情報と社会そして人間

川合　慧
放送大学

2014年11月

1

あらまし

- 情報と社会の要素 － 通貨を例として
  - 通貨と決済について
  - 新しい通貨（情報通貨）
  - ビットコイン
    - 技術的要素と通貨機能及び運用
- 情報と人間 － 情報技術発展の未来
  - 自然・社会の発展と進化の法則
  - シンギュラリティ（singularity）

2

ビットコイン（BITCOIN）

情報環境と通貨

実現の仕組み

社会の中での運用

3

マウントゴックス破産！

仮想通貨「ビットコイン」の取引所マウントゴックスが，
2014年2月28日に民事再生手続きを申し立て
490億円相当のビットコインが消失！！
同年4月16日　上記申し立て棄却．資産保全命令から破産へ

仮想通貨？
ビットコイン？
ビットコインの仕組みは？
そもそも通貨とは何？

4

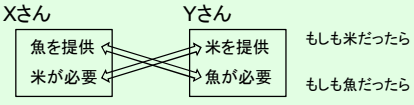
通貨：社会活動の一要素

- 通貨とその機能
  - 通貨：流通貨幣の略
    「国家など」によって価値が保証されたもの
  - 通貨の主要機能
    - 決済手段（支払い）
      等価値の物と交換する　　物品・サービスなどを買う
    - 価値尺度（物差）
      価値を測る尺度　　値段を知る（鑑定団！）
    - 価値保蔵
      「価値」を手元に保持する　　あれば安心

5

需要と供給

- 自給自足社会では通貨は不要
- 分業と物々交換：市場経済の誕生
  - この場合，需要と供給の二重の一致が必要
- 各々が：何かを提供し，何かを必要とする

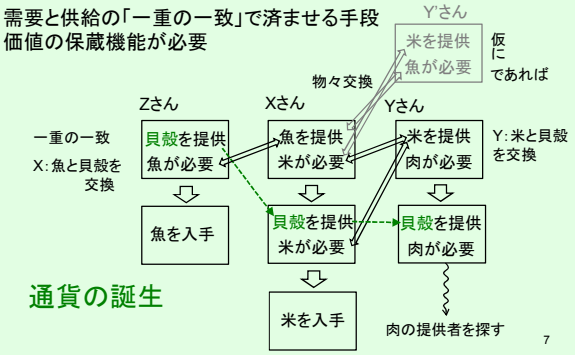


- このままでは物々交換が成立しない
- これで初めて需要と供給の二重の一致が実現

6

交換と価値の保蔵

需要と供給の「一重の一致」で済ませる手段
価値の保蔵機能が必要



通貨の誕生

通貨の働き

- 需要と供給の「一重の一致」だけでよい
  - お金があれば，欲しかった洋服が（店から）買える
- 常に使用できることが重要
  - 価値の保蔵の機能が重要
  - 皆がある程度蓄積しておくようになる
- 皆が共通に認めている必要がある
  - 貴金属（金，銀），宝石類
  - 紙幣，コイン（権力の裏づけによる）
  - それ自体に価値は不要 → いろいろな可能性

ヤップ島の石貨

- パラオで切り出し
- “苦労度”が価値となる
- 直径30cm～3m
- 重いものは動かさずに所有者を石貨に記入

日比谷公園にあるもの
直径約1メートル強
大正13年に1000円の価値

通貨の種類

- 通貨の形態

	実物資産	金融資産					プリペイド型	非金融・電子情報
		債券	紙幣・貨幣	決済性預金	定期性預金	その他		
現物	○	△						
国家通貨		△	○	○	△	△	△	
電子情報								○

金，銀，宝石など
借用書
権力の裏づけ
普通預金など
定期預金など

設問：銀行システム内の電子データは通貨か？

通貨と複製

- 通貨の複製・改ざん
  - 価値尺度，価値保蔵の面で問題となる
  - 社会的な対処
    - 通貨偽造を犯罪とする　通貨偽造罪（刑法第148条）など
    - 複製を極めて困難にする
      すかし，ホログラム，潜像，マイクロ文字，など
    - 偽造「通貨」を流通させない
      偽造検知の習慣
- それでは電子情報通貨は？

電子通貨の実現

- 電子情報を通貨とするには
  - コピーが極めて容易であることへの対処
    - 偽造を犯罪とする　△
    - 複製を極めて困難にする　×
    - 偽造「通貨」を流通させない　×
    - 電子的処理のセキュリティを高める　△
  - 対策の案
    - 所有者しか使えないようにする
      - “所有者”の概念が必要
    - コピーが無いことを保証する方式を採用する
      - 衆人監視システムの利用（一案）

