent the remaining $70 holding,
80. now owned by the Borrower,
81. and the $30 holding now owned by Lender One,
82. having been repaid.
83. Next, Lender One exercised their right
84. to request a transfer of the outstanding IOU contract
85. to another lender.
86. One bank transfers it to another.

87. Let's call them Lender Two.
88. This results in the old IOU
89. contract getting archived
90. and a transfer request to Lender Two
91. being created in its place
92. to represent the latest state of the world.
93. This is important, this proposed Accept Workflow
94. cause it means you can't force
95. Lender Two to accept this.
96. Lender Two can choose to accept this request
97. and if they do, it results in the creation
98. of a new IOU contract
99. that represents the real-world obligation
100. that the Borrower now has to pay back
101. the remaining $70 to Lender Two
102. instead of the original Lender One.
103. Our Borrower can now exercise her right
104. to repay the outstanding $70 loan
105. to Lender Two in partial repayments
106. of $30 and $40, respectively.
107. Each of these repayments results
108. in a transaction to the Ledger
109. that includes the archival of the current IOU contract,
110. the archival of the contract
111. representing the Borrower's current cash holdings
112. before the repayment is made,
113. the creation of a new contract
114. representing the cash holding
115. now owned by Lender Two
116. after they've been repaid.
117. At the end, you can see
118. that there are no active IOU contracts
119. on the Ledger anymore
120. as our Borrower has fulfilled their obligations to pay.
121. Lender One has an active cash contract
122. representing the $30 that was repaid to them
123. by the Borrower;
124. while, Lender Two has two active cash contracts
125. representing the 30 and $40
126. repaid to them by the borrower.
127. This is a simple example of a Smart Contract in practise
128. and I hope you can see they're not too scary
129. and can be quite useful as
130. we automate complex workflows
131. amongst multiple different parties.

5.4.1 Use Case: Blockchain for Health Insurance (Alan Cheung from Hong Kong Applied Science and Technology Research Institute (Astri))

1. Hello everyone, I'm Alan Cheung.
2. I'm from the Hong Kong Applied Science Technology
3. Research Institute,
4. the largest government-owned
5. R&D centre in Hong Kong.
6. Today I'm honored to share with you
7. our experiences in blockchain.
8. ASTRI has been involved in research and development
9. of blockchain technology for the past few years.
10. We have developed innovative technology
11. and commercial solutions for blockchain systems.
12. Examples include, blockchain scalability
13. and performance enhancement,
14. cross system smart contracts,
15. and also hardware accelerator for mining
16. and processing transactions, etc.
17. In the past we have also collaborated
18. with the Hong Kong Monetary Authority
19. to publish technology white papers
20. and completed a few blockchain projects,
21. related to financial industries.
22. One of the mandates of ASTRI
23. is to commercialise our technology,
24. especially in Hong Kong.
25. In the past few years,
26. we have been developing blockchain applications
27. with our clients from different industry areas.
28. I would like to illustrate one use case today,
29. the medical insurance claim blockchain,
30. and talk about how to make use of the technology
31. and help our clients to solve their problem.
32. Traditionally, a patient submits a medical invoice
33. which is issued by the clinic
34. to the insurance company after a visit.
35. The submission can be done in one of the two ways,
36. one of them is patients can send hard copies
37. of the invoice to the insurance company.
38. Some insurance company also accept patient
39. to scan copies of the invoice
40. and submit through web services or apps.
41. The insurance company processes the claim
42. and reimburses the patients if approved.
43. Usually the clinic and doctors
44. are not involved in the claim process.

45. So what are the problems and challenges?
46. A lot of paperwork is involved
47. in handling received hard copies
48. or even soft copies of the invoices.
49. There's also a lot of human processing
50. which is expensive and error prone.
51. The claim process is susceptible
52. to insurance fraud such as double claim.
53. In the double claim,
54. a patient sends soft copies of the same invoice
55. to multiple insurance companies
56. to get more reimbursements than he should.
57. Since the insurance companies process
58. the received claims independently,
59. it is difficult for them
60. to detect such a double claim fraud.
61. So why does the customer want to use blockchain?
62. Because it allows insurance companies
63. to share in this trusted platform
64. in processing claims on blockchain.
65. It allows them to see if an
66. invoice has already been claimed
67. through other insurance companies,
68. and therefore blockchain helps
69. to prevent double claim fraud.
70. It would also reduce paperwork.
71. Clinics can save information
72. of the invoices in blockchain
73. and the invoice information can be seen
74. by respective insurance companies
75. who the provided patient has granted permission.
76. It also streamlines the claim operation.
77. Blockchain smart contract controls the process
78. of filing and processing medical claims
79. and the system can release invoice information
80. to insurance companies
81. as soon as the patient grants
82. the permission to the company.
83. Blockchain systems can also
84. update the patients with the status
85. of his claim, approval or rejection status
86. as soon as the insurance company has issued them.
87. So the scope of the system is as follows,
88. the system connects all three user groups,
89. including the medical service providers,
90. such as doctors and clinics, patients,
91. and insurance companies.

92. And how it works?
93. After providing the medical service to the patient,
94. the clinic will submit the invoice's information
95. to the blockchain.
96. The patient will file the claim
97. to the respective insurance company
98. through blockchain as well.
99. The patient then grants permission to the company
100. to view the clinic invoice.
101. The target insurance company will examine
102. the patient claim information
103. and the clinic invoice information in the system.
104. It will also examine the records
105. to see if the patient has already filed a claim
106. to another insurance company
107. to avoid double claim.
108. After the insurance company has decided to accept
109. or reject the claim,
110. it will store its decision to blockchain,
111. and the decision will also be
112. seen by the patient as well.
113. So what are the technical
114. and business challenges?
115. Nowadays, some clinics
116. are still operating without computers,
117. not to mention some advanced clinic software,
118. and also the connection
119. to legacy payment system,
120. may not be as straightforward as we think.
121. It also takes time to understand
122. the data privacy protection requirements
123. and also the business logic
124. in order to develop a workable
125. system for this industry.
126. So what have we learned?
127. It takes time for users to
128. adopt to new technologies,
129. therefore, working with a client
130. that already has a group of clinics
131. and also willing to try blockchain in mind
132. would be very beneficial.
133. Also, interoperability between
134. blockchain and legacy systems
135. is an important part of the
136. widespread use of blockchain
137. in corporate settings.

5.4.2 Use Case: Blockchain & PropTech (Alan Cheung from Hong Kong Applied Science and Technology Research Institute (Astri))

1. We are going to illustrate another interesting use case
2. in the so-called proptech industry:
3. the property sales blockchain.
4. The sales of new residential flats or properties
5. is a process that involves not only the purchaser
6. and property developer,
7. but also the solicitor who processes the legal matters
8. and purchase payments.
9. Also, it may include the mortgage lenders
10. who process the purchaser's application for mortgage.
11. Traditionally, the purchaser signs a so-called PASP,
12. preliminary agreement for sale and purchase,
13. with the property developer
14. when they want to buy a flat.
15. The agreement specifies the property information,
16. purchaser's personal information, the price,
17. the payment terms, and also available rebates.
18. The developer sends piles of legal papers and
19. agreements to the solicitor through courier services.
20. After receiving the materials,
21. the solicitor handles and
22. processes the paper documents
23. and keeps track of the purchaser's required payments
24. prior to signing the official contract.
25. Within a fixed number of days,
26. the purchaser must fully pay the preliminary payments
27. and sign the formal agreement,
28. otherwise the sale may be deemed as forfeited.
29. The solicitor sends the process
30. status to the real estate developer
31. periodically about the purchaser payment status
32. and also the purchaser's signing
33. of the formal agreements.
34. The purchaser may apply for mortgage
35. applications independently
36. to different banks.
37. Individual banks advise the purchaser
38. that the application has been approved,
39. and the purchaser will inform the solicitor
40. of his mortgage application status as well.
41. The solicitor will contact the bank
42. to release the fund to pay the developer.
43. The solicitor and the developer will complete the sales
44. once all the payments and legal

45. matters have been settled.
46. So what are the problems and challenges?
47. There are a lot of paper forms that
48. need to be sent to the solicitor.
49. Also, the developer gets updated on
50. the purchaser's payment status
51. only periodically, but not in real time.
52. Sometimes, it needs human processing of data
53. before synchronisation can be done.
54. The solicitor needs to spend quite a lot of effort
55. in processing mortgage matter as well.
56. The buyer, on the other hand,
57. often spends a lot of time
58. checking with the developer, the solicitor,
59. about the status.
60. He may also try to shop for the best mortgage offer
61. from different banks,
62. either by making a lot of trips to different banks
63. or making a lot of phone calls.
64. Not to mention, he also needs to bring
65. a lot of personal and purchase documents
66. to all of the banks.
67. To summarize: it is very tedious for all of the parties,
68. and this process has been lasting for a long time.
69. So why do the customers want to use this blockchain?
70. First of all, the developer wants to remove the delay
71. caused by physical transfer of paper forms
72. to the solicitor through courier service.
73. Also, the sale and purchase information can
74. be safely stored in blockchain and read by the solicitor.
75. Standard copies of legal documents
76. can be stored in a system as well,
77. by the means of the fingerprints
78. of these legal documents
79. would be stored in the blockchain
80. to certify the authenticity of these documents.
81. The developer wants to gain up-to-the-minute status
82. of the purchase information.
83. Instead of receiving a status from the solicitor
84. in a less-frequent basis,
85. the developer now will be able to see the status
86. once the solicitor has added the status to the system.
87. A blockchain system enables purchasers, solicitors,
88. and mortgage lenders to work closely
89. in processing the application and release of mortgage
90. in a trusted platform.
91. The solicitor can also see

all the outstanding mortgage
applications of the purchaser.
Once the mortgage lender approves the application,
it will be immediately seen by the solicitor,
who can then proceed to arrange for a fund release.
So the scope of the blockchain system includes
all of the parties, including the property developer,
solicitor, mortgage lender, purchasers,
are all connected in blockchain.
Information updated to the blockchain
is immediately seen by relevant parties.
Some of the relevant documents,
whether digital or scanned,
may be stored in the accompanied off-chain storage,
while their digital fingerprints
can be stored in blockchain for proof.
The system enforces strict access control
such that each purchase is
assigned to one solicitor only.
Only this solicitor can access
the information of the purchase.
Also, no mortgage lender can access
the information of the sales
until the purchaser has granted them permission.
What are the technical and business challenges
in this system?
Since the system involves different user groups
who have different business practices
and operation preferences,
it takes significant amounts of effort
to design such a system
to meet the needs of each user group.
The storage of certain personal information
has to conform to legal requirements,
that those information has to be erased
after a certain length of time.
So what have we learned in this system?
We need to work the overall system
to comply with the legal requirements,
such as data privacy protection
and personal information storage.
Smart contracts need to be
designed in a very flexible way,
such that it could adapt to the future changes
in the purchase flow and different
access control scenarios.
We hope in the future that all parties will enjoy

to use the new blockchain system
and have much better user experiences.

5.4.3 What Are the Benefits of Blockchain in Banking? (Johnny Cheung, General Counsel, B.C. Technology Group)

Hello, my name is Johnny Cheung
and I'm the Group General Counsel
of BC Technology Group.
Today I'll be sharing with you
various applications of blockchain.
Blockchain technology is still in its infancy
but it has already disrupted different industries
and sectors.
This technology revolution can be compared
with the evolution of the use of the internet,
which has altered the way we live
in the past couple of decades.
There are actually numerous examples
or applications of use of blockchain.
To name a few in finance, healthcare, media,
government, and real estate.
But let's spend more time to discuss
the use of it in the banking and finance sector
as well as the healthcare sectors,
to illustrate our points.
In the banking sector, blockchain holds the potential
to transform the industry
by reducing potential costs
and labour savings.
Talking specifically about the
banking and finance sectors,
hundreds and thousands of funds are being
regularly transferred from one part of the world
to another every day.
Traditionally, it operates on the basis
of highly dependent manual networks.
As a result, the banking and finance sector
is prone to errors and frauds that could lead
to a crippled money-managed system.
Blockchain provides a very high level
of safety and security when
it comes to exchanging data,
information, and money.
It allows users to take advantage
of the transparent network infrastructure,
along with the low operation costs

42. with the help of decentralization.
43. A centralized database for
44. operations and money management
45. traditionally is vulnerable and highly prone
46. to cyber attacks as the single point of failure.
47. And such a system can be exploited by hackers.
48. For example, in early 2017, there was a series
49. of attacks on card processing in Eastern Europe.
50. The criminals penetrated the banks' infrastructure,
51. obtained access to the card processing systems,
52. and increased overdraft limits.
53. They also disabled anti-fraud systems
54. that would notify the bank of fraudulent transactions.
55. In each case, the average theft amount
56. was about five million and in total
57. about 100 million was lost in these series of attacks.
58. In another case,
59. while banks in Nepal were closed for holidays,
60. criminals used SWIFT to withdraw money.
61. The bank were able to track transactions
62. and recover significant portion
63. of the stolen money funds only due to timely response.
64. With the use of the blockchain platform
65. is secure, non corruptible technology
66. can be operated on a distributed database system.
67. Since the blockchain is distributed,
68. there is no chance of a single point of failure.
69. Each transaction is store in the form of a block,
70. either with a cryptographic mechanism
71. which is extremely difficult to corrupt.
72. With a good and secure blockchain platform
73. we can easily eliminate cyber crimes
74. in attacks of banking and financial sectors
75. taking place now.

