Dr. Christian Kümmerle
Hariharan Vijay Iswaran
Abheek Das

February 25, 2025

Bitcoin: Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010

Midterm Exam – Solution Keys

Name:

Charlotte ID:

- Please try to answer each question within the allocated space after each question. If you need more space for a question, use the space on blank pages or at the very end of the exam, and indicate this fact at the respective question.
- You are allowed to use one US letter-sized "cheat sheet" of paper (front and back), with handwritten notes on it.
- You are allowed to use a non-programmable calculator.
- Beyond that, this exam is a closed book / closed notes exam. No other tools are allowed.
- There is a maximal reachable number of points is 75 points.
- The working time of the exam is 75 minutes.
- The exam contains a total of nine printed pages.

Signature:

Question 1: **(8 Points)**

There a divergent views on historical origins of the concept of "money" in human societies.
Briefly describe **two different theories** on how money came to be in human societies.
For **each** theory, mention **either a proponent of the respective theory** or a **historical example for why this theory could be applicable** (2-3 sentences each).

1. The commodity theory of money states that historically, humans encountered the problem of efficient trade with each as different people produce different goods, which enables trade by barter only if a "coincidence of wants/interest" exists. Over time, certain commodities or goods with desirable properties (scarcity, durability, divisbility) emerge as money to serve as medium of exchange to facilitate trade. Proponents: Adam Smith, Carl Menger Historical Examples: Emergence of (unminted) metal money such as Bronze Aes Rude in Ancient Rome, spade money in Zhou dynasty in China, minted coin moneys in China, Greece, Rome

2. The credit theory of money describes money as a record of obligations or debt between individuals. In particular, it implies that money corresponds to a token of trust/ a technology within the community that can be used to settle these obligations. Proponent: David Graeber Historical Examples: Bank notes issued by banks in commodity monetary standard (e.g., gold standard), limestones on Yap Island incoding debts as commodity-based public ledger

3. There is also the theory that describes money as originating from primitive collectibles (such beads made from shells, mammoth ivory beads, Kula necklaces, Kula armshell, etc.) that allowed for efficient wealth transfer across generations and that could build trust and mitigate risks for altruism in human societies. In particular, these collectibles could served several purposes, such as as family heirlooms, starvation insurance, mitigation of aggression, or facilitate an efficient marriage market. Proponent: Nick Szabo Historical Examples: Above; Mitigation of war in Iriquois Confederacy, advantage of homo sapiens vs. Neanderthals

4. The state theory of money (not explicitly covered in class) states that it derives is usefulness from a standardization / issuance by a governmental authority, e.g., through its acceptance for paying taxes.

5. Other possibilities: Money as good with best monetary properties - Proponent: Parker Lewis

Question 2: **(3 Points)**

List the **three different key functions of money** that most monetary theorists agree on (bullet points are sufficient).

- Store of Value
- Medium of Exchange
- Unit of Account

Question 3 (Choose one): **(2 Points)**

Under a so-called *gold standard*, what is the primary mechanism that maintains the value of a currency?

a) Governments set the exchange rate based on international trade balances.
b) The currency value is tied to a specific quantity of gold.
c) The value is determined solely by market forces between competing private banks, which may or may not back the currency by gold.
d) The currency consists only of gold or silver coins, and the value is guaranteed through the scarcity of these.

Question 4 (Choose one): **(2 Points)**

To make sure that the data in the Bitcoin blockchain has not been changed, which property of cryptographic hash functions is crucial?

a) Pre-image resistance
b) Puzzle-friendliness
c) Hiding property
d) Collision-Freeness

Question 5: **(3 Points)**

Which statements about cryptographic hash function used in the Bitcoin protocol are NOT correct? Please choose **two** statements as exactly two are not correct.

a) The input has to be of fixed length.
b) The output has to be of fixed length.
c) They are used to construct hash pointers.
d) In bitcoin mining, computing one hash function output requires specialized mining hardware (ASICs).