通貨の管理

- 権威・権力による
  - 発行，流通，回収などを管理
  - 社会の価値基盤の役割
  - 「違法」な活動を排除
  - 通貨政策が可能
- 権威によらないことは可能か
  - 「参加者」による自発的な活動
  - 発行，流通の「自動化」を目指す
  - 価値基盤となりうるか

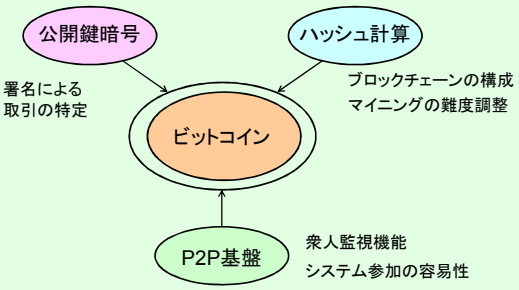
13

ビットコインの概要

- 可能性提案　2009年（Nakamoto）
  - 権威によらない自由参加型を目指す
- 複製防止方法
  - 所有者の概念を導入
    - 支払者，受領者を明確にする
    - ⇒ ある種の暗号システムを使用　公開鍵暗号
  - 複製が無いことを保証する方式
    - 衆人監視システムによる　P2P通信
- システムの維持
  - システム維持のインセンティブ　報酬の仕組み

14

ビットコインの情報技術



15

暗号：従来型

- 秘密鍵方式
  - もとのデータ（平文，ひらぶん）を
    - ある方式で　・・・ たとえば英文字を「進める」
    - あるパラメタ（鍵）で　・・・ たとえば3文字　A→D，B→E，・・・
    - 変換して暗号文を得る（シーザー暗号）
  - 暗号文から平文（復号）
    - 同じ形式で　・・・（同上）
    - 暗号化と逆のパラメタで　・・・ たとえば－3文字
    - 変換して平文を得る

THE OPEN UNIVERSITY OF JAPAN （平文）
⇒ WKHRSHQXQLYHUVLWBRIMDSDQ（暗号文）

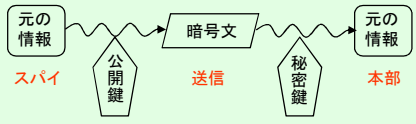
16

公開鍵暗号

- 従来型では鍵の秘匿に多大な労力が必要
  - 他国に送り込んだスパイ，長期潜航している潜水艦
    ゾルゲ事件，Uボートとエニグマ
- 暗号化と復号を分離できて，

“暗号化鍵から復号鍵を求めるのが非常に困難”
であれば，どちらか一方は公開できる

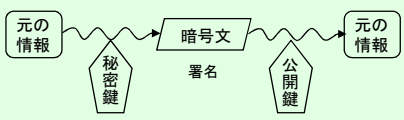
- 情報 ⇒暗号化鍵（公開鍵）で暗号化 ⇒暗号文
- ⇒復号鍵（秘密鍵）で復号 ⇒情報



17

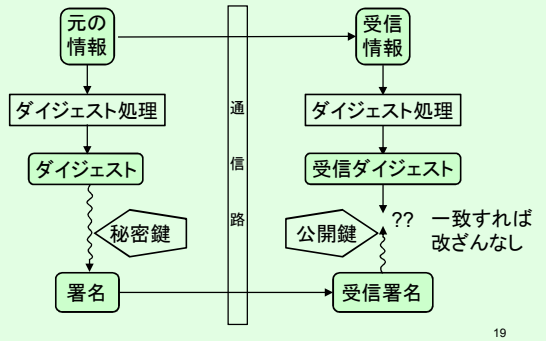
電子署名

- ある文書が正統な人によって書かれたことを保証
- 作成者本人の秘密鍵で“暗号化”しておく
  - 作成者の公開鍵で“復号”できればOK
  - 改ざんされていると正しく“復号”できない
- 秘密鍵→公開鍵で元に戻せる方式であることが必要



18

電子署名の実際

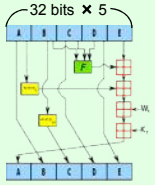


19

ハッシュ関数－1

データのダイジェスト作成

- 入力値から，規則性のない固定長の値（ハッシュ値）を生成
- ハッシュ値から元の値はほとんど復元できない
- 通信文のダイジェストに使用
- Secure Hash Algorithm (SHA)
  - SHA-1（160ビット）
  - 右図の操作を80回繰返した結果をそれまでの値に蓄積
  - 現在ではSHA-2（256ビット）を使用



20

ハッシュ関数－2

- 元データの軽微な差が“拡大”される
- 元データの復元は不可能
- 軽微な差と結果の例

"The quick brown fox jumps over the lazy dog"
16進数: 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12 (160ビット)
英文字：L9ThxnotKPzthJ7hu3bnORuT6xI=