5.4.4 How Can Blockchain Technology Benefit the Healthcare Industry? (Johnny Cheung, General Counsel, B.C. Technology Group)

1. In addition to the banking
2. and finance sector, blockchain technology has also
3. impacted the healthcare sector.
4. Critical patients' data
5. and information remains scattered across
6. different departments and systems.
7. Due to this inefficiency, crucial data is sometimes
8. not accessible in times of need.
9. The current healthcare ecosystem cannot

10. be considered complete,
11. as multiple players in the system
12. do not have a system in place
13. for smooth process management.
14. Many healthcare facilities today are still dependent
15. on outdated system for keeping records for patients.
16. These systems hold the functionality
17. of keeping local records of the patients' data.
18. This can sometimes make it
19. difficult for doctors to diagnose,
20. which is time consuming for the doctor
21. and hard for the patient as well.
22. Another time consuming
23. and tedious process that results in high costs
24. in the industry is health information exchange.
25. Since patients do not have any
26. control over their health data,
27. the chances of identity thefts, financial data crimes,
28. and spamming are increasing every day.
29. Because of the problem we just discuss,
30. the healthcare system is crying out for a system
31. that is smooth, transparent, economically efficient,
32. and easily operable.
33. Blockchain has the power to bring out
34. a great breakthrough in the ecosystem
35. and it can easily bring changes
36. in the healthcare management of the patients.
37. With the aid of this technology,
38. patients will now be responsible
39. for handling their own records,
40. therefore, getting the overall control of their own data.
41. Blockchain holds the ability to successfully improve
42. patient care quality, while maintaining
43. the funds at a very reasonable rate.
44. For example, in the 1970s, a system called
45. electronic health records, or EHRs,
46. were implemented for billing purposes
47. and have not been updated since that time.
48. While being an important tool for doctors
49. to track patients' medical records, past prescriptions,
50. and test results, the lack of standard
51. health record parameters
52. and security threats can make the EHR management
53. a difficult process.
54. Blockchain platforms can be used to consolidate
55. patients' information from various sources.
56. These newly integrated patient

57. records can be visualised
58. through easy-to-follow, informative,
59. and standardised portals or apps
60. for better treatment, improved traceability and security,
61. and higher quality of health outcomes.
62. MIT has developed a decentralised record network,
63. called MedRec, for managing
64. electronic medical records.
65. Google's DeepMind initiative is collaborating
66. with the UK's National Health Service to build
67. a private platform for secure tracking
68. of patients' health data.
69. All the previous challenges
70. and hindrance that occur in layers
71. of authentication can now be eliminated.
72. The vision for blockchain to disrupt
73. the healthcare sector is there.
74. Just imagine a healthcare
75. system where all the information
76. is easily accessible by doctors,
77. patients, and pharmacists, at any time.
78. Blockchain allows the creation
79. and sharing of a single common database
80. of health information at a much lower cost.
81. This database would be easily
82. accessible by all the parties
83. involved in the ecosystem,
84. no matter which electronic medical system they use.
85. It offers higher security
86. and transparency while allowing
87. doctors to find more time
88. to spend on patient care and their treatment.
89. It also allows better sharing of statistics
90. of research on medical data.
91. That would have the effect to facilitate clinical trials
92. and treatments, therapies, and improve our health.
93. Indeed, this is so powerful
94. and have great positive impact
95. to the whole healthcare system.
96. End of transcript. Skip to the start.

5.4.5 Institutional Investment Opportunities in the Digital Asset Space (Henri Arslanian from PwC)

1. Hi there.
2. Very excited to be here.
3. As most of you know, my name is Henri Arslanian.

4. My passion and my focus in life
5. is the future of the financial service industry.
6. I'm very excited to share with you all
7. over the next couple minutes some of the trends
8. that we're seeing with institutional investors
9. and digital assets.
10. I want you to take home
11. six big trends that we're seeing.
12. One is the entry of institutional players, stable coins,
13. large technology firms coming into digital assets,
14. central banks, crypto funds, security tokens,
15. and I'll finish with blockchain,
16. so a lot of space to cover.
17. Hang on tight, and let's kick it off.
18. First of all is the entry of institutional players.
19. Make no mistake, a couple of years ago,
20. Bitcoin and blockchain
21. developments were happening a lot
22. by real, two guys and a T-shirt in San Francisco
23. or in a basement in Moscow
24. or in a café in Sydney.
25. But now, over the last one or two years,
26. we're seeing a lot of the developments take place
27. in the broader digital asset space
28. being driven by institutional players.
29. That has been very, very interesting
30. because many of you have been saying
31. that as banks and large financial institutions
32. are getting into the digital assets space,
33. it could be a game changer.
34. But that's not easy.
35. Trust me, for someone who's worked with banks
36. and with fintech for many years, it's very difficult
37. to plug in fintech inside a bank.
38. Imagine trying to plug in crypto or digital assets.
39. It's even more complicated.
40. There's a lot of issue, like a lack of expertise,
41. the reputational risk, the uncertainty.
42. I always tell everybody that if you want to get involved,
43. if you want to go on Friday
44. afternoon and enjoy your weekend
45. and have a good time, you should not get involved
46. in digital assets because
47. the space moves so fast,
48. it's 24/7, and crypto markets never, never sleep.
49. But really, we've been seeing
50. globally three big approaches

51. when it comes to traditional financial institutions
52. approaching digital assets.
53. The first one has been firms
54. purely investing in companies.
55. Firms like Goldman Sachs, for example,
56. have invested in firms like Circle or BitGo,
57. investing as a way to learn about the ecosystem.
58. Another type of company have been those
59. who have been trying to do partnership
60. with digital assets companies.
61. One example is Nomura
62. that has done a partnership with Ledger.
63. Again, Nomura has traditional clients.
64. Ledger is a French digital crypto custody solution,
65. a security company.
66. Actually they partnered towards a service to market.
67. So that's second category.
68. Third category are companies
69. that are setting up new entities
70. purely focused on digital assets.
71. A great example of that is Fidelity in the U.S.
72. where they set up a complete new entity
73. to entirely deal with digital assets.
74. And it's been very interesting what's been happening
75. right now when it comes to traditional
76. financial institutions, but watch this space
77. it's increasingly likely that we're going to see
78. even more financial institutions enter the space.
79. Second big development are stable coins.
80. I mean think about this: if today I send you a Bitcoin,
81. first you'll be very happy, but the problem
82. is you actually don't know what the value
83. is gonna be one day, one week, one month from now.
84. It's not a very stable store of value so far.
85. This is why we've been seeing a lot of interest
86. increasingly on stable coins.
87. What is a stable coin?
88. It's a crypto asset that is backed one to one
89. by U.S. dollar or other fiat currencies.
90. This ensures that if I send you a stable coin equivalent
91. of $1 you're going to have $1 one week, one month,
92. or one year from now as well.
93. This has been very interesting for institutional players
94. because for let's say who people are trading crypto
95. at the institutional level,
96. whenever the markets are choppy
97. or it becomes very volatile instead of selling

98. all their Bitcoin and moving
99. to cash, they can simply
100. go and keep it into a stable
101. coins which they remain
102. in the digital assets space,
103. but they can have something
104. that is stable until they want to come back
105. and actually trade actively.
106. But also, the other big development
107. has been financial institutions
108. looking at using stable coins.
109. For example think about all the different
110. inter-bank transfers that we have.
111. From transfers the bank is doing with the central bank,
112. or actually all the different transactions
113. that happen between banks on daily basis.
114. This is actually quite not only cumbersome,
115. but they also operate in the
116. same way for many decades.
117. And this is the interesting thing is now
118. enough financial institutions are looking how they can
119. potentially leverage this technology themselves.
120. For example JP Morgan recently
121. announced the JPM coin,
122. which says basically that if a customer
123. gives them a dollar they can issue them one JPM coin.
124. And then between clients of JP Morgan
125. they can transfer those JPM coins,
126. basically completely bypassing this existing
127. traditional rails that exist that are cumbersome
128. and a bit slow and costly in many regards.
129. But the other big development,
130. the third big development,
131. you need to know about is what's happening
132. with large technology firms.
133. Because while a lot of startups
134. in the last couple months have been pushing innovation,
135. have been bringing forward new innovation
136. to the broader blockchain space,
137. the big game changer could be large technology firms.
138. Companies that people trust, people are familiar with,
139. and also companies that people generally believe
140. that will be here for next couple years.
141. Think about a firm like Amazon, that has over dozens
142. of millions of Amazon Prime members in the U.S.
143. You know if you buy all your
144. daily necessities on Amazon,

wouldn't you maybe use them
as a digital currency as well?
What if Amazon gave you Amazon coin
that gets you for example
discount on your next purchase?
But also if everybody trusted that
Amazon will be here in couple
years, maybe we can use an
Amazon coin on a daily basis.
Well, the best example of this
happened literally recently
last week in early June when
Facebook announced the creation
of something called Libra, their
own global crypto currency.
Which is very very interesting.
Just think about it.
Facebook has over two billion users.
Think about how many times
you use your WhatsApp,
your Facebook messenger,
or your Facebook app on a daily basis.
You trust Facebook.
I mean often you put pictures of your kids
or your parties on Facebook or on Instagram.
Now imagine now if Facebook brings together
a lot of these organisations and there's a currency,
in their case Libra, which is backed by a basket
of different global assets held at tier one custodians.
And if people can send each
other these Facebook Libra coins
think about your domestic helper in Hong Kong
that wants to send money back to the Philippines
who can do it now instantaneously at no cost
and the person receiving it will get it on its app,
on a WhatsApp instantaneously.
Or think about the Bangladeshi worker working in Dubai
who wants to send money
back home who now can do it
without avoiding those intermediaries who previously
have been in business a long time and can do it directly.
And this opens a whole new
world of opportunities as well.
From micro payments to actually getting other
more peer to peer emergent solutions
very very exciting development to watch out.
This is very relevant to central bank crypto currencies.

