Дежавю: что общего у крипто-бума с пузырем доткомов?

Директор Департамента по работе на рынках капитала АО «Россельхозбанк»
Иванов Анатолий Евгеньевич
XV Российский облигационный конгресс, Санкт-Петербург, декабрь 2017 г.

История создания ПК

Ламповые ЭВМ (1945-1955)	Транзисторные ЭВМ (1955-1965)	Интегральные схемы (1965-1980)	Микропроцессор (1980-?)	Мобильные устройства
•Вторая мировая война, развитие радиотехники •1945 г. - Джон Моучли, Джон Эккерт- первая ЭВМ ENIAC •1945 г. - архитектура фон Неймана • 1953 г. IBM 701- первый коммерческий компьютер IBM	•1947 г. -Джон Бардин, Уолтер Браттейн, Уильям Шокли - транзистор •1961 г.- PDP-1-первая серийная транзисторная машина •IBM - популярные модели: 7094, 1401 •Суперкомпьютеры: 6600, 7600 и Cray-1	•1958 г.- Роберт Нойс-кремниевая интегральная схема •Компьютеры стали компактнее, быстрее и дешевле. Наступает эра ПК •1964 г. - IBM System 360 - первая серия масштабируемых компьютеров. Пример открытого стандарта. •1970 г.-DEC-PDP-11-популярные мини-компьютеры в 70-е годы •1976 г. -первый серийный ПК Apple-1	•1971 г.-Intel 4004-первый микропроцессор (4-битный) •1979 г.-Intel 8086-первый 16-битный микропроцессор •1981 г.-IBM PC- первый массовый ПК IBM •1985 г.-Intel 386-первый представитель линейки Pentium •1985г.-Вирт. Н. «Алгоритмы + структуры данных = программы» •Компьютер с сокращенным набором команд (RISC)	•9 января 2007 г. - iPhone первого поколения •23 сентября 2008 года-первая версия Android •2010 г.-iPad

Эволюция сети Интернет

1961—1970

Противостояния СССР и США

1957 г.-СССР запустили спутник

Необходимость в бесперебойной системе связи для оповещения о ракетной атаке

Работа над новой системой связи ARPANET

29 октября 1969 г.-первый успешный сеанс связи

1971—1980

1971 г. -электронная почта

1972 г.- Кан-идея открытой архитектуры сети

1972-1974 гг.-протоколы Telnet, FTP, TCP

1976 г.- локальная сеть Ethernet

1981—1990

1981 г.-протокол IP

1 января 1983 г.-переход на TCP/IP

1983 г.-ARPANET переименовано в «Интернет»

1984 г.- система доменных имен DNS

1988 г.-протокол мгновенной передачи текстовых сообщений IRC, первый вирус-Червь Морриса

В 1989 г. -Тим Бернерс-Ли-концепция Всемирной паутины

Протокол HTTP, язык гипертекстовой разметки HTML и идентификатор URL

1990 г.-начало коммерциализации Интернета

1991—2000

1993 г. – веб-браузер NCSA Mosaic, отправная точка dot.com эры

Новая экономика: электронная коммерция

1994 г.-Internet Service Privider-возникновения хостинга, как услуги предоставления веб-сервера

Бум интернет компаний: 1995 г.- IPO Netscape; 1996-1998 гг.-суперуспешные IPO Amazon, eBay и Yahoo; 1999 г.-IPO интернет-компаний составило 60% всех IPO; 1995-2000 гг.-пятикратный рост NASDAQ Composite

10 марта 2000 г.-достигнут пик индекса в 5132,52 пункта, который упал к концу дня на 1,6% до 5048,62

2000-2002 гг.- пятикратное снижение NASDAQ Composite. 9 октября 2002 г. индекс достиг минимума в 1114,11 пунктов. Рыночная капитализация интернет-компаний потеряла $5 трлн.

2000 — по н. в.

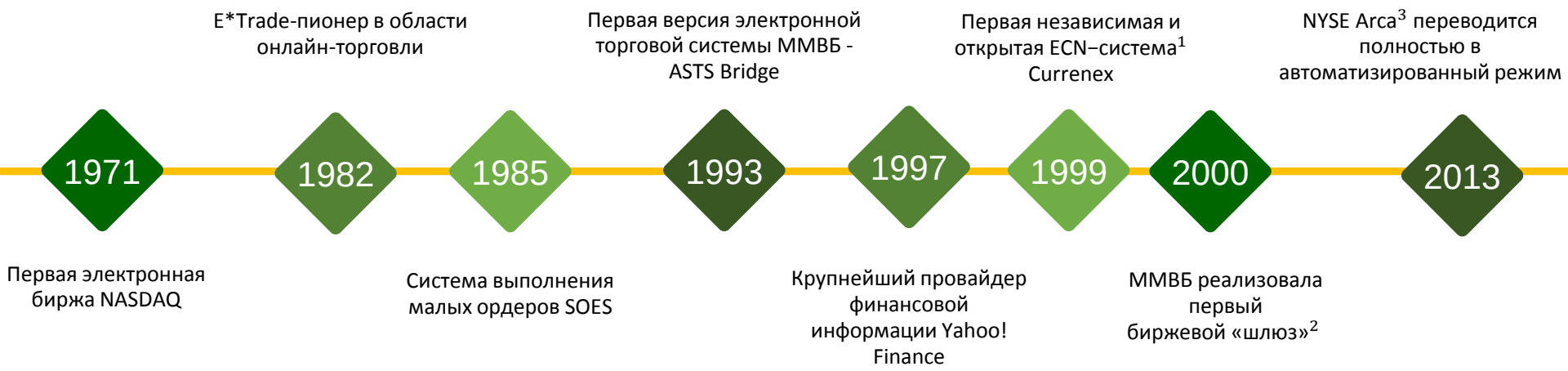
2003-2006 гг.-соцсети: LinkedIn, MySpace, Facebook, Twitter, Vkontakte