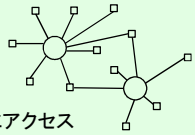
違いはこれだけ！

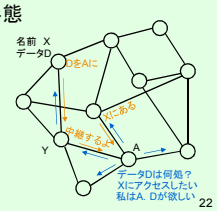
"The quick brown fox jumps over the lazy cog"
16進数: de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3
英文字：3p8sf9JeGzr60+haC9F9mxANtLM=

21

P2P通信

- データの管理と通信の方式
  - サーバ・クライアント型
    - いくつかのサーバにデータを集約
    - 多数のクライアントがサーバ（群）にアクセス
    - 通常のインターネット利用の形態
  - Peer to Peer型（P2P）
    - 参加するコンピュータ全体でデータを蓄積
    - データへのアクセスもコンピュータ全体に対して行う





22

P2Pシステムの例

- Napstar（1991～2000，2003～ ） ファイル共有ソフト
  - 著作権無視のコンテンツ流通で敗訴
  - その後DRM付きコンテンツを販売（Digital Right Management）
- Winny（2002～ ） ファイル共有ソフト
  - PCの内部情報をばらまくウィルスAntinnyで問題化
  - 開発者も著作権侵害行為幇助で逮捕
    - 最高裁で無罪 ソフトは価値中立
- Skype（2003～） 音声通話を主とするシステム
  - カタログ等は多数のスーパーノードで管理
  - スーパーノードは自動選択される
    - 規準：高性能CPU，大容量メモリ，Skype起動時間が長い
  - ゲートウェイ使用で一般電話網にも接続

23

P2Pの特性

- P2Pの特徴
  - スケーラビリティが高い
    - システムが大きくなっても特定のノード（サーバ）に負荷が集中しにくい
    - 動画配信などで有効
      ネットワーク全体に高負荷をかけやすい面もある
  - コストが低い
    - 高価なサーバや高額な回線費用を回避できる
  - 耐障害性が高い
    - 災害時に有効

24

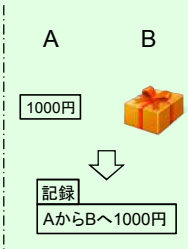
通貨機能の実現

- 皆が共通に認めていること
  - 利用するコミュニティの大きさによる
- 偽造が困難なこと
  - 偽造そのものの困難さ
- 適度な流通量が保障されること
  - 発行と回収のメカニズムが必要

25

通貨の使用と偽造

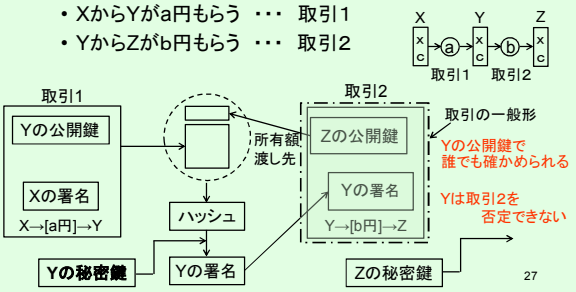
- 通貨の使用
  - “AがBから1000円で品物を買った”
  - =“1000円がAからBへ移動した”
  - 通貨所持者の移動記録が重要
  - 匿名性は別の問題
- 通貨の偽造とは？
  - 偽の「通貨」を作成する
  - だけではなく
  - 使用することが問題
- ビットコイン方式：偽の使用記録の作成を防ぐ



26

取引記録

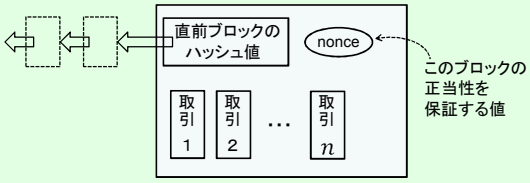
- 改ざん等の防止
  - 取引き関係者の暗号データを付加する
    - XからYがa円もらう ・・・ 取引1
    - YからZがb円もらう ・・・ 取引2



27

ブロック

取引記録をまとめたもの：ブロック



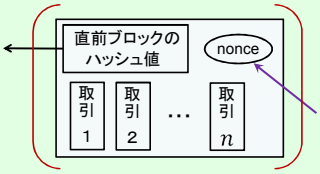
全体としてチェーン状になる：ブロックチェーン
ブロック：誰がいつ作成するか
⇒一定条件を満たせば誰でも可能！！