192. Because the big question is,
193. while for a lot of central banks
194. what is happening with Bitcoin is still quite marginal.
195. There may be a hundred million
196. or so Bitcoin trading a day,
197. but that's peanuts compared
198. to the volume of transactions
199. happening in existing financial systems today.
200. But actually, also a lot of startups
201. do not challenge the authority of a central bank today.
202. But what if, with Facebook for
203. example, and their new coin?
204. Technically with two billion users
205. Facebook could be the biggest
206. central bank in the world.
207. And this is why it is gonna be very interesting
208. how central banks are going to
209. react over the coming months,
210. so watch out for some potential developments
211. from that perspective.
212. For example one big debate is whether a central bank
213. is going to issue its own central bank digital currency.
214. Well, there's been some tries on that.
215. Many countries from the
216. Marshall Islands to others
217. have been trying to promote this idea.
218. Why don't they issue their own digital currency?
219. But actually there's a bit of reticence as well
220. from many of the central banks as well.
221. For example the European Central Bank recently said
222. that while that could be a good idea, it may not be ideal
223. because the risk for population is that people
224. take their money away from banks and actually come
225. and buy digital currencies issued by the central bank.
226. And this may create financial stability,
227. a rise of interest rates, and potentially
228. some issues with the traditional banks.
229. This is definitely an area to watch,
230. especially with some of the recent developments
231. happening with large technology firms.
232. Another big development is the rise of crypto funds.
233. This is really interesting when you look at how
234. institutional players are entering the crypto space.
235. If you go back in time to the 1990s, in the early 1990s
236. venture capital firms, hedge funds, private equity firms
237. were really becoming more mainstream.
238. What has happened though, at a time,

239. a lot of the institutional investors they start investing
240. in these VC funds, hedge funds, P funds,
241. and they started to learn about the sector.
242. And then over the next 10, 15, 20 years
243. they started bringing these skills in house.
244. For example today, some of the big pension funds they
245. operate like their own private equity funds internally.
246. And the same may happen with crypto hedge funds.
247. Today the industry is really at its early days
248. when it comes to crypto hedge funds, but really expect
249. that a lot of the first moves that institutional investors
250. may do in digital assets may happen via crypto funds
251. where they could put some money, watch,
252. learn how the industry operates,
253. and gradually, gradually, gradually they can actually
254. learn it and be more active in the space.
255. Another big development going
256. on has been security tokens
257. and this is very exciting.
258. Because imagine today maybe if I live in a big building
259. I can not afford to buy the big building myself.
260. In many cities these big buildings
261. cost couple hundred millions or a couple billion dollars.
262. But now, imagine, if I could buy
263. a little tranche of this building.
264. I could buy lets say for a thousand dollars
265. or even a hundred dollars of this big building.
266. What that enables me is that
267. I'm able to get some liquidity,
268. because today a big building
269. only couple people can buy it.
270. But if I'm able to separate into little, little pieces
271. that enables actually more people
272. to actually be able to afford this asset.
273. But what's even more interesting now we're able
274. with security tokens to completely streamline
275. what we call corporate actions.
276. Today the way we pay a dividend for example
277. it happens every quarter or
278. every six months or every year,
279. and it's a very cumbersome process.
280. And also it's hard to even
281. know who your shareholders are.
282. It's still a challenge for many public large companies.
283. With security tokens I can know at all times
284. who my shareholders are, and if I want to make
285. a corporate action, a dividend payment for example,

286. I can make it instantaneously in a matter of seconds.
287. So this is an area where a lot of institutional players
288. are also taking a look at.
289. A lot of them are exploring the space
290. and thinking and wondering can this generally change
291. financial services as we know today?
292. We're still at the very early days and there's still a lot
293. of work to be done but we've seen in the recent months
294. people actually tokenize buildings in New York,
295. some projects in Latin America, so really a lot
296. of interesting things coming ahead in this space as well.

5.5.1 Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 1) (Brian Tang from Asia Capital Markets Institute (ACMI))

1. When Facebook announced its Libra initiative
2. in June 18, 2019, it reflected a dramatic new stage
3. in the evolution of the use of blockchain
4. and distributed ledger, or DLT, its governance,
5. and potential regulation.
6. My name is Brian Tang.
7. I'm the founder and managing director of ACMI,
8. which fosters capital markets professionalism,
9. including with respect to online capital marketplaces.
10. I'm also the founding executive director
11. of LITE Lab@HKU, that promotes
12. law, innovation, technology,
13. and entrepreneurship at Hong Kong University's
14. Faculty of Law in conjunction
15. with the Department of Computer Science.
16. To better understand Libra, one would benefit
17. from a greater appreciation of three influences
18. that appear significant to its creation
19. and design, namely Tencent's WeChat, Bitcoin,
20. and Hedera's Hashgraph.
21. Most of the Silicon Valley internet companies that arose
22. in the aftermath of the dot-com
23. boom were primarily driven
24. by advertising or eyeballs business models.
25. With venture capitalist funding often forcing focus
26. on rapid growth over short-term revenue or profit,
27. many of these business models that were built around
28. personal data being mined, used,
29. and sold have led to the privacy issues witnessed today.
30. In China, unlike the West, credit
31. and debit card penetration remains relatively low,
32. and pioneering internet companies often incorporated

33. transactions, even small ones,
34. into their business models
35. that led them to become fintechs much earlier.
36. For example, online payment
37. and escrow system, Alipay, was launched
38. by e-commerce platform Alibaba in 2004
39. and started with providing prepaid payment services
40. by Alibaba's consumer-to-consumer,
41. or C2C, platform, Taobao,
42. and business-to-consumer, or B2C, platform, Tmall,
43. and then, to more than 460,000 online
44. and local Chinese businesses.
45. In 2013, Alipay overtook PayPal,
46. then owned by C2C platform,
47. eBay, as the world's largest mobile payment platform.
48. To incentivize customers
49. and suppliers to keep or add more renminbi
50. into its mobile ecosystem,
51. Alipay offered to pay them
52. interest through Yuebao, or leftover treasures,
53. that same year, which within a few years,
54. became the world's largest money market fund.
55. In January 2011, messaging service, WeChat, or Weixin,
56. was launched by Hong Kong-listed
57. and Shenzhen-based company, Tencent.
58. In what Alibaba's founder Jack Ma called
59. a Pearl Harbour attack, WeChat introduced
60. its Red Packets, or Hongbao feature,
61. during the 2014 CCTV Spring Festival Gala,
62. the most watched television event show in the country,
63. with a promotion where users were incentivized
64. to shake their phones to receive prizes
65. of digitally transmitted traditional gift money.
66. Wall Street Journal reported that 16 million transfers
67. were made in 24 hours
68. and within a month, WeChat Pay's user base
69. expanded from 30 million to 100 million.
70. WeChat was also prescient in popularising the use
71. of phone-scannable QR codes that allowed offline
72. transactions to be made without
73. physical wallets or cash.
74. According to Statistica, WeChat has 1.112 billion
75. monthly active users in Q1 2019.
76. This user base is more than
77. the population of Europe and Russia combined
78. and is only behind Facebook, WhatsApp,
79. Facebook Messenger, and Google's YouTube.

80. According to CAICT WeChat
81. Economic and Impact Report 2018,
82. WeChat drove 333.9 billion renminbi
83. or approximately 48.5 billion
84. U.S. dollars in home services,
85. entertainment, and travel services in 2017.
86. TechNode reports that WeChat
87. can now handle transactions
88. in 13 different currencies in 25 countries and regions.
89. And in 2018, 688 million people
90. used WeChat Red Packet during Chinese New Year Eve.
91. Unlike at banks, all of these transfers
92. are free to customers, other
93. than a 0.1% withdrawal fee
94. when funds are transferred from
95. the customer's WeChat wallet
96. to his or her bank account.
97. At Berkshire Hathaway's celebrated
98. annual shareholders meeting in 2018,
99. Charlie Munger specifically called out WeChat
100. as a competitor to watch for against
101. credit card company giants
102. American Express, Visa, and Mastercard.
103.

5.5.2 Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 2) (Brian Tang from Asia Capital Markets Institute (ACMI))

1. In 2009, the famous white paper on bitcoin,
2. A Peer-to-Peer Electronic Cash System
3. by Satoshi Nakamoto, was released.
4. To solve the double-spending problem
5. to create a digital currency, the white paper proposed
6. an open-source blockchain of distributed ledgers
7. where transactions are verified
8. by proof of work or mining by peer-to-peer nodes.
9. The Ethereum protocol that went live in 2015
10. added smart contract elements to the blockchain
11. that enabled fundraising for
12. projects through token sales
13. and the launch of initial coin offerings, or ICOs.
14. In addition to anti-money laundering, or AML,
15. and counter-terrorist financing, or CFT, concerns
16. about illicit transfer of funds,
17. ICOs have resulted in fraud, misselling and
18. and unauthorised offerings of securities
19. and currency outflows.

20. Globally, regulators worldwide
21. have had a mixed reception
22. regarding cryptocurrencies, with some countries,
23. such as China and India, effectively banning them.
24. However, global convergence of views
25. of some regulatory aspects are emerging.
26. In June 2019, the Financial Action Task Force, or FATF,
27. adopted and released an interpretative note
28. and guidance for the regulation
29. of virtual asset service providers, or VASPs,
30. for AML and CFT purposes, and these apply worldwide.
31. In the meantime, many public blockchain
32. and DLT use cases are being piloted,
33. ranging from sovereign self-identity, or SSI frameworks,
34. to the creation of non-fungible tokens, or NFTs,
35. as well as security tokens to represent
36. different traditional illiquid asset classes,
37. such as real estate and art.
38. However, to date, adoption of blockchain-distributed
39. applications, or dapps, has not fully lived up
40. to expectations, with the most used dapps
41. relating to gambling.
42. At the same time, non-public or permissioned
43. blockchain projects for enterprises,
44. which do not involve cryptocurrencies,
45. such as from R3's Corda
46. and IBM's Hyperledger consortiums,
47. are being piloted across multiple jurisdictions.
48. These include at least five
49. trade finance blockchain consortia.
50. To address concerns regarding trading volatility
51. and the lack of asset-backing of cryptocurrencies,
52. stable coins have recently
53. been developed that are backed
54. by a collateral of certain main currencies,
55. such as the U.S. dollar.
56. However, the adequacy of
57. and custody arrangements regarding
58. many of the stable coins have been the subject
59. to inquiry and in some cases, litigation.
60. In October 2018, the Financial Stability Board, or FSB,
61. concluded, "Based on the available information,
62. crypto-assets do not pose a material risk
63. to global financial stability at this time.
64. However, vigilant monitoring is needed
65. in light of the speed of market developments."

5.5.3 Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 3) (Brian Tang from Asia Capital Markets Institute (ACMI))

1. As previously mentioned, many other DLTs
2. have also emerged, with an
3. increasing number seeking
4. to provide enterprise-grade solutions.
5. Announced in March 2018,
6. Hedera's Hashgraph is a proof-of-stake directed
7. acrylic graph, or DAG, based on gossip protocol
8. and a virtual voting mechanism,
9. with impressive claims
10. that is able to be thousands of times faster
11. than existing blockchain protocols
12. and has high security based
13. on Asynchronous Byzantine Fault Tolerance or ABFT.
14. Users who own HBAR tokens
15. but do not run a node proxystake their account
16. to a node and share the HBAR transaction fees.
17. In community testing on the mainnet at the time
18. of this recording, Hashgraph's high speed
19. and low cost promises fascinating
20. peer-to-peer micropayment
21. and Internet of Things applications.
22. To prevent the contentious forking
23. that has occurred for open-source protocols
24. like Bitcoin and Ethereum that divided the community
25. of developers and token holders,
26. the Hashgraph consensus
27. algorithm is patented by Swirlds,
28. which is controlled by
29. Hedera's founders Leemon Baird
30. and Mance Harmon, and then licenced to Hedera.
31. Most relevantly, to enable
32. and demonstrate a world-class enterprise ecosystem,
33. Hedera created a global governing council
34. and announced on February 2019
35. that its initial members comprised
36. telecommunications companies
37. Deutsche Telekon and Swisscom,
38. financial institution Nomura Holdings,
39. media company Magazine Luiza, law firm DLA Piper,
40. together with Swirlds as initial network nodes.
41. Hedera is seeking 39 global blue chip organisations
42. in 18 sectors to form its council.

5.5.4 Facebook's Libra – Development in Blockchain, DLT and Cryptocurrency (Part 4) (Brian Tang from Asia Capital Markets Institute (ACMI))

1. In February 2014, Facebook acquired WhatsApp
2. for 19.3 billion U.S. dollars
3. in its largest acquisition to date,
4. and in the same year, it hired David Marcus,
5. PayPal's president who oversaw
6. that company's acquisition
7. of digital wallet, Venmo, parent company, Braintree,
8. to run Messenger.
9. In 2017, Marcus was also appointed
10. to the board of directors
11. of cryptocurrency exchange, Coinbase,
12. and resigned after five months
13. to become Facebook's new blockchain research head.
14. In 1Q 2019, Facebook reported an incredible
15. 2.38 billion monthly active users,
16. with the largest user base being in India.
17. In the same period,
18. WhatsApp has 500 million daily active users worldwide.
19. In March 2019, its Mandarin-speaking founder,
20. Mark Zuckerberg, posted a blog
21. on a privacy-focused vision
22. for social networking, describing Facebook's new focus
23. on private messaging for interaction,
24. including businesses, payment, commerce,
25. and ultimately, a platform for many other
26. kinds of private services.
27. Although not specifically named,
28. this has been widely interpreted as his intent
29. for Facebook to emulate the
30. approach and success of WeChat.
31. With the announcement of Libra in June,
32. The Economist declared that,
33. "Facebook wants to create
34. "a global currency" with the stated aim
35. of financial inclusion to provide free transactions
36. to serve the 1.7 billion unbanked across world.
37. Libra will be an opensource
38. and at least initially, permissioned stablecoin
39. backed by a basket of different
40. currencies that will enable
41. free payment transactions, where the transaction costs
42. will be covered by the up to 100 members
43. of the Libra Foundation,
44. of which Facebook is but one member.