Question 6 (Choose one): **(2 Points)**

Bitcoin's principle of using distributed digital ledgers to keep ownership of digital money accountable was pioneered by...

a) Bit Gold (proposed by Nick Szabo)
b) Hashcash (proposed by Adam Back)
c) Chaumian e-cash (proposed by David Chaum)
d) E-Gold (proposed by Douglas Jackson)

Question 7: **(6 Points)**

List the defining properties of a finite field and give an example for finite field.

A finite field is a set F that together with the two operations "$+$" (called addition) and "$\cdot$" (called multiplication) that satisfies all of the following properties:

- If $a, b \in F$, then $a + b \in F$ and also $a \cdot b \in F$.
- There exists an additive identity element $0 \in F$ that satisfies $a + 0 = a$ for any $a \in F$.
- There exists a multiplicative identity element $1 \in F$ that satisfies $a \cdot 1 = a$ for any $a \in F$.
- For any $a \in F$, there exists an additive inverse (denoted as $-a$) in F that satisfies $a + (-a) = 0$.
- For any $a \in F \setminus \{0\}$, there exists a multiplicative inverse (denoted as a^{-1}) in F that satisfies $a \cdot a^{-1} = 0$.

Example: $F_3 = \{0, 1, 2\}$, or any $F_p = \{0, 1, 2, \ldots, p-1\}$ for any prime p or any p where $p = q^n$ for some prime q.

Question 8: **(12 Points)**

Let 'FieldElement' be a class that represents an element within a finite field of the order p (order specified by second input argument).

Consider two finite field elements a = FieldElement(2, 7) and b = FieldElement(3, 7). In other words, we consider the finite field $F_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

a) What is $a +_f b$? Compute the result.

Since $a = 2 \in F_7$ and $b = 3 \in F_7$,

$$a +_f b = (2 + 3)\%7 = 5\%7 = 5$$

b) What is $a -_f b$? Compute the result.

$$a -_f b = (2 - 3)\%7 = -1\%7 = 6$$

c) What is the multiplicative inverse of a?

$$a^{-1} = 2^{-1} = 2^{7-2}\%7 = 32\%7 = (4 \cdot 7 + 4)\%7 = 4\%7 = 4$$

The second equality holds due to Fermat's little theorem.

d) What is a^{-3}? Compute the result.

We can use the result of c), such that

$$a^{-3} = (2^{-1})^3\%7 = 4^3\%7 = 64\%7 = (9 \cdot 7 + 1)\%7 = 1\%7 = 1.$$

e) What is the additive inverse of b?

-b = (7 - 3) %7 = 4 % 7 = 4.

f) Consider c = FieldElement(2, 9). Is $a == c$?

No, the two field elements are not the same, as they are elements of different fields (different

order).

Question 9: **(3 Points)**

What does Fermat's little theorem state?

Fermat's little theorem states that for each prime number p and each n that is not divisible by p,

$$n^{p-1}\%p = 1,$$

(can be also written as $n^{p-1} \bmod p = 1$.
(Alternative formulation: $n^p\%p = n\%p$).

Question 10: **(2 Points)**

Consider two points $A = (-1, -1)$ and $B = (-1, 1)$ on the elliptic curve $y^2 = x^3 + 5x + 7$. What is $A + B$?

a) Point(18 ,77)_5_7
b) Point(infinity)_5_7
c) Point(2, 0)_5_7
d) Point(-2, 0)_5_7

Question 11: **(8 Points)**

Consider the elliptic curve $S_{-1,4} = \{(x, y) \in F_{13} \times F_{13} : y^2 = x^3 - 1x + 4\}$ **over the finite field** $F_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. $A = (2, 6) \in F_{13} \times F_{13}$ and $B = (1, 11) \in F_{13} \times F_{13}$ are two points on $S_{-1,4}$ (you do not have to verify this).
Calculate $A + B$. State the applicable formulas for getting your results, and show your work.