28

マイニング

ブロックの追加

- 作成しようとするブロック



これ全体のハッシュ値が
非常に限られた値(目標値)
になるような
nonce値を求める

実際の手順

nonce を選ぶ → ハッシュ → 限られた値になればOK

失敗

これを多数回繰り返す

29

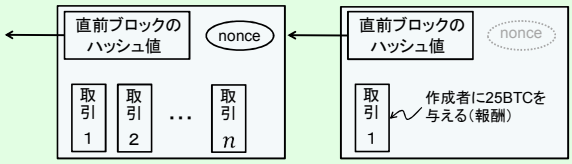
マイニングの速度

- マイニングの目標値
  - きわめて小さなハッシュ値
  - 現在はおよそ
    “先頭の70ビット／256ビットがゼロ”の値
  - 目標値が小さくなるとマイニングが難しくなる
  - ブロックが約10分ごとに作られるように
    目標値が(2週間ごとに)調整される
    - 10分より短 → 目標値を難しくする
    - 10分より長 → 目標値を易しくする

30

マイニングの報酬

- 報酬を求めて一番乗りを競う
- 成功したらブロックを作成

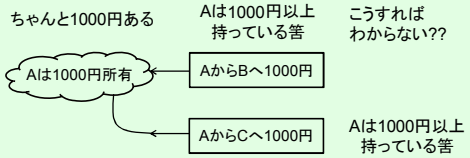


- 報酬は50BTCから始まり21万ブロック(約4年)ごとに半減
- 最小単位(0.00000001BTC)を割ったら発行停止
- 2140年頃に約2100万BTCが発行され，以後増えない

31

通貨の偽造

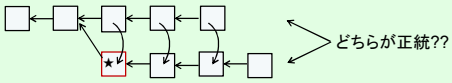
- 偽造:裏付けのない移動記録の作成
  - Aが1000円しか持っていない時に
  - AからBへ1000円移動し，かつ
  - AからCへ1000円移動した
  - 順番にやると所持金不足が発覚する！



32

ブロックチェーンの分岐－1

- 偽造等を行おうとすると ･･･
  - 取引経緯であるブロックチェーンの模造が必要
  - ところが，これまでの経緯はすでに公報されている
  - 新しい部分チェーンを作る必要がある
    ⇒正当部分と偽造部分が分岐する



  - 偽造部分以外を全部取り込む必要がある
  - 最長チェーンを正統なものとする(原則)

33

ブロックチェーンの分岐－2

- 模造チェーンの作成可能性
  - 他の参加者全体よりも速く
    (分岐)チェーンを伸ばせればよい
  - 全計算能力の50%を越えれば可能
    - グループマイニングで現実味
    - 40%越えの例あり
- ブロックチェーンの分岐
  - 数時間程度の実例あり
    - 協議により解決
  - 単ブロック分岐は普通に発生している

34

マイニング競争

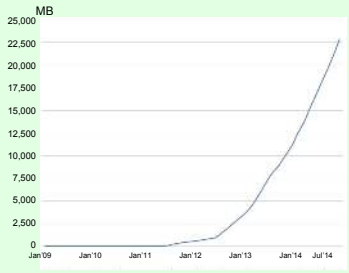
35

現実のビットコイン

- 取引は「未確認取引」プールへ蓄積
  - 未確認取引状況
- マイニングされると1個のブロックとなる
  - 確認ブロックの生成の様子

36

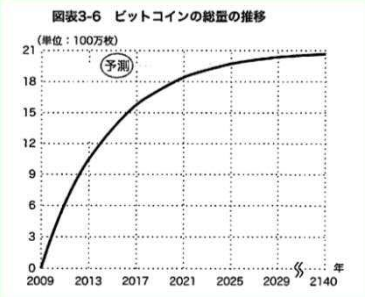
ブロックチェーンの大きさ



2014年11月7日現在
329,000ブロック

2014年頃に
6,929,999ブロック
マイニングは終了
後は手数料収入

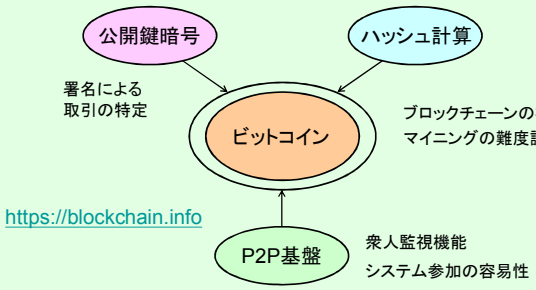
ビットコイン総量



マイニングの難度と
報酬額で制御
⇩
希少価値の保持

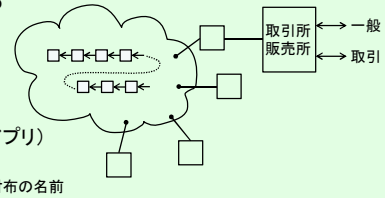
2014年頃に
6,929,999ブロック
マイニングは終了
後は手数料収入

ビットコインの情報技術



ビットコインの運用

- P2Pで構成される
  ブロックチェーン



- ウォレット（財布アプリ）
  - 参加すると
    - 公開鍵：その財布の名前
    - 秘密鍵：取引に使用
  - 保管の方法
    - オンライン（ホットウォレット）　ネットワークセキュリティに問題
    - オフライン（コールドウォレット）　無くすと大変
    - 紙に印刷（ペーパーウォレット）　見られると大変