45. And each of whom will invest 10 million U.S. dollars
46. in Libra Investment Tokens, or LITs,
47. and benefit from the interest earned
48. from the fiat funds in the Libra Reserve.
49. The founding council members of the Libra Foundation
50. consist of 28 world-class leaders
51. from across different industries, including,
52. in payments, Mastercard, PayPal, and Visa,
53. in technology and marketplaces, eBay,
54. Facebook, Lyft, Spotify, and Uber,
55. in telecommunications, Vodafone,
56. in blockchain, Coinbase,
57. in venture capital, Andreessen Horowitz,
58. and finally, for nonprofits
59. and multilateral organisations who do not need to pay
60. the $10 million, Kiva and Women's World Banking.
61. Facebook plans to create its own digital wallet, Calibra,
62. that will need to comply with AML requirements
63. for users on-ramping and off-ramping fiat currency.
64. While an incredibly innovative initiative
65. that has brought together many major global players,
66. Libra's sheer potential size
67. and ambition has already caused some concerns.
68. Legislators in the U.S.
69. and EU have called for greater scrutiny
70. before Libra proceeds further.
71. Bank of England Governor
72. and former FSB chairman, Mark Carney, has said
73. "We will look at it very closely
74. and in coordinated fashion at the level of the G7,
75. the BIS, the FSB and the IMF.
76. So open mind, but not open door."
77. Given Facebook's 2.38 billion monthly active users,
78. plus the user base of the other
79. significant council members,
80. this attitude is not surprising.
81. If it were a country,
82. Facebook alone would be the
83. largest country in the world.
84. And its proposed introduction of a global currency,
85. not only makes it a potential systemic risk,
86. but also purports to allow mainly for-profit
87. private sector multinational companies to impact
88. monetary policy, especially over smaller nation states.
89. It also should be recalled that cryptocurrency is banned
90. in India, which is Facebook's largest user base.
91. Many proponents aim for blockchain

92. and DLT to be the new decentralised Web 3.0 payment
93. and identity layer in the internet technology stack.
94. Accordingly, public blockchain proponents,
95. such as Consensys' Joe Lubin, have called Libra,
96. "a centralised wolf in a decentralised sheep's clothing."
97. Currently, global banking
98. and finance relies on the financial messaging network
99. created by the cooperative
100. Society for Worldwide Interbank
101. Financial Telecommunications
102. or SWIFT, in 1974, which enables its 11,000-member
103. institutions in 200 countries to quickly, accurately,
104. and securely send money transfer messages
105. to confirm transactions
106. and handles U.S. $5 trillion worth of transactions a day.
107. Yet, settlement and payment
108. of those transactions can take days.
109. With DLT technologies for enterprises,
110. like Ripple, seeking to compete in this space,
111. and JP Morgan's recently
112. announced USD-backed stablecoin,
113. JPM Coin, to enable instant settlement
114. and payment between the bank's
115. global institutional clients,
116. SWIFT introduced Global Payments
117. Innovation, or GPI, in 2017
118. to speed up the processing
119. time of cross-border payments.
120. The week after Facebook's Libra announcement,
121. SWIFT announced that pending the success
122. of its current proof of concept trial with R3,
123. it would soon be enabling payments on DLT-based
124. trade platforms on SWIFT gpi,
125. thereby automatically passing them
126. onto the banking system.
127. It'll be fascinating to see how the Libra saga,
128. together with the overall interaction
129. and tension between distributed
130. and centralised approaches to global finance
131. and payments, unfolds.

Module 5 Reference Reading

References and Suggestions for Further Reading in Module 5

- Nicola Atzei, Massimo Bartoletti, Tiziana Cimoli, "A survey of attacks on Ethereum smart contracts", 2016.

- Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, "A survey on the security of blockchain systems", 2017.
- Hai Wang, Yong Wang, Zigang Cao, Zhen Li, Gang Xiong, "An overview of blockchain security analysis", 2018.

Module 6 The "Evil Sides" of Blockchain and Legal Regulations for Blockchain

Welcome to Module 6

Dear Learners,

Welcome to Module 6 – The "Evil" Sides of Blockchain and Legal Regulations for Blockchain. In the last Module, we looked at security and privacy concerns of a blockchain platform and learnt about some of the risks with blockchain solutions, as well as, the benefits and opportunities in using blockchain for different industrial applications.

In Module 6, we are happy to introduce five guest speakers to you, among others, Bowie Lau (Founder & MD of MaGESpire) will talk about the "dark" side of blockchain. Then, Malcolm Wright (Chief Compliance Officer at Diginex) will speak about criminal use of payment blockchains. Furthermore, we will hear from Charles d'Haussy (Director of Strategic Initiatives at ConsenSys) who will share his views on whether blockchains need regulation

Professor Douglas Arner of HKU Law Faculty (Course director of Introduction to FinTech) will discuss the global practice and the role of financial regulations for blockchain. And we will also learn about global digital assets regulatory trends from Henri Arslanian (FinTech & Crypto Leader for Asia, PwC).

This is an exciting week. May you enjoy the great contents from our guest speakers.

HKU Blockchain and FinTech Course Team

Module 6 Learning Objectives

After completing Module 6, learners should be able to:

- **understand there is an "evil" (negative) side of blockchain, in particular, relating to cryptocurrency;**
- **understand why bitcoins (or cryptocurrency) provide a means for criminals to collect ransom for the ransomware attacks, and doing money laundering;**
- **understand the risks of investing on cryptocurrency and the security concerns of using cryptocurrency exchanges;**
- **understand the necessity of regulation for cryptocurrency and the exchanges.**

6.1.1 The Evil Sides of Blockchains Part 1 Ransomware

1. Welcome to the last module of our blockchain course.
2. In the first four modules,
3. we talked about the basics
4. about blockchain technologies,
5. and also the properties of blockchain,
6. what are the good points and the positive sides
7. of blockchain technologies.
8. From the last module, we started
9. to look at the negative sides
10. of blockchain technology.
11. For example, we talked about the scalability
12. of blockchain technology.
13. And also, we talked about the security
14. and privacy issues saying
15. that it may not be 100% secure if you try
16. to use blockchain technologies.
17. In this module, we want to take this further.
18. We want to focus on the evil sides of blockchain.
19. In particular, we want to talk about cryptocurrency,
20. for example, Bitcoin.
21. In this module, we want to talk about four topics.
22. The first one is the ransomware, the second one
23. is money laundering, and the third one is because a lot
24. of people are trying to use cryptocurrency
25. for investment, so we want to investigate
26. whether investing in cryptocurrency is risky or not.
27. And finally, we also want to talk about the issues
28. in using the cryptocurrency exchanges.
29. The first topic we want to talk about is ransomware.
30. So, what is ransomware?
31. Ransomware in fact is a one type of the malware.
32. Malware, refers to malicious software.
33. It's a generic term referring
34. to those harmful programs
35. that hackers usually use to cause damages
36. to people's computers,
37. servers, or computer networks.
38. Let me give you some examples.
39. Virus is a type of malware, worms,
40. Trojans, even spyware,
41. they are classified as one type of malware.
42. Then what is ransomware?
43. Ransomware is kind of like a kidnapping software.
44. Of course, they're there not trying to kidnap your files,
45. but instead what they do is they try to encrypt your files

46. in your hard disc so that you can't access
47. to it without a private key,
48. and then they will try to ask for a payment
49. which is the ransom before
50. giving you the encryption key.
51. Probably, everybody heard about the Wannacry
52. which is a very famous ransomware that encrypt a lot
53. of people's files and ask for the ransoms.
54. The point is that the attack
55. is not only for private enterprise or private companies,
56. they also aim at hospitals,
57. public transportation department,
58. and also include the police department.
59. Now, if you think about it, in a hospital,
60. if the ransomware can attack
61. into all the patients' records
62. and encrypt all the patients records,
63. and the hospital has no way to decrypt the records,
64. then how can they treat the patients?
65. So what they have to do is to pay the payments.
66. Similar to the kidnapping, for the criminals,
67. the most difficult part for a kidnapping case
68. is to get the ransom because it's easily tracked
69. by the police.
70. Now, then we will see how
71. Bitcoin can help these criminals.
72. Let me remind you one
73. of the advantage of Bitcoin is anonymous.
74. It means that it's very difficult to trace
75. where the Bitcoin goes and who is the owner
76. of the account the Bitcoin that received the payment.
77. For ransomware, what they usually do is they will ask
78. for payment in terms of Bitcoin.
79. Now, let me give you a concrete example.
80. This is an email received by a victim
81. that has been attacked by a ransomware.
82. Now, if you look at it carefully,
83. then you can see that they ask you to do the following
84. in order to get the private key to decrypt the files,
85. otherwise you're not able to access all the files
86. that they encrypted.
87. Step one, you can send us .7 Bitcoin
88. for each affected PC,
89. or if you want to retrieve all the private keys
90. for all the affected PCs, they give you a discount.
91. They ask you for three Bitcoins.
92. Of course, they also will give you the accounts

93. of the Bitcoins where you can deposit the Bitcoins.
94. Once you deposit the Bitcoins,
95. you send them an email,
96. they check it, and if it's okay,
97. then they will release you a software
98. that contain the encryption key
99. so that you can decrypt all your files
100. and get back the access to all the files.
101. So this is how they try to obtain the ransom
102. from the victims.
103. In fact, they're organised crime.
104. They even have customer service to talk to you online
105. if you say that "Oh, I don't know how to buy the Bitcoin…
106. I don't know how to deposit the Bitcoin
107. into your accounts."
108. They have customer service that
109. you can talk to them online
110. to teach you how to buy the Bitcoins
111. and how to do deposit in order to get the decryption key.
112. To conclude, you can see
113. the criminal actually take advantage
114. of Bitcoin's anonymous property to avoid being traced
115. to get the ransom.
116. It's very, very difficult if you still remember
117. what we talked about to trace who is the owner
118. of the Bitcoin account.
119. This is the first example of how the bad people,
120. the criminals make use of Bitcoin to do evil things.
121. Let me give you another example.
122. Have you heard about dark web?
123. In fact, dark web is just like what you have seen
124. in the movie.
125. This is the part of the internet
126. that will not be indexed
127. by common search engines like Google.
128. If you use Google to search it,
129. you might not be able to get access
130. into these dark web websites.
131. What they do is they use solely the special software
132. in order to access to this dark web,
133. and based on this software,
134. your identity will be kept anonymous
135. and you are not traceable.
136. You can imagine that this becomes a hotbed
137. for criminal activities.
138. Of course, I want to emphasise that not all parts
139. of the dark web are related to criminal activities,

but a significant part of it is actually related
to criminal activities.
In fact, if you can get into the dark web
using the software,
you can actually buy the credit card numbers
people stole already, some credential
to the bank account so that you can get the money
from the bank accounts, and you can buy drugs,
guns, counterfeit money, or even you can hire hackers
to hack some of the websites,
and also you can buy the hacking tools
from these dark web websites.
You know how they get the money back?
They use Bitcoin.
Bitcoin become the defacto currency of the dark web.
Also, because of the non-traceable
property of the Bitcoin,
it's very difficult for the law enforcement
to keep track where the money goes
and how they can get the money.

