NOTULENSI

Date: May 27th 2015

Place: Nusa Dua Convention Center, **The 3rd International Conference on Information and Communication Technology (ICOICT 2015)**

Presentasi dari KeyNote Speaker: **Kouichi SAKURAI**

Notulis: Dini Turipanam Alamanda, Telkom University

Kyushu University/ Institute of Systems, Information Technologies and Nanotechnologies (ISIT)

Title: "**New Infrastructure and Applications Developed From a Cryptocurrency BITCOIN and a Platform EthereUM"**

1. Bitcoin: Virtual becomes REAL. Now available in more situations both for electroninc devices and SIM CARDS even in Restaurants & Bars and in the hospitals
2. Bitcoin: World Wide. Available at more than 5000 sites. Japan is 40 and Indonesia is 54 especially in Bali
3. Bitcoin here in Indonesia. Indonesia is now one of the most popular area (menurut saya sih targeted area) for BITCOIN based on the data that the number of Indomart is more than 10000
4. In greenschools of Indonesia, the mechanism of bitcoin is told
5. Indonesia Start to Embrance Bitcoin for web-hosting service and hotel payment
6. Headline on Bitcoin:
    a. Regulations for bitcoin (Singapore, China, Japan)
    b. Abuses, Crimes and Lawsuits (Bitcoin mining malware; Malware spread via skype works as Bitcoin miner; Mt Gox Bankrupty)
    c. Getting popularity and Uitility (First Bitcoin ATM in Singapore; World cup betting system "Bitkup)
7. Regulations for Bitcoin: :Singapore clamps down on Bitcoin exchanges with new regulations PC WORLD, Mar 13, 2014
8. Singapore plans to regulate local bitcoin exchanges to stop the virtual currency from being used in money laundering and terrorist financing schemes, autorities said
9. Bitcoin set fresh Chinese regulatory attack .. (financial times, Apr 2 2014). Bitcoin exchanges in China are braced for yet another blow from the central bank that would imperil their survival
10. Japam's rulling party dropsi Bitcoin regulation plans...(zd net, June 19, 2014)
11. Takuya Hirai, an LDP lawmasker and leader of the Japanese party's internet media
12. Abuses, Crimes and Lawsuites. "Mt Gox files for bankruptcy, hit with lawsuit" ... (Reuters, Feb 28, 2014)
    a. Mt. Gox, once the world's biggest bitcoin exchange filed for bankruptcy protection in Japan on Friday
13. "Mt Gox"
    a. Lost 650 thousands bitcoins (=$120 million)
    b. Attacks from the ouside?

14. Cyber Research on Bitcoin
    a. From Economics
    b. From Regal Aspect
        i. Promote or Restrict BIT (COIN) NOMICS
    c. From Science and Engineering (Big Influence has arisen)
15. Influence of BITCOIN
    a. Infromation and communication technology
    b. Business and Economic
    c. Privacy
    d. Math & Cryptography
    e. Computer Science
16. History of Virtual Currency <Bitcoin arose necessarily>
    a. 1st Period: “Paypal”; via internet
    b. 2nd Period: “Edy” “Suica”; with noncontact technology
    c. 3rd Period: “Square”; with smartphone
    d. 4th Period: BITCOIN?
17. Centralized Vs Decentralized <A Rough History>
    a. PGP (1981 - ~): Public Key Crypto Suites; Deentralized (“Web or Trust”)
    b. PKI (1994-~): With the history of SSL mainly; Centralized
    c. Bitcoin: Electornic Currency; Decentralized
18. Proof of Work: a Key Notion for Global Consnsus = Evidence of “Working Hard” = NONCE
19. Hash (Nonce|Previous Hash Val|Present Block) < 2ND
    Hard to find but easy to verify
20. Why Global consensus?
    a. Avoid :double spending ; “to find another answer, hopeless hard”
    b. Proof of work avoids “double spending” (GREAT INVENTION)
21. Global Consensus: Puzzle of Byzantine Problem:”How can we block “double tounged”
22. Variations: “Proof of XXX”
    a. Proof of Knowledge: prior invention
    b. Proof of work: proof of computation
    c. Proof of Space: a Kind of proof of work
23. Problems on Bitcoin:
    a. Prob 1: Poor coding invites Transaction Malleability
    b. Prob 2: Anonymity might cause illegal use (drug, weapon, malware)
24. Anonymity of Bitcoin:
    a. Many Accounts can be made from your ID
    b. One time account enables perfect Anonymity
25. Bitcoin needs A LAW to prefent illegal user
26. The Life of BITCOIN
    a. How long can have bitcoin’s life
        i. Unexpected crypto attacks
        ii. The life of crypto-algoritm (EDCSA, SHA)
        iii. 20 years or 30 years??
        iv. Vs Physical Gold
    b. Cf DES → 2 key TripleDES → AES

        i. NIST vs ISO/IEC
    c. How to design new crytocurrency with longer life? 10 YEARS? 20 YEARS
27. Bitcoin: REVISITED
    a. Chryptocurrency 1.0
        i. Value security = difficulty of Hash Calc
        ii. Many invetments make much money. Software imp(slow)ASIC imp (accelerated)
    b. P2P Currency
    c. Distributed Ledger System
    d. Transaction with Digital Signature
28. Two aspects of Bitcoin
    a. Digital curency with central bank (but price gyrates) → creates many "altcoins" → integration → P2P Platform to exchange worth something → pursue the concept
    b. Blockchain as public ledger of transaction
29. New Business Application with P2P. On decentralizing prediction markets and Order books WEIS2014.
    a. J Clark et al
    b. I Concordia Univ
30. LATEST HOT NEWS. Metadisk for file sharing
    a. File sharing application
        i. "a pierce of software not a company"
    b. Distributed cloud strorage