ビットコインの取引

- 取引所
  - 取引の代行を行う
    - マウントゴックスもその一つだった
    - etwings, BtcBox, Quoine など
    - 世界：Bitstamp, BTC-e, Kraken
- 販売所
  - 売買のみを代行する
    - bitFlyer, Payぴっと, 山吹通商, ヤフオク！

ビットコイン ATM

ビットコインと社会

- ビットコインの広まり
  - 最初は同好会的（2009～　）
    - レートは1～10セント／ビットコイン程度
  - キプロスの財政危機（2013年3月）
    - ギリシャの財政危機（2009年）が原因
    - EUによる支援を受けるため銀行預金に課税／凍結
    - レートが10ドル～200ドルに上昇
  - 中国人民銀行の利用禁止通達（2013年12月）
    - レートが1200ドルに上昇

各国等の判断

・米国：通貨でなく資産で課税対象（IRS 2014/3/25）

・中国：金融機関での取引禁止（2013/12）

・タイ：違法の判断→関連法制定(2013/7)

・スェーデン：通貨でなく資産（2014/1）

・ラスベガスの2カジノで利用可能に（2014/1）

・旅行サイトExpediaで利用可能に(2014/6)

・デルが導入（2014/7），ペイパル（決済大手）(2014/12)

43

日本での扱い

- 日本：2014/3/7閣議決定
  - 通貨としては認めない
    - 強制通用力は無し（受取り拒否ができる）
    - 銀行法・金融商品取引法の対象外
    - ⇒銀行はコインの売買仲介や口座開設はできない
  - 取引は課税対象（法人税・所得税・消費税）

44

ビットコインのもたらしたもの

- 電子通貨の可能性を実証
- 仕組み的に未熟な面を有する
  - 自由参加方式は実現したが・・・
  - 派生効果（副作用）
    - マイニング用電力の浪費，マネーロンダリング
  - 社会・権威との擦り合わせ不足
    - 既存の枠組みの中に位置づける動きあり
  - 「実価値」との関係が薄い
    - 利用の広がりで調整される可能性あり
- 今後の淘汰による発展に期待
  - 他の情報通貨　一覧（2014）

45

シンギュラリティ

--技術進歩の特異点--

- 技術進歩の速度
- 情報技術の性質
- 近未来予測

46

進歩について

- あらゆる分野において種々の“進歩”が見られる
- “進歩”の速度は一定ではない
  - “進歩”を促す状況自体が“進歩”する例が多い
  - コンピュータの性能向上で顕著
  - 情報技術の「万能性」がもたらす問題

⇩

- “進歩”が質的に変わることはないのか
- “進歩”が制御不能になることはないのか

47

一般的な技術進歩の様子

- コンピュータの計算力に支えられた技術進歩の例
  - 質問応答システム
    - 「人間的」応対が目標
  - ゲームプレイ
    - 人間の知的活動へのコンピュータの利用
  - ヒトゲノム解析
    - 超大規模データの解析
    - 医療分野への影響

48

質問応答システム

- チューリングテスト (1950)
  - 対話による「知性度」のテスト．2014に合格マシン
- 精神医療用対話システム ELIZA (1964)
  - 実世界の知識はほとんどない
  - 人間側が感情的に没入する例多し
- 質問応答システム Watson （IBM 2009～）
  - 2011年クイズ番組「ジェパディ！」で人間に勝つ
  - 性能80TFLOPS．70GBのテキストデータが基本
- 受験システム 東ロボくん （NII 2013～）
  - 2013年に偏差値45.1，2014年に47.3

49

ゲームプレイ：チェス

- 1997年コンピュータが人間に勝つ
  - 当時の世界チャンピオンのカスパロフと対戦
  - 1回目（1996年2月）はカスパロフが3勝1敗2分け
  - 2回目（1997年5月）はコンピュータが2勝1敗3分け
- コンピュータ：Deep Blue （IBM）
  - 1989年より準備
  - 32ノード ＋ 専用プロセッサ512個
  - 2億手／秒の先読み
  - 対戦相手（カスパロフ）の過去の棋譜を基とした評価関数を使用

50

ゲームプレイ：将棋

- 人間との対局
  - 80年代 人間の初級者以下
  - 1995年頃 アマチュア初段程度
  - 2005年 プロに角落ちで勝利
  - 2007年 渡邊竜王といい勝負．奨励会三段と認定
  - 2008年 アマチュア名人を破る
  - 2010年8月 女流王将に勝つ
- 強さの比較
  - 2014年：持ち時間の短い対局で人間トップと対等
  - 2015年：名人戦の環境で人間トップと対等（予測）