6.1.2 The Evil Sides of Blockchains Part 2: Money Laundering

1. The second example is money laundering.
2. What is money laundering?
3. To make it very simple, it's basically the art
4. of making money that comes from source A,
5. usually source A is illegal, look like it comes
6. from source B, and source B usually is a legal channel.
7. Now, if you look at money laundering
8. in a high level manner, usually it involves three steps.
9. The first step is called placement.
10. Placement is trying to insert the dirty money
11. into a legal system.
12. For example, you can deposit the money
13. that you gained from the transactions into a bank,
14. and the second part is
15. so once the dirty money gets into the legal system,
16. the second part is, we want
17. to confuse law enforcement using multiple transactions
18. to make it very difficult to trace where the money goes.
19. For example, you can have multiple transactions
20. across different countries.
21. For example, you can use the
22. money to buy Forex in overseas,
23. buy stocks, etc.
24. After this layering, because

25. of the cross-country manner,
26. the law enforcement, it's very difficult
27. to trace where the money goes
28. and where the money comes from.
29. Finally, the last step is called integration.
30. In this integration step, the money
31. that's being laundered will go back to the owner.
32. Now, if you look at these three steps,
33. you can see that placement
34. is one of the most dangerous steps.
35. Without cryptocurrency, people usually do it this way:
36. They will try to deposit the money in small amounts
37. using many multiple accounts,
38. or they buy fake accounts from real people
39. and they try to insert the dirty money
40. into the legal system bit by bit.
41. Layering is also another important step
42. because for layering if you do not do a good job,
43. the law enforcement may be able to trace
44. where the money goes and
45. where the money comes from.
46. Let's try to take a look at how Bitcoin
47. can help this kind of criminal activities.
48. If you think about it carefully, if you try to go
49. to your bank account to open a new account,
50. what do you need to do?
51. You need to provide proof
52. of your identities, and also
53. you need to give the proof
54. of your address.
55. In fact, this is known as the KYC requirement.
56. KYC refers to know your customer requirement.
57. This is a common requirement for all countries
58. if you try to go to a bank to open an account,
59. it's the requirement from the law.
60. On the other hand, we know that for Bitcoin
61. or many other cryptocurrencies,
62. there's no universal regulation governing people on
63. how to open an account.
64. In fact, I do not need to give you my identity
65. nor my address in order to open an account
66. to trade Bitcoins.
67. Now, the consequence or the implication is very simple.
68. Then you can see the dirty money can easily get
69. into the cryptocurrency market
70. without people knowing your identity.
71. In other words, you can easily

open a cryptocurrency account
in one of the exchanges in the world
and try to use your real money
to buy the cryptocurrency
without showing who you are
and where you live, then your money will be converted
into the cryptocurrency, the crypto coins easily.
The second part,
I hope you still remember the transactions
on cryptocurrencies also can be anonymous
or password anonymous
and can cross country boundaries as well.
You can see that this actually facilitates
the layering step in money laundering
because it's very difficult to trace where the money goes
if it's cross-country boundaries.
Let me give you an example.
This is a very well-known marketplace
in the dark web called Silk Road.
They open a marketplace of people to buy illegal things
in the dark web.
If you look at the flow of the payment system
in Silk Road, so what the buyer will do
is they try to exchange real currency for Bitcoin.
In fact, they can easily find the exchanger
for them to do it.
What they do is, after they get the Bitcoin,
they can transfer the Bitcoin to the Silk Road accounts
and the buyer can easily make purchases,
and the Bitcoin will be held in the Silk Road account
until the order is finalised.
And of course, Silk Road tries to make profit
by taking the commission on the transactions.
And after the vendor is paid,
the vendor can move the Bitcoin
from the Silk Road account to their own account,
and through another exchange,
they can actually convert the Bitcoin
into real currency as well.
Now then in this way, you can see that it's not easy
to trace where the money comes from
and where the money goes because many
of the Bitcoin exchanges,
they may not require the buyers or the sellers
to identify themselves or provide the proof
of their address.
Of course, the real situation for money laundering

119. is even more complicated.
120. I just want to show you some simple examples saying
121. that it's very easy to use Bitcoin to do money laundering.
122. Now, I hope you understand
123. the second point of it now.

6.1.3 The Evil Sides of Blockchains Part 3: Cyber Currencies

1. Now let us proceed to the third example.
2. Right now, people try to buy cryptocurrencies,
3. for example Bitcoin, as an investment, and of course,
4. a lot of people make a lot of money,
5. and maybe some of the people
6. lose a lot of money as well.
7. If you look at the chart I provided here,
8. you can see that the price of Bitcoin
9. as well as other cryptocurrencies
10. actually fluctuated a lot
11. in the recent years.
12. Let me give you some example.
13. The highest price that Bitcoin
14. achieved was in December 2017.
15. It's about US $20,000.
16. Compare to Bitcoin at the beginning at 2009,
17. it's only US $.009 per Bitcoin, and then you can see
18. that it's already increased a lot.
19. If you look at right now, 2019, the current price
20. is about 8,000.
21. You can see that actually the Bitcoin price
22. fluctuates a lot.
23. Now let me give you some more figures
24. then you can see that actually the price
25. of the cryptocurrency fluctuates only in a few hours
26. or even in a few days.
27. From its peak in December 2017, the Bitcoin drops
28. by already 65% in February, 2018.
29. You can see that it's only like two months.
30. The price can drop by 65%.
31. Another example, in the same day, May 30th of 2019,
32. the price of Bitcoin drops from 9,000 to 8,000.
33. It's actually about an 11% drop on some exchange
34. only within a few hours.
35. So you can see that we should try
36. to answer a more important question,
37. can we treat cryptocurrency as an investment tool?
38. Is it risky?
39. I want to tell you the truth.

40. In fact, it's very risky.
41. First of all, we do not have,
42. or only have limited regulation governing people
43. how to trade cryptocurrencies.
44. In other words, the investment is not protected
45. by the law unlike those at stock markets.
46. And it's also very unclear what are the factors
47. that will affect the price of the cryptocurrency,
48. even worse than buying stocks.
49. Of course buying stocks we also do not know completely
50. what factors will affect the price of the stock,
51. but for cryptocurrency it's even more difficult
52. to make an estimation for when the price will go up
53. and when the price will go down.
54. Because we do not have a lot
55. of regulations governing
56. how we trade the cryptocurrencies,
57. so in fact it might be possible
58. that the price can be manipulated by some big players.
59. Although we do not have an affirmative answer,
60. but some evidence already show
61. that the so-called whales,
62. the big whales means that they're having a lot
63. of cryptocurrency on hand, who can try to buy
64. and sell a large amount of Bitcoin in a very short time,
65. will actually affect the price immediately.
66. Let me give you one example.
67. On April 3rd, 2019
68. at about midnight, the price
69. of Bitcoin is around 4,190,
70. but then just one hour later,
71. the price actually increase to 4,900.
72. If you think about it, it's about already 20% increase
73. in an hour, and people look at the history again,
74. and then people suspect that
75. there had been a single order
76. of about 20,000 Bitcoins that
77. triggered the price change.
78. If you look at the 2017 Bitcoin price bubble,
79. you remember the highest
80. price was at December 2017, right?
81. You know why people think that
82. the price went up so quickly?
83. They believe that it was created by the rumour saying
84. that the mainstream finance people
85. were about to invest in cryptocurrencies.
86. So that's why everybody tried to get the Bitcoin

87. so up goes the price.
88. Now, to conclude, you take your own risk
89. if you try to invest in cryptocurrencies.
90. The main reason is, right now, not all the countries
91. have very complete regulations
92. that can govern the trading of cryptocurrencies.
93. In other words, the regulation is not in order yet.

6.1.4 The Evil Sides of Blockchains Part 4 Cyber Security Exchanges

1. Now finally, I want to talk
2. about cryptocurrency exchanges.
3. Now, a cryptocurrency exchange
4. is just like a stock exchange.
5. Now, whenever you want
6. to trade cryptocurrency,
7. you need to go into one of
8. these cryptocurrency exchanges.
9. Unfortunately, again, there
10. are no common regulations
11. for these exchanges in the world.
12. But on the other hand,
13. there are more than 500
14. cryptocurrency exchanges
15. in the world right now.
16. And if you look at the figures,
17. the combined daily trade
18. volume of the top 10 exchanges
19. is more than U.S. $6.5 billion,
20. so it's a lot of transactions,
21. a lot of money involved in
22. these cryptocurrency exchanges.
23. My question is, which exchange is more reliable?
24. Or are they actually reliable?
25. I'll give you a very recent incidence
26. so that you know what happened to these exchanges.
27. There's an exchange in Canada
28. which is Canada's largest cryptocurrency exchange.
29. Recently, the CEO, the
30. founder died in December, 2018
31. at a very young age, 30 only.
32. But the problem is, the company claimed that
33. only the CEO has the encryption key
34. to a lot of wallets that contained the cryptocurrencies.
35. Because he died and his laptop was encrypted
36. and everything was encrypted,
37. so they're not able to access this kind of money.

38. The amount of money is about U.S. $190 million.
39. All the investors' money was
40. not able to be accessed from then on.
41. If you look at the incidences,
42. you'll find something interesting or strange.
43. So about U.S. $190 million
44. that cannot be accessed
45. because the founder died in December, 2018,
46. and he is the only one who has the access key.
47. So Ernst and Young was appointed by the court
48. to take a look at this case.
49. And according to a report, what they found out is,
50. it's so strange that even after the founder die,
51. the company, they claim that they made a mistake
52. transferring another 103 bitcoins to a wallet
53. that only the founder has the access key to open it.
54. In other words, the transfer
55. was done in February, 2019,
56. but actually the CEO died in 2018, December
57. and only he has the access key.
58. These 103 bitcoins were gone and
59. nobody can access it anymore.
60. This case actually aroused a lot of interest
61. in most of the investigators in the world.
62. And some of the investigators actually found that
63. based on the public data,
64. they claimed that in fact in those wallets,
65. the money was gone already,
66. was empty eight months before the CEO died.
67. There's a rumor whether the CEO actually died
68. or he faked his death and stole all the money.
69. From this simple incident,
70. you can see that it's not completely safe
71. to put your money into this kind of exchange,
72. and because of the lack of regulations,
73. we are not sure which exchange
74. is more reliable than the other.

6.2 The "Dark" Side of Blockchain (Bowie Lau from MaGESPire)

1. Hello, I'm Bowie Lau, founder of MaGESpire
2. which is a Blockchain Venture Development
3. and Education group in Hong Kong.
4. For all of the good things
5. blockchain can bring to the world
6. including helping organisations
7. drive technological transformation,

8. disruption, and growth,
9. there is also a dark side of blockchain.
10. In this short video, I'm going to take you over
11. the evil sides of blockchain.
12. Greed is the hardest thing to shake out
13. in the blockchain crypto space.
14. Some of you may remember,
15. Gordon Gekko in the movie
16. "Wall Street" immortalised the words "Greed is good."
17. But, we all know how that ends
18. if it is unrestrained greed.
19. It devastated the dot-com boom in the late 90s
20. and it has the potential to do the same again.
21. As of December 2018, over a billion dollars
22. have been stolen through ICO scams.
23. And as the number of start-ups
24. looking for ICO funding increased,
25. so did the number of scams and vanishing acts.
26. In a recent report,
27. The Wall Street Journal indicated that
28. out of 1,450 start-ups analysed,
29. more than 270 were literally what we could call trash,
30. or tokens created uniquely to rip off investors.
31. There are also manipulative
32. and predatory market practises
33. that seem prevalent in cryptocurrency exchanges.
34. Most notorious is the "Pump and Dump" schemes
35. that give false temporary impression
36. of great growth story,
37. and immense liquidity in certain cryptocurrencies
38. and often these are accompanied by fake news.
39. Beware, if something sounds too good to be true,
40. then it probably is too good to be true.
41. Hacking is another problem the crypto world faces
42. in security, both physical and cyber of exchanges,
43. platforms and smart contracts.
44. 2018 turned out to be a record-breaking year
45. for crypto exchange hacks,
46. but there have been other kind of hacks as well
47. like the DAO hack in July 2016,
48. that split the Ethereum blockchain world into two,
49. and more recently KICKICO who experienced a breach
50. where tokens estimated to be worth around
51. eight million US dollars were stolen
52. due to a compromised private key of a main wallet.
53. Sources of such hacks fall into two categories,
54. internal or external.