$S_{-1,4} = \{(x,y) \in F_{13} \times F_{13} : y^2 = x^3 - 1x + 4\}$

$A = (2, 6), \quad B(1, 11)$

$s = \frac{y_2 - y_1}{x_2 - x_1} = \frac{11-6}{1-2} = \frac{5}{-1} = 5 \cdot (-1)^{-1} = 5 \cdot (-1) = -5 \equiv 8$

$x_3 = s^2 - x_1 - x_2 = 64 - 2 - 1 = 61 = 9$

$y_3 = s \cdot (x_1 - x_3) - y_1 = 8 \cdot (-7) - 6 = -56 - 6 = -62 = 3$

The final result is $A + B = (x_3, y_3) = (9, 3)$.

Question 12: **(3 Points)**

Complete the following code snippet to scalar-multiply the point with a (positive) integer scalar number k.

```
class Point:

    def __init__(self, x, y, a, b):
        self.a = a
        self.b = b
        self.x = x
        self.y = y

    def __rmul__(self, k):
        result = self.__class__(self.x, self.y, self.a, self.b)
        for i in range(k - 1):

            ____result = result + self___ # Write your code in the blank.
        return result
```

`result += self.` is also correct.

Question 13 (ECDSA): **(9 Points)**

The Elliptic Curve Digital Signature Algorithm is a digital signature scheme that leverages the difficulty of the discrete logarithm problem for elliptic curve points over finite fields, which we studied in class.

a) Let k be a secret private nonce, m the message to be signed, e the private key, r the public nonce, s the signature and G the generator point. For ECDSA as used in Bitcoin, write down the steps that are being computed by the *signing function* of ECDSA.

b) Alice accidentally revealed the secret private nonce k to Bob, who has received the output (r, s) from the signing function of ECDSA, as well as the message m. Bob plans to steal Alice's funds by cracking her private key e using k, r, s, and m. Explain how Bob is able to derive the private key e using the information he possesses.

a) The key steps are the following ones.

- Compute $R = k \cdot G$,
- Define r as the x-coordinate of the elliptic curve point R,
- Compute $z = \text{hash}(m)$ (where $\text{hash}(\cdot)$ is the twice application of the SHA-256 cryptographic hash function),
- Compute $s = (z + r \cdot e) \cdot k^{-1} \bmod n$, where n is the order of the group generated by the generator point G.
- Return (r, s).

b) In the signing function of ECDSA, the signature s is being calculated as

$$s = (z + re)k^{-1} \bmod n$$

where $z = \text{hash}(m)$. After multiplying both sides with $k \bmod n$, we obtain

$$ks = \text{hash}(m) + re \bmod n.$$

Solving this for e results in

$$e = (ks - \text{hash}(m))r^{-1} \bmod n,$$

which contains only quantities that we have access to.

Question 14: **(3 Points)**

Below code verifies the Schnorr signature s for the message `m`, given the public nonce `R` and the public key `P`. **Fill in the blanks to complete the function** $schnorrverify(P, m, s, R)$**.** (Hint: You have also access to the generator point `G` of the elliptic curve, which generates the generator group that is of order `n`.)

```
def schnorrverify(P, m, s, R):
  P_xonly = P.x.num.to_bytes(32, 'big')
  R_xonly = R.x.num.to_bytes(32, 'big')
  m = m.encode()
  z = int.from_bytes(sha256(sha256(R_xonly + P_xonly + m)), 'big') % n

  target = ___R + z  P_____

  return target == _____s G_____________
```

It is also possible to set target $= s \cdot G$ and then target$== R + z \cdot P$.

Question 15 (Choose one): **(2 Points)**

Chaumian e-cash comes with essentially ideal privacy for...

a) the sender
b) the recipient
c) neither the sender nor recipient
d) both the sender and the recipient

of the digital coin.

Question 16 (True or False): **(2 Points)**

It is impossible to trace back the sender of a Bitcoin transaction more than one step as blind signatures are being used in the Bitcoin protocol.

a) True
b) False

Question 17 (Short Essay): **(10 Points)**

Provide at least **three different arguments for** or **against** the claim:

"Economic systems tend to converge on a single form of money."

Substantiate your arguments based on socioeconomic or historical data or based on the works of some of the authors we discussed in class.
Hint: You can also provide some arguments for and some against.

Possible arguments in favor of the claim:

- The set or group of individuals using the same form of money can be considered as a monetary network, as exchange of goods between these individuals is facilitated through a