51

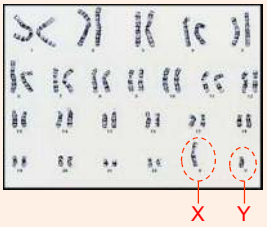
ゲームプレイ：囲碁

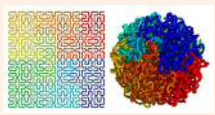
- 1969年（アメリカ）38級程度
- 1990年代 アマチュア上級者レベル
- 1993年 モンテカルロ手法の導入
  - 乱数的着手による評価
- 2006年 モンテカルロ木探索
- プロ相手の成績
  - 2007年 プロ四段に八子で勝利
  - 2008年 プロ九段に八子で勝利
  - 2011年 プロ五段に六子で勝利
  - 2013年 プロ名人と四子で互角
- まだまだ先が長そう・・・・

52

ヒトゲノム：染色体

- ヒトの染色体
  - 24種の線状染色体（1842年～）
  - 22番目までは一対．23，24番目は単独
    - 性染色体 X,Y
    - XX⇒女性，XY⇒男性
    - 大きさ：Xが1098，Yが78
  - 実はヒルベルト曲線状に折りたたまれている

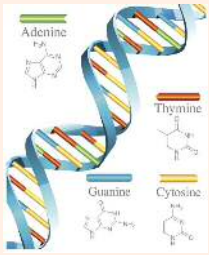




53

ヒトゲノム：ゲノム

- 染色体からゲノム
  - 染色体の構造
    - 2重らせんのDNA
    - 構成要素（塩基）
      - A，T，G，C
      - AとT，GとC が対になる
  - 塩基対の数：ヒト 31億
    - 大腸菌：460万
    - ショウジョウバエ：2億弱
    - イネ：4億
    - 小麦：170億



54

ヒトゲノム解析

- ヒトゲノム計画
  - 31億塩基対全配列の解読
  - 1984年に提案，1991年に開始
  - 2000年にドラフト，2003年4月に完了
- ゲノムの一定の配列が遺伝子として働く
  - ゲノムの配列と位置⇔遺伝子　対応は解明中
- 2万強の遺伝子を同定
  - イネ科の植物の方が多い
  - ウニとほとんど同じ数で共通が7割

55

ゲノム解析手法

- ショットガン・シークエンシング法
  - 大量の短い配列から全体を構成する

第1回のショットガン配列：XXXAGCATGCTGCAG
TCATGCTTAGGCTAXXXX

第2回のショットガン配列：TTAGGCTAXXXX
XXXAGCATGCTGCAGTCATGC

再構築された配列：XXXAGCATGCTGCAGTCATGCTTAGGCTAXXXX

  - 数千から数百万の断片を扱う．エラーもある．
  - 多数のスパコンでも何か月もかかる
  - 一時は特許問題も生じた

56

知識蓄積の加速
- プライスの発見 -

- プライス (Derek J. de Solla Price, 1922-1983)
  - 王立協会学術論文誌のページ数(1665-1850)
  - 毎年2倍になることを発見(1950頃)
  - 解釈：知識の蓄積が蓄積を加速している
  - 他の業績
    - 理研の原爆研究を明らかにした（戦後）
    - アンティキティラ機械の解析（1959）
      - 古代ギリシャの歯車式天体運行表示機
    - プライスの法則(1963)
      - 研究成果の半分は研究者数の平方根の人数が出す
      - 100人いると，成果の半分は10人の仕事

57

コンピュータの技術進歩

- 初期は手作り
  - 人間の思考・作業の速度で行われる
- 作成の自動化
  - 人間の手作業の部分の自動化
  - 正確性，作業速度が向上
- 設計の（半）自動化
  - 目標を達成する手順を「計算」
- コンピュータの設計・作成自身にもコンピュータが適用可能

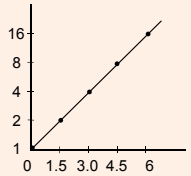
58

ムーアの法則

- Gordon E. Moore（1926 －　　）
  - インテル社の設立者の一人
  - フェアチャイルドセミコンダクタ社（1957 －　　）
  - インテル（1968 －　　）
- 集積回路のトランジスタ（ゲート）数の予測（1975年）
  - “18ヶ月ごとに2倍になる”