Same as bank robbery,
this can be executed as an internal job
or by an external actor.
Sometimes bad coding habits
and unforeseen logic cases
can be harmful when deploying immutable
or unchangeable smart contracts.
Sometimes, intentional back doors
with not so honourable intent that go undetected
can also compromise smart contracts.
This is not to say smart contracts are to blame,
but the practitioners programming these
smart contracts just like any other software
development need to be mindful of vulnerabilities and
edge cases, and should have adequate
contingency plans.
Just follow the famous quote
from Andreas Antonopoulos,
a Bitcoin and blockchain expert,
“Your keys, your bitcoin.
Not your keys, not your bitcoin.”
On the other hand, more recently came up the case
Quadriga exchange.
The unexpected death of Gerald Cotten,
the CEO of popular Canadian exchange QuadrigaCX,
had left more than $140 million
of users’ funds inaccessible,
since he was the only one in the company
able to access the money.
According to Gerald’s wife,
Gerald accidentally died in his trip in India
back in December 2018.
They claim that Cotten held
sole responsibility for handling the funds and coins,
and the remaining team members have had no luck
accessing the exchange’s cold wallets
ever since he passed away.
This is an extreme example of key man risk.
Since 2009, estimates suggest criminals have used
the hyper-connected cryptocurrency ecosystem
to launder well over $2.5 billion USD
worth of dirty Bitcoin.
Bitcoin is easily laundered
through unregulated exchanges.
Unregulated cryptocurrency exchanges,
those without proper Know Your Customer
and anti-money-laundering procedures

can also be used to clean Bitcoin, even without using
a cryptocurrency mixing service beforehand.
Just like a Virtual Private Network, VPN
scrambles your IP address
which by the way,
is an unique address identifying
your computer and location.
IP stands for Internet Protocol
and makes it difficult to track your browsing activity.
Mixing is a concept in cryptocurrencies
where a single transaction is merged,
and mixed with multiple other such transactions,
either real or fake with an intention
of making it difficult to trace,
or establish a clear audit trail of transactions
from source to destination.
One of the significant risks associated
with digital currencies is the ability
of criminals and terrorists,
to use these new technologies
for their own benefit.
While information on each transaction is recorded
on the blockchain,
this data is not directly linked to names,
physical addresses or other identifying information.
This makes ownership of digital currencies anonymous
to a certain degree,
and complicates efforts by law enforcement agencies
to identify individual transactions
and link them to users.
Terrorists using cryptocurrency to evade detection
and to fundraise.
Terrorists, like other criminals use cryptocurrency
because it provides the same form of anonymity
in the financial setting,
as encryption does for communication systems.
By fundraising and making financial transactions
online with Bitcoin,
terrorists and other criminals can avoid interference
from financial regulators,
or other third-parties who might otherwise
take steps to prevent their operations.
Studies show that Bitcoin featured
in high-profile investigations
involving payments between criminals,
and has been used in more
than 40% of these transactions

149. in the European Union.
150. People are using darknet
151. to conduct lots of illegal activities.
152. Darknet is basically a clunky version of the Internet
153. which uses special programme to hide your IP address.
154. The programme is called the Onion Router,
155. and it sends your IP address through multiple places
156. around the world juch like the rings of an onion layers.
157. The infamous pioneer of the dark web's large-scale
158. illegal trade platform was Ross Ulbricht.
159. He was the person behind Silk Road,
160. the biggest online marketplace that started out
161. as an experiment,
162. and turned into the go-to resource
163. for buying and selling drugs and fake documents,
164. as well as money laundering,
165. running things with Bitcoin as the main currency.
166. The dealers were then sending the drugs
167. via post or left them in PO boxes.
168. Other options may also include providing buyers
169. with detailed instructions
170. of where they can pick up their sensitive purchase.
171. And closer to home, family lawyers are worried that
172. couples who are getting divorced
173. might end up buying cryptocurrency
174. to hide their money from the court.
175. Similarly, bankrupt companies could stash their funds
176. in cryptocurrency so they
177. don't have to pay out creditors.
178. Therefore, when the company is liquidated,
179. they won't be able to sell anything
180. because there won't be anything to be found.
181. Take ownership of your own destiny
182. in an increasingly cyber world
183. with complex technologies like
184. Blockchain, AI on the rise.
185. Equip yourself with basic cybersecurity knowledge
186. and question anything that sounds too good to be true.
187. If you are dealing in large value digital assets
188. or cryptocurrencies,
189. please follow clean wallet habits
190. like cold wallets and multi-signature wallets
191. with trusted parties.
192. And more importantly don't be evil.
193. That's all from me.
194. Thanks for watching.

6.3 Criminal Use of Payment Blockchains (Malcolm Wright from Diginex)

1. Today we will look at criminal use
2. of payment blockchains,
3. and what is being done to mitigate
4. cryptocurrency financial crime.
5. It is useful to start with some headline figures.
6. According to a 2018 Europol report,
7. three to four billion US dollars is laundered
8. through the cryptocurrency ecosystem.
9. That number is still small compared
10. to the one to two trillion US dollar estimate
11. for the traditional financial sector,
12. but is recognised to be growing
13. and the international community has moved
14. rapidly to take mitigating actions.
15. In October 2018, the global anti money laundering,
16. or AML, standards-setting body, the FATF,
17. issued a statement that it would seek
18. to issue regulatory standards
19. for firms that provide cryptocurrency services.
20. It was noted that this work was considered urgent,
21. and so by June 2019 the FATF
22. had issued recommendations on cryptocurrency
23. that countries should adopt.
24. Countries follow FATF recommendations
25. or risk facing actions that would be detrimental
26. to their economic growth.
27. The FATF introduced five activities
28. that countries should regulate for.
29. First, exchange between virtual assets
30. and fiat currencies.
31. Second, the exchange between one or more forms
32. of virtual assets.
33. Third, transfer of virtual assets
34. from one party to another.
35. Fourth, safekeeping and/or administration
36. of virtual assets.
37. Lastly, participation in
38. and provision of financial services
39. related to an issuer's offer
40. and/or the sale of a virtual asset.
41. The FATF then produced a guide for countries
42. and virtual asset service providers,
43. or VASPs for short.
44. VASPs are considered any firm offering
45. the previously mentioned activities.

46. This means that if you are considering building
47. or operating a VASP,
48. you will likely require a licence in every country
49. where you will have customers.
50. From the regulatory perspective,
51. VASPs will now operate in the same way
52. as financial institutions,
53. with the same compliance controls.
54. This means that if you sign up with a VASP
55. you will need to conduct full Know Your Customer,
56. or KYC, procedures such as a selfie identification
57. and providing proof of address,
58. or confirming that the source of funds
59. that are added to your account.
60. Further requirements also mean
61. that if you are sending funds
62. to another person's cryptocurrency address
63. you will need to provide details
64. on who that person is.
65. Moreover, if you are receiving cryptocurrency
66. from a third party
67. then you will need to give accurate details
68. on yourself to the sender.
69. All this means that the perceived anonymity
70. of cryptocurrency is drastically reduced,
71. and with it the opportunity
72. to use the ecosystem for financial crime.
73. Cryptocurrency also benefits from another measure
74. to prevent financial crime that is not available
75. to the traditional financial sector.
76. Blockchain analytics enables
77. transparency and traceability
78. on the history of coins and wallets.
79. Thus, VASPs can check whether an address
80. or a wallet has a suspicious past,
81. such as having received funds
82. from an online drugs marketplace on the dark web.
83. Such tools can also check the history to see
84. if there has been any attempt
85. to hide the tracks of the coin's history,
86. which again could be a sign of suspicion.
87. One area that is causing concern
88. amongst law enforcement and regulators alike
89. is the use of cryptocurrencies
90. with privacy-preserving features.
91. Otherwise known as privacy coins.
92. These are coins where the history,

93. and even the details of the transaction itself,
94. can be hidden.
95. It is worth noting here
96. that not all privacy coins are created equal,
97. and that a desire to use a privacy coin
98. does not make one a criminal.
99. But Europol did report in 2018
100. that there had been a shift by criminals
101. towards using one particular privacy coin
102. called Monero.
103. So what are the major financial crimes
104. we see in cryptocurrency right now?
105. The most widely spoken about
106. is cryptoexchange hacking.
107. In 2018, Ciphertrace reported
108. that approximately one billion US dollars
109. had been stolen from cryptocurrency exchanges.
110. After the theft, hackers will use various techniques
111. to split the coins up into smaller amounts
112. and spread over multiple accounts before cashing out.
113. This is known as money muling.
114. Dark web sales are then also still highly prevalent
115. and also widely reported.
116. The dark web, an area of the Internet
117. that runs anonymously and cannot be indexed
118. by search engines like Google,
119. offers goods and services for sale
120. including drugs, guns,
121. stolen debit and credit cards,
122. and Crime as a Service
123. where criminals provide their services
124. to assist with cashing out
125. illegally obtained cryptocurrency
126. back into real money.
127. The instant, cross-border nature of cryptocurrency
128. also makes it an attractive means
129. of funds transfer for criminals.
130. In the traditional world, cash would have been used
131. and transported across borders
132. to pay a drug cartel for the manufacturer
133. where distribution was in a different country.
134. With cryptocurrency, it can be instant and online.
135. But as regulators tighten their approach towards VASPs,
136. and in particular crypto exchanges,
137. it will be much harder
138. to conduct this activity through an exchange.
139. Finally, money mules form a key strategic part

of any money launderer's toolkit.
Cryptocurrency is no different.
Money mules are individuals offered a commission
in return for their assistance.
They may be unaware of the illegality
of what they are doing.
For example, in the UK, schoolchildren
have been recruited by organised crime gangs
to use their bank accounts.
The criminal sends 500 pounds
to the money mule's account,
the money mule might keep 10%
and then send the remainder
on to an account the criminal instructs.
This has been transferred into the cryptocurrency world,
making easier where exchanges have low
or no KYC to open an account
or they have KYC-free transaction thresholds.
With all this said, cryptocurrency has legitimate uses
and it is not just for criminals.
In fact, according to the blockchain analytics firm,
Elliptic, the percentage of criminally derived funds
is decreasing against the overall traded volume.
With the advent of regulation for VASPs
we would expect that number to drop further
as the legitimate cryptocurrency exchanges
understand their customers
and their trading partners better.
Ultimately, cryptocurrency's future
will look more like banking
than a fringe activity of its early days
and with it, a greater safety and protection
will be assured, not only for customers,
but also for the victims
of financial and social crimes.

6.4 The Role of Financial Regulations for Blockchain (Professor Douglas Arner, Faculty of Law at the University of Hong Kong)

1. Hello, my name is Douglas Arner.
2. I'm a professor at the University of Hong Kong.
3. Today, we're going to talk a little bit
4. around the role of financial regulation
5. when we talk about blockchain and FinTech.
6. And I know for some of you
7. working in technology areas,
8. that this whole idea of regulation seems strange

that basically there are many in the technology area
who feel that when we're thinking
about new technologies, innovation,
that we should take a hands-off approach,
leave them alone for a while.
And that is very often the case though, even in tech,
there are rising new questions about that
when we look at Facebook, or Amazon,
or even Alibaba and Tencent
in China about what can happen
when you leave an industry unregulated
perhaps for too long.
But we're talking about finance.
And finance is perhaps the most regulated
industry in the world.
And that means that if we are talking about blockchain
in finance, we're talking about FinTech and blockchain.
By nature, we are talking about involvement
in a regulated industry.
And so we have to think about
how does regulation apply to blockchain
when you take it into the financial services context.
And I think when we think about regulation,
and particularly financial regulation,
there are really a series of traditional approaches
when faced with a financial innovation.
And many uses of blockchain in finance
are very much innovations.
The first of those is really to do nothing.
In other words, we say, right, we're not going to step in,
we're not going to do anything,
we're going to see how this develops.
And then later on, maybe we'll decide
whether we need to do anything or not.
And this is an approach
that a number of countries have taken.
But as the role of blockchain,
particularly some of its leading applications,
like cryptocurrencies and Initial Coin Offerings
have grown larger and larger,
an increasing number of regulators around the world,
at the global level, at the regional level,
at the domestic level, at the industry level,
are taking a look at what sort of approaches.
At the other end of the spectrum is prohibition.
And there are often questions about
with a new financial innovation, is this a good idea?