IoT-Интернет вещей

2009-2013 гг.-мессенджеры: WhatsApp, Viber, Telegram

2015 г.-Telegram-канал

Развитие финансовых рынков в интернете



1 Electronic Communication Network — электронная система осуществления сделок купли-продажи биржевых товаров, устраняющая роль посредников
2 Специализированные интерфейсы для подключения удаленных терминалов инвесторов к торговой системе ММВБ при помощи Интернета
3 Подразделение NYSE Euronext

История криптовалют: криптография, ранние идеи

Хэш (англ. «hash»- путаница)

- 1640 г.-**Малая Теорема Ферма:** Если p — простое число, a — целое число, не делящееся на p, то a^{p-1}-1 делится на p
- 1953 г.-Ханс Петер Лун-идея **хэш-кодирования**-преобразования массива входных данных произвольной длины в битовую строку заданной длины при помощи определённого алгоритма-хэш-функции
- 1079 г.-**конструкция Меркла-Дамгарда**-разбивает входное сообщение на блоки и работает с ними по очереди с помощью функции сжатия, каждый раз принимая входной блок с выходным от предыдущего прохода. Используется в алгоритмах MD5, SHA-1, SHA-2

Цифровая подпись

- 1976 г.-Уитфилд Диффи, Мартин Хеллман –революция в шифровании, появление **криптографии с открытым ключом**. **Алгоритм Диффи-Хеллмана** позволял двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Уязвимость «посредника»: злоумышленник может просто вклиниться в канал передачи данных
- 1977 г.-Рональд Ривест, Ади Шамир, Леонард Адлеман- криптографический алгоритм **ассиметричного шифрования RSA**. Имеется два ключа: открытый и закрытый
- 1985 г.-Нил Коблиц, Виктор Миллер-использование эллиптических кривых для создания криптосистем (Bitcoin использует ECDSA secp256k1)
- 1991 г.- Филипп Циммерман-**PGP**-первая широкодоступная программа, использующая шифрование с открытым ключом

Первые электронные деньги

- 1990 г.-Дэвид Чаум-**Digicash**-первая электронная валюта
- 1997 г.- Адам Бэк –**Proof-of-Work** Hashcash. Изначально применялась для уменьшения количества спама и DoS-атак (PoW в Bitcoin использует SHA256 вместо SHA1)
- 1998 г.- Вэй Дай-идея общедоступного глобального регистра **«b—money»**
- 1998 г.-Ник Сабо-алгоритм децентрализованной цифровой валюты **«bit-gold»**

История криптовалют: Bitcoin, Альткоины

- 2008 г.-Сатоши Накомото-**White Paper Bitcoin**
- 2009 г.-генерация первого блока, первая транзакция
- 2011 г.-появление первых альткоинов
- **Namecoin**-первый альткоин, связывающей Bitcoin с DNS. Устойчив к цензуре и работает вне рамок регулируемого интернета
- **Litecoin**-наиболее успешный альткоин. Использует хеширование Scrypt вместо SHA256, отличается более высокой скоростью проведения денежных операций и небольшим объемом блоков
- Второй известный представитель семейства Scrypt –**Dogecoin**
- **Proof-of-Stake (PoS)**-альтернатива Proof-of-Work. Вероятность формирования участником очередного блока в блокчейне пропорциональна доле, которую составляют принадлежащие этому участнику расчётные единицы данной криптовалюты от их общего количества
- Валюты с гибридным подтверждением PoW и PoS: **Peercoin** (SHA256) и **Novacoin** (Scrypt)
- 2012 г.-**Ripple**-не альткойн. Вместо блокчейна создана система «платёжных шлюзов», которая делает токены Ripple интересными для банковских расчетов
- 2012 г.-алгоритм **CryptoNote**, использующий «кольцевую подпись»
- **Bytecoin**-первая криптовалюта, использующая алгоритм CryptoNote

История криптовалют: «Крипто 2.0»

- До июля 2013 года ПО всех криптовалют, кроме Ripple, базировалось на открытом исходном коде Bitcoin. Затем стали появляться альтернативные платформы, которые помимо криптовалюты поддерживают различную инфраструктуру — биржевую торговлю, магазины, мессенджеры и прочее

- Криптовалюты второго поколения: **Mastercoin** (надстройка над блокчейном, позволяющая заключать криптографически подтвержденные смарт-контракты), **Nxt** (100% PoS)

- 2014 г.-самая нашумевшая криптовалюта второго поколения **Ethereum**. Не просто цифровая валюта, а также открытая многофункциональная платформа на основе технологии блокчейна, работающая на базе умных контрактов , которая позволяет разработчикам создавать и разворачивать децентрализованные приложения

- Приватные криптовалюты: **Dash** (X11- последовательность 11-ти криптографических алгоритмов) и **Monero** (Crypto Note)

- 2016 г.-первая по-настоящему анонимная валюта **Zcash**, основаная на протоколе **zero-knowledge proof**. Принцип действия протокола предполагает, что одна из взаимодействующих сторон способна убедиться в достоверности математического утверждения, не имея при этом никакой другой информации от второй стороны

- 2017 г.- суперуспешное ICO системы смарт-контрактов **Tezos**, альтернативной Ethereum. Удалось собрать $232 млн.

- На сегодняшний день существует более 1000 криптовалют