2年後　2.5倍
5年度　10.1倍
10年度　101.6倍
20年後　10321.3倍

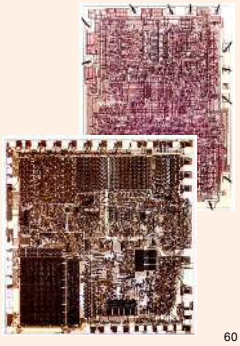
  - 後に“2年ごと”に修正



59

実際のゲートカウント

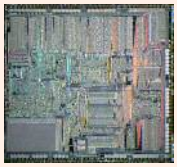
- Intel 4004 (1971)
  - 最初のCPUチップ，ビット幅4
  - ゲート数：2,300
  - クロック：750kHz
  - 速度：0.06MIPS(60,000命令/秒)
  - 以後 8008, 8080
- Intel 8086 (1978)
  - 最初の16ビットチップ
  - ゲート数：29,000
  - クロック：10MHz
  - 速度：0.75MIPS(750,000命令/秒)
  - 以後 80186, 80286

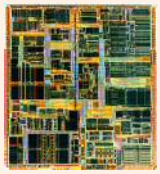


60

実際のゲートカウント(続)

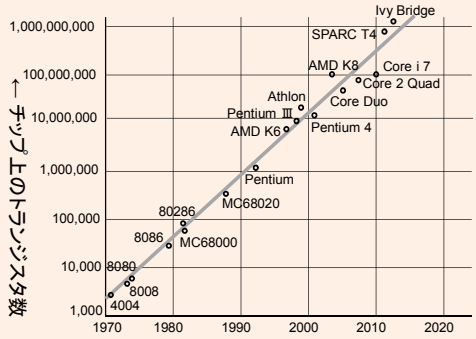
- Intel 80386 (1985)
  - 最初の32ビットチップ
  - ゲート数:275,000
  - クロック:32MHz
  - 速度:11MIPS(11,000,000命令/秒)
  - 以後 80486
- Intel Pentium (1993)
  - 外部接続64ビット
  - ゲート数:3,200,000
  - クロック:200MHz
  - 速度:200MIPS(200,000,000命令/秒)
  - 以後 P-Pro, P-2, Celeron, P3, P4





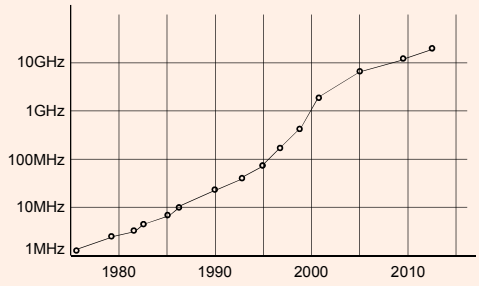
61

ICチップの集積度



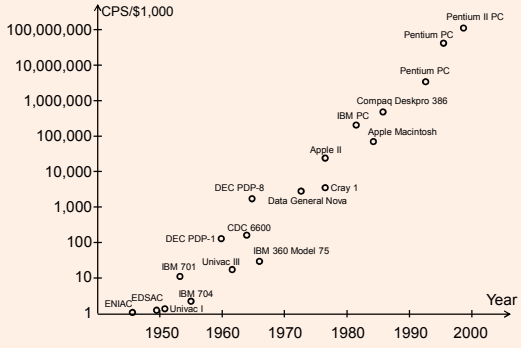
62

クロック速度



63

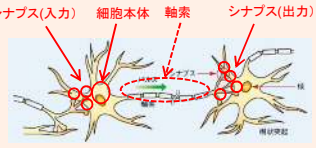
一定コストの計算力



64

ニューロコンピュータ
－自己学習能力の実現－

- 人間の脳の働きを模倣して,「解析済み」ではない自己組織化的な能力を目指す
  - 大規模回路の実現により可能性が高まってきた
- 脳の神経構造
  - ニューロンと軸索・シナプス
  - 本体の電位を軸索沿いに伝達
  - シナプスの間隙を化学物質で伝達



65

ニューロコンピュータ
－自己学習能力の実現－

- 人間の脳のニューロンとシナプス
  - ニューロン数　大脳160億，小脳700億
    - ちなみに　マウス 7000万，ラット 2億
  - シナプス数(一つのニューロンあたり)
    - 8000～10000
  - シナプスによるネットワークの構成の発生メカニズムは未解明
    - 特殊状況に反応するニューロン群は存在する
    - 初期のランダム接続から学習により構成？
    - 接続に関する情報がゲノムに存在する？