Is it something that we should allow at all?
And actually, we have a range of countries
which have prohibited certain aspects
of the use of blockchain in financial services.
Certainly, China is probably
the most high profile example,
with prohibitions on ICOs,
prohibitions around a range
of cryptocurrency exchanges, cryptocurrency uses.
But at the same time, a very positive approach
to blockchain more generally,
but a very prohibitive approach to certain aspects,
particularly certain financial transactions.
Between those spectrums,
most jurisdictions are working with a range of options.
Some are beginning to use the existing legal
and regulatory frameworks to try to take it in.
Others are putting in place new legislation,
places like Switzerland
or New York State in the United States
have put in place new legislation
to deal with specific aspects of blockchain
in financial services such as payments,
or in the context of Switzerland, more generally.
So what are we saying?
I think, generally speaking, we can say
that the trend in regulation of blockchain
in the area of finance is
towards a functional approach.
What do I mean by that?
I mean, that instead of
having a system, a law,
a framework that deals
with blockchain generally,
we look at its uses.
What is the technology being used for?
And what sorts of regulatory concerns
does the technology raise in that specific context?
And so, we're seeing a range
of different functional ways
that blockchain is being used
in the financial services sector.
Some of these are largely outside of regulated areas,
things where you are using blockchain
for certain forms of contracts.
This is likely to be outside
of the regulatory framework,

103. but it is likely to be under the general legal framework
104. for contracts.
105. Others are around private ordering.
106. How do you set up industry standards,
107. for instance, from the international
108. standards organization,
109. so that you know whether or not
110. this is a proper blockchain,
111. a good blockchain, a
112. functional blockchain.
113. Likewise, we're seeing an increasing use in most places
114. of general consumer protection legislation,
115. the idea that consumers should be able to rely
116. on what is stated in an online context.
117. But where we're seeing most of the activity
118. is in the highest profile case uses,
119. the first, cryptocurrencies,
120. the second in the context of financing,
121. and the third in the context of exchanges.
122. If we look at currency and payments,
123. every country in the world has a framework
124. for regulating payments.
125. Payments are something
126. that have a very important role in society
127. and hence, a clear regulatory need.
128. And as a result, in most jurisdictions,
129. if you are building a blockchain
130. based payment framework,
131. you are going to be dealing
132. with the same payment regulatory framework
133. as a non-blockchain based payment framework
134. and certainly that is the trend that we're seeing.
135. Lots of questions about certain blockchain systems,
136. creating new currencies, new forms of money.
137. And in every country in the world,
138. there is legislation about what constitutes a currency.
139. And countries have taken very different approaches.
140. Japan is taking an open approach
141. to allowing it to be a currency,
142. China is taking a very restrictive approach.
143. The end result is that the decision
144. of whether or not something is legally a currency or not
145. depends upon the individual countries
146. and the users within those.
147. Where we're seeing perhaps the most activity
148. is around financing.
149. This started out in the context of ICOs,

150. it is expanded in the context
151. of things like Security Token Offerings, STOs,
152. and now Exchange Token Offerings.
153. So we see different frameworks
154. depending on the type of financing
155. that is being undertaken.
156. Is it actually a donation?
157. If it's actually a donation to support research,
158. then very limited regulation.
159. Is it a pure utility function?
160. Is it something where you have a token
161. which can be used for a licence or some product
162. that will be produced in future?
163. That is what we would think of as utility
164. or reward-based systems.
165. And these generally fall into areas
166. of consumer protection and contract law.
167. Or is it a financial instrument?
168. And if it's a financial instrument,
169. the trend increasingly in major jurisdictions
170. from the United States, to the UK, to Hong Kong,
171. to Singapore, is to treat that
172. under the traditional financial regulatory framework.
173. And what we're seeing in the market
174. is an increasing decision by participants raising funds
175. to support blockchain-based activities
176. to structure those accordingly,
177. but still large amounts of money being raised.
178. And finally, the real focus of most global
179. as well as domestic regulators today is on exchanges.
180. Exchanges where digital assets can be bought,
181. sold, listed and traded, why?
182. Because these bring together
183. large amounts of digital assets.
184. They bring together a range of different participants.
185. And they also bring with them risks, the risks of hacking,
186. the risk of fraud, the risk of manipulation,
187. and as a result, we see a very strong trend
188. to bring digital asset exchanges of all forms
189. into a regulated environment.
190. To the extent that digital asset exchanges
191. in many jurisdictions have applied for formal licences
192. to be treated as with other exchanges.
193. At a global level, the G20, the Financial Stability Board,
194. the International Organisation
195. of Securities Commissions,
196. and others are all focused heavily

197. on how to develop appropriate frameworks
198. to regulate digital asset exchanges
199. so that participants and investors can feel safe
200. in the products which they are buying
201. and have the confidence to see the industry grow.

6.5 [Does Blockchain Need Legal Regulations? (Charles d'Haussy)

1. There're a lot of activities for the blockchain industry
2. which do not need regulation.
3. So the blockchain industry is making progress
4. on many topics which are not regulated
5. because they are just simple
6. or they are just technology regulated.
7. The thing is blockchain offers a lot
8. of financial services use cases
9. which people have a very strong appetite for
10. but when you start to deal with money,
11. you come into the world of financial services
12. where there is regulation.
13. Not everyone is allowed to transact the money,
14. to build services on top of the money.
15. So that's where the regulations comes in.
16. The regulations take some time.
17. In some places of the world
18. or in some topics before they give full regulation.
19. Some jurisdictions decide to basically regulate
20. from day one,
21. some of the regulation gives space
22. to technology to go before starting to regulate.
23. So there is mainly different approaches
24. in terms of regulations.
25. We see every month different regulators
26. around the world starting
27. to get their head around the concept of blockchain,
28. the concept of digital assets.
29. So concept of digital currencies
30. and deciding to give licences
31. to different operators to either start
32. to operate an exchange, for example,
33. or start to accept that the identity of people
34. can be distributed or identity of people
35. can be owned by themselves
36. through some kind of blockchain application
37. and digital wallets.
38. So the regulations in some
39. ways sometimes are slowing down

40. the industry a little bit
41. but the regulators are also doing their job.
42. The regulators have a big
43. mandate to protect the investors,
44. to protect the consumers
45. and in a way, sometimes it takes some time
46. to regulate but it's a good thing
47. because at the end of the day,
48. they want to make sure that the best experience
49. or the technology would be available
50. when the technology is ready.
51. I think there are two types of regulation
52. which are around the blockchain technology.
53. The first regulations are about privacy and data privacy.
54. Some jurisdictions are very sensible about data privacy,
55. they are very sensible about encryptions
56. and it sometimes touches the world
57. of blockchain technologies.
58. Another family of regulations
59. which impact the blockchain technology
60. or involve the blockchain technology
61. are the regulations around the financial services,
62. when it comes to money services operations,
63. when it comes to securitization of assets.
64. Nowadays people can tokenize a full building
65. and they can sell a building
66. in different kind
67. of digital shares representing this building, for example.
68. So there are regulations around that
69. and some regulators take the time
70. to make sure that this is done properly,
71. that there are no money laundering activities happening,
72. that the people investing in these kind of products
73. are authorised to invest, understand the product as well.
74. So I think everyone is doing their job here
75. and the technologies are bringing innovations
76. and the regulators are understanding these innovations
77. and trying to basically give a framework around them
78. so these innovations bring good to the users.

6.6. Global Digital Assets Regulatory Trends (Henri Arslanian from PwC)

1. Hi, there.
2. Very excited to be here with all of you today.
3. As many of you know, my name is Henri Arslanian,
4. and really, my passion
5. and my focus in life is the future

of the financial service industry.
And I'm very excited to have the opportunity
to share with you all today
some of the global digit assets regulatory trends
that are taking place in our exciting world today.
But before I start, let me give you a warning.
Whoever tells you they're an
expert when it comes to crypto
or digital assets, you gotta run away.
I can tell you, I spend 24/7 of my time in this space.
I spend my time on digital assets
and the future of finance on weekends, evenings,
and I have absolutely no idea where
the industry will be one month from now
because things are changing so fast.
But at least, today, I want to share with you five trends,
really, very relevant trends that I think could be relevant;
the importance of regulatory clarity on crypto,
best practises we are seeing
when it comes to regulatory trends, U.S. requirements,
some developments we're
seeing with FATF and KYC AML,
and finally, some tax developments as well.
And hopefully, with these, you will be able to make
your own decision on where you believe the industry,
when it comes to digital assets, is heading
when it comes to regulatory trends.
Excited?
Let's kick it off.
First of all, regulatory clarity.
One thing that's very important to understand
is that, compared to two or three years ago,
there is increasing level of regulatory clarity
around the world.
I would personally argue that
even some of the regulators
that I deal with are way more knowledgeable
on digital assets than the average
financial services professional.
But just to give an idea,
my team recently did a study at PWC,
and we found that about 60%
of regulators have released
some type of crypto guidance or regulations
in the last couple of months,
and this represents almost 90% of global GDP.
Another study, recently, by Cambridge University

53. said that something around only 5% of regulators
54. don't have somebody looking at crypto internally.
55. But really, what's been remarkable,
56. if you saw the number
57. of countries that have issued clarity on this topic.
58. For example, many countries in Asia,
59. countries like Thailand, for example,
60. or Hong Kong or Japan, have come up
61. with very interesting regulations
62. when it come to digital asset space.
63. But also, in the Middle East, countries like Bahrain,
64. for example, that have, now, some of the most complete
65. and comprehensive of crypto
66. regulatory fabrics out there.
67. But also, some of the countries
68. would surprise many of you.
69. For example, France is positioning itself
70. as one of the leading centers when it comes to ICOs
71. and the broader digital asset space.
72. With some of the new proposals in France,
73. you'll even be able to file your documents in English,
74. which is a pretty good thing for France.
75. When you look at, globally,
76. some of the trends happening
77. on the regulatory perspective,
78. there are really three big approaches.
79. And I think this is important because
80. as you think about regulatory clarity for digital assets,
81. it's really important to think about how
82. certain countries are addressing it.
83. For example, some countries have taken
84. a very principal-based approach,
85. which is the first category.
86. Countries like Liechtenstein or countries like Gibraltar,
87. for example, when you look at Liechtenstein,
88. the regulations don't even talk about
89. blockchain or crypto or digital assets.
90. They talk about trusted technologies.
91. They try to stay completely agnostic
92. of the underlined technology that underpins
93. whatever is taking place.
94. The second category are countries that are putting
95. digital assets inside their existing framework.
96. A good example of that is actually where I am right now,
97. in Hong Kong, where since last November,
98. the Hong Kong regulators came up with some guidance
99. that says that any licenced fund manager,

there's about 2,500 or so in Hong Kong,
can have up to 10% of their portfolio in crypto
with no additional licencing conditions.
Again, taking digital assets,
putting it inside the existing framework,
and actually try to put some guidelines around.
The third category are countries coming up
with really bespoke regulatory frameworks.
Great example of this is Bermuda,
Malta, Bahamas, and so on
and so forth, were really trying to craft legislation
specifically for the digital asset space.
For example, if we look at the legislation of Malta
or Bermuda, the rules really specify what does a player
in the digital asset space need to do
to be regulated in their jurisdiction.
And this is really interesting what's happening because,
frankly, regulators are increasingly have done their job
and have provided the level of clarity at the industry,
not only needs, but also, deserves.
However, doesn't mean there's regulatory clarity
that everything is easy.
There's still a lot of challenges.
For example, there's number of
challenges for policymakers.
One of them is, while despite coming out
with all the regulatory clarity that you want,
maybe some of the members of your ecosystem
are not as active, for example, banks.
Despite a lot of regulatory clarity globally,
opening a bank account still remains
one of the biggest challenge
for digital assets companies.
But the other challenge is,
for example, is ongoing monitoring.
For example, as a regulator, you could enact
the best regulations you want, but then,
you actually need people to be able to enforce it,
people who understand digital assets.
And that's quite tricky because as you would expect,
a lot of traditional regulators
or those who have been a regulator for a long time
may not be as familiar with digital aspects
as you would expect.
And they often need to hire people externally to come
and join the regulator to provide
in that level of expertise.

147. So very interesting what's
148. happening from that perspective.
149. Second thing that have been going on
150. is really the rise of best practises
151. and this is very exciting because what has happened
152. over the last couple of months,
153. as a lot of the industry players realise
154. that the regulations were not coming fast enough,
155. they decided, by themself, to come together
156. and abide by some series of best practises
157. that can bring the industry forward.
158. A great example for this is KYC
159. and AML; know your customer
160. and anti-money laundering regulations.
161. The beauty of a lot of these
162. crypto exchanges, for example,
163. is that they were able to leverage
164. the latest regtech technology using tools,
165. like biometric face identification,
166. using series of selfies to able
167. to actually do your onboarding.
168. And this is, trust me, is way better than
169. going to your old school bank,
170. showing them a copy of your passport,
171. them making a photo copy, and putting a stamp
172. and saying that it's a certified true copy.
173. And this is why a lot of that, the exchanges,
174. arguably may even have better KYC
175. and AML then some of the traditional banks.
176. But also, what's been really happening,
177. a lot of them are increasingly putting in place
178. internal governance, internal controls as well,
179. to make sure that they have in place the best practises.
180. However, there's still challenges.
181. For example, despite all these best practises
182. being developed, regulatory clarity as well,
183. unfortunately, sometimes there are bad apples.
184. For example, recently, in Canada,
185. there was an exchange called Quadriga
186. where the CEO unfortunately died suddenly in India
187. and now there's about more than $150 million of assets
188. belonging to over 115,000 clients
189. that are completely not accessible anymore.
190. Again, so over the next couple of months
191. and years, there will be more
192. regulations covering exchanges
193. or other industry participants, but at least for now,

194. there's a bit more best practises
195. that are being developed.
196. Another third, big development going on you have
197. to keep an eye on is what's
198. happening in the United States.
199. What's been really interesting is a lot of the big
200. U.S. regulations, in many cases, have a global remit.
201. For example, when it comes to regulation
202. from the Department of Justice
203. or Department of Treasury in the U.S.,
204. they often apply to any U.S. person
205. and what is a U.S. person?
206. It applies to American citizens or permanent residents
207. that are located anywhere in the world,
208. or from a business perspective,
209. it also includes are corporation or company
210. that is also physically located in the United States.
211. So this actually is a pretty good remit
212. when you think about it.
213. For example, most recently in the United States,
214. they very clearly said that
215. any U.S. persons are prohibited
216. from entering into transactions with people
217. who are on these specially designated nationals,
218. what we call SDNs.
219. These are individuals that the U.S. government
220. puts on a list, that is, on a sanctions list,
221. and with whom U.S. persons
222. are not allowed to transact.
223. And this also applies to the crypto space
224. because it's been very clear, for example, OFAC,
225. which is the Office of Foreign Assets Control,
226. made it very, very clear, saying that actually
227. crypto assets are within the remit of OFAC.
228. And it's been very, very interesting to see how
229. these U.S. regulations may
230. apply their companies globally.
231. For example, more recently, two bitcoin addresses
232. were put on this specially designated national list
233. that is put together by the U.S. Treasury.
234. This means that any person who actually transacts
235. with these bitcoin addresses
236. can actually be come into trouble by the U.S. authorities.
237. And there's many cases of enforcements
238. have taken place in the U.S.
239. and also, outside of the U.S.
240. by American government bodies.

241. The big development you need to follow
242. is what's happening with FATF.
243. The FATF is a very interesting government body.
244. It's called a Financial Action Task Force, that
245. actually tries to bring together issue recommendations
246. on a lot of these topics that are popping up.
247. What's been really interesting is, since last February,
248. some guidance was being issued on digital assets
249. and in Orlando, in June of 2019,
250. some guidance was finally
251. approved in an FATF meeting.
252. It says that, basically, any crypto exchange that sends
253. a transaction to another, basically,
254. whenever there's a beneficiary
255. and there's a sender, now, the
256. parties from this transaction
257. need to know who the originator is,
258. basically who's the sender, what's their account number,
259. what's their physical address,
260. what's the beneficiary's name,
261. what's their account number,
262. so on and so forth, basically,
263. putting a lot of the requirements that exist
264. in the traditional banking financial services world
265. into the digital assets world.
266. And that is not very easy
267. because, frankly, in many cases,
268. it's like taking a horse
269. and trying to fit it into a car and to make the engine run.
270. It doesn't work very well, but this is why there's a lot of,
271. actually, industry now talks on how best
272. the digital assets space can satisfy these requirements,
273. but at the same time, do it in a way that
274. leverages the latest technology
275. and frankly, is more appropriate for new developments,
276. like blockchain and digital assets.
277. One other big development, as
278. well, that is worth to watch,
279. is what's happening on a tax and accounting side.
280. While you may thing we're getting there
281. when it comes to regulatory developments,
282. but I can tell you, when it comes to regulations,
283. when it comes to accounting and
284. tax, we're still way behind.
285. And that's also quite important
286. because in order for people
287. to use digital assets, regulators have to make it clear

288. whether any tax are due on some of these transactions,
289. but also, what are the accounting standards
290. and how, actually, from an accounting perspective,
291. you need to look at digital assets.
292. 'Cause if you think about it, double-entry accounting,
293. that was created a couple hundred years ago,
294. was not necessary forecasting things like bitcoin
295. that were going to pop up couple hundred years later.
296. This is why it's going be very interesting to see
297. what's going to happen when it
298. comes to accounting standards,
299. standard setters, especially when it comes to topics
300. like audits, for example,
301. that is still a requirement legally in many countries.
302. And these are some of the big developments going on
303. right now in the broader digital assets ecosystem.
304. That's all I had in time with you guys all today,
305. but hopefully, this is exciting and insightful,
306. and it was a pleasure sharing with you all
307. some of the trends happening on the regulatory front.

6.7 Virtual Asset Custodian Regulation (Urszula McCormack, King & Wood Mallesons Partner)

1. Hi, my name is Urszula McCormack
2. and I'm a partner of King & Wood Mellesons
3. here in Hong Kong.
4. I have two particular focus areas.
5. I have focus on financial technology
6. and financial crime
7. and I've had a particular interest
8. in virtual assets and blockchain for quite some time.
9. I also sit on the FSC's FinTech advisory board
10. and a very happy participant
11. of many associations here and abroad.
12. Today I am going be speaking to you
13. about the regulation of virtual asset custody.
14. And there are three things that are relevant to this.
15. What custody means for virtual assets.
16. What the custodian actually does.
17. And where this all happens.
18. So what does custody mean for virtual assets?
19. It means controlling the private key.
20. That is, the string of letters and numbers
21. that binds with the public key
22. and allow a transaction to occur.
23. Now, this private key could be in a few different forms.

24. It could be electronic, on a laptop,
25. on a mobile phone,
26. on a physical hardware wallet,
27. or even on a piece of paper
28. or etched into a gold bar.
29. So custody can also involve controlling something
30. that holds the private key.
31. For example, I might only be a custodian
32. for the safe deposit box
33. that contains your piece of paper
34. that contains the private key.
35. Increasingly, there are also self-custody software
36. and hardware solutions
37. that assist with key management.
38. They can be quite simple
39. or they might help you split a private key
40. into multiple pieces,
41. so that different people hold different parts
42. and have to come together
43. to direct the transaction.
44. Self-custody solutions tend not to be regulated
45. as a custody service,
46. because technology itself is generally not regulated
47. but you have to carefully examine
48. the precise technology,
49. contracts and laws involved
50. to make sure that's the case.
51. The next point we consider
52. is what the custodian actually does.
53. And this is generally governed by
54. what the custodian agrees to do in a contract,
55. but sometimes this could be implied
56. by law or even imposed by regulators.
57. And there are six typical things that a custodian does.
58. The three core functions are: (1) to hold the asset,
59. (2) is to protect the asset,
60. usually through segregation from other assets,
61. cybersecurity and operational controls,
62. and now increasingly through insurance.
63. (3) And the third function
64. is to move the asset on instruction,
65. this could be a transaction-by-transaction instruction
66. or under a standing authority
67. But many custodians go beyond that role,
68. they may, for example,
69. (4) analyse the asset and certain patterns that occur.
70. (5) They might manage the asset

71. and even invest it for you
72. or (6), they could use the asset themselves,
73. and potentially even profit from it,
74. if that's the agreement that you have struck,
75. for example, instead of paying fees.
76. Now, depending on where this is all happening,
77. where it is being marketed,
78. different regimes apply
79. to these custody services.
80. And yes, the regulations are different.
81. However, there're some general themes.
82. First of all, direct regulation
83. of virtual asset custodians is increasing.
84. The core obligations that are typically imposed
85. on custodians directly include
86. licensing, being fit and proper,
87. conducting AML/KYC controls
88. and complying with ongoing prudential standards.
89. If the custodian also invests the virtual asset
90. and manages it for you,
91. then it's very common for a different regulatory regime
92. to apply as well.
93. For example, in Hong Kong,
94. the Companies Registry TCSP licensing regime applies
95. to trust and company service providers,
96. serves custodians,
97. but the Securities and Futures Ordinance
98. could also kick in if the custodian
99. is managing virtual assets that include securities.
100. A similar approach applies in the UK and Singapore,
101. but things are rapidly developing.
102. There is also indirect regulation
103. of virtual asset custodians.
104. What this means is that regulated entities
105. that use custodians as part of their business
106. are subject to strict rules
107. about how the virtual assets are held.
108. This could include things like
109. making sure the custodian
110. is regulated in a certain way,
111. that the assets are appropriately
112. segregated and protected,
113. and potentially also insured,
114. that specific technology standards are applied
115. and that there are specific rules applied
116. to hot versus cold storage and other things.
117. Again, taking Hong Kong as an example,

118. the Securities and Futures Commission
119. has issued guidance for fund managers
120. that use virtual assets
121. as part of their business
122. and those standards include custody rules.
123. The SFC's conceptual framework
124. for exchanges also has rules regarding custody.
125. In both cases,
126. each party's also subject to the general law.
127. This includes not laundering money
128. or financing terrorism,
129. complying with privacy law,
130. thinking through bankruptcy and insolvency rules,
131. complying with consumer protection laws
132. and considering how trust law might inform
133. the obligations that the custodian has.
134. So what is happening globally?
135. There are two key developments.
136. First of all, the Financial Action Task Force,
137. the international standards setter
138. for anti-money laundering, counter-terrorist financing,
139. has formally recommended
140. that all virtual asset service providers,
141. including custodians, be regulated and subject
142. to the world of FATF AML/KYC requirements,
143. including customer due diligence,
144. screening and monitoring, and so on.
145. Secondly, there are many virtual asset-specific laws
146. and regulations emerging.
147. Malta, Japan and Bermuda are three examples of this,
148. and Bermuda also provides one of the most detailed
149. Codes of Practise issued so far.
150. Now, I also recommend keeping an eye out
151. for industry developments.
152. Associations such as
153. the Hong Kong FinTech Association,
154. ASIFMA and Global Digital Finance
155. are producing excellent practise guides.

Module 6 Reference Reading

References and Suggestions for Further Reading in Module 6

- **Masarch Paquet-Clouston et al., "Ransomware payments in the Bitcoin ecosystem", Journal of Cybersecurity, 5(1), 2019.**
- **Rolf van Wegberg et al., "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin", Journal of Financial**

Crime, 25(1), 2018.

- David Lee Kuo Chuen et al., "Cryptocurrency: A new investment opportunity?", Journal of Alternative Investments, 20(3), 16-40, 2018.
- K. Krombbolz et al., "The other side of the coin: User experiences with bitcoin security and privacy", In Proceedings of Financial Cryptography and Data Security, 20th International Conference (FC 2016), p.555-580, 2017.
- A.F. Neil Gandal et al., "The impact of DDOS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox", Proceedings of the 15th Annual Workshop on the Economics of Information Security, abs/1411.7099, 2016.
- Andres Guadamuz and Christopher Marsden, "Blockchains and Bitcoin: Regulatory responses to cryptocurrencies", First Monday, 20, 2015.

Read More

Leave a Reply

Your email address will not be published. Required fields are marked *

COMMENT

NAME *

EMAIL *

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search ...

Subscribe

LEARNTHINGS.ONLINE TELEGRAM GROUP

RSS

IPFS for Beginners – Interact With IPFS By Javascript

In this article, we'll learn how to interact with IPFS by javaScript programming language. It's one way to make your own application to interact with IPFS. The post IPFS for Beginners – Interact With IPFS By Javascript appeared first on LearnThings.Online.

Subscribe

Facebook Rename Its Libra Wallet Project Calibra to Novi

2020 May 26, Facebook rename its Libra wallet project Calibra to Novi. It makes its name more separate from Libra. Novi plans to launch its App in 2020. The post Facebook Rename Its Libra Wallet Project Calibra to Novi appeared first on LearnThings.Online.

Libra Appoints It's General Counsel, a Former HSBC, and Goldman Sachs

On May 19th, 2020, the Libra association appoint Robert Werner, an Ex-HSBC & Ex-Goldman Sachs the founder and CEO of GRH Consulting, as its general counsel. The post Libra Appoints It's General Counsel, a Former HSBC, and Goldman Sachs appeared first on LearnThings.Online.