どちら？

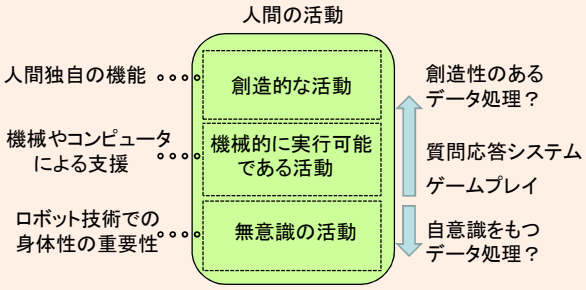
66

人工ニューロンの実現

- 脳の神経回路網のシミュレーション
  - ニューロンとシナプスを人工的に構成
  - 脳への刺激と反応とをシミュレートする
- シナプスプロジェクト（2008～，IBM他）
  - 目標：100億ニューロン100兆シナプス
    in 2リットル by 1キロワット
  - 4年前　256個
  - 2013年100万ニューロン10億シナプスのチップを実現
    16個あわせて1600万個

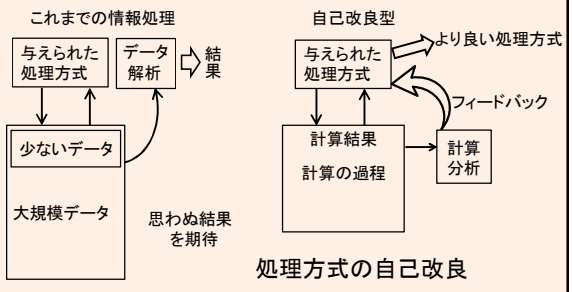
67

人間の活動とコンピュータ



68

コンピュータと創造性



ビッグデータ解析

処理方式の自己改良
≒創造性（？）

69

シンギュラリティ予想

- コンピュータの振舞いの知的度合が増加
  - 計算素子数の増大と処理能力の進展による
- 脳細胞の数と計算速度で見積もると‥
  - 細胞数860億，活動0.1ミリ秒
  - ⇒ 10^{15}／秒
  - 計算素子では10^{10}／秒
  - 量的には高々10万倍！
    - ムーアの法則では「25年後」に実現!?

70

シンギュラリティ予想-2

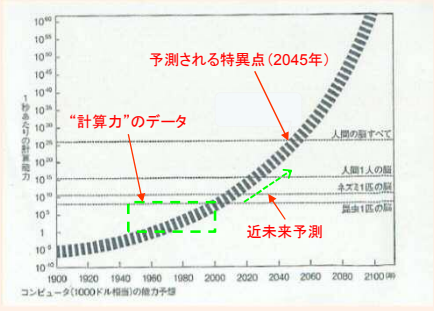
- 技術的特異点（シンギュラリティ）
  - 技術進歩が人間の把握能力を超える時点
  - 人間の脳のシミュレーション　10^{16}~10^{19}計算/秒
  - 全人類の脳のシミュレーション　10^{26}計算/秒
  - 自己改良ソフトウェアが出現すれば，さらに加速

  - これまでの進歩曲線による予測

71

シンギュラリティ予想-3

レイ・カーツワイル（1999，2005）



72

シンギュラリティ予想-4

- 特異点以後テクノロジー進化は機械主導
  - 人間側の進歩と理解力が追いつかなくなる
- 自己改良(≒創造性)の実現がキーポイント
- シンギュラリティ以降は？
  - 人類は不要 → 抹殺　　ターミネータ
  - 人類は付属物 → 飼育　　マトリックス
  - 人類の機械化(enhanced)　　アンドロイド
    - ナノテクノロジーの発展も必要
  - 機械が人類に愛想尽かし → 機械は宇宙の他所へ

73

シンギュラリティ研究

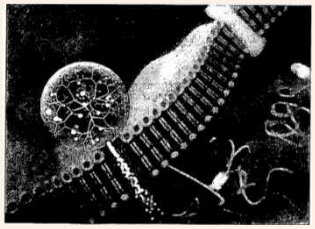
- シンギュラリティ大学(2008，アメリカ)
  - Google, Cisco, Nokia 出資
- シナプスプロジェクト(2008～，IBM他)
  - 目標:100億ニューロン100兆シナプス
    in 2リットル by 1キロワット
  - 人間の脳のデジタルレベルシミュレーションを目指す
  - 2013年に100万ニューロン10億シナプスを実現
- ヒューマン・ブレイン・プロジェクト(2013，EU)
  - 人間の脳の分子レベルのシミュレーション
  - 最終目標:人間の脳のエミュレーション

74

人体機能の強化
カーツワイル

- ナノテクノロジーも同様に発達すると
  - 極微装置を体内に入れて治療
  - 身体能力を増強
  - 強化人間となる

ガン細胞を探り当て
専用薬剤で攻撃



75

技術の将来は

■ ■ ■

76

ゲート数の進展

時　期	型　番	ゲート数	ビット幅	クロック	線幅	MIPS
1971.11	4004	2,300	4	0.75	10	0.06

77

ゲート数の進展

時　期	型　番	ゲート数	クロック	線幅	MIPS
2006.0	Core2Duo	291,000,000		65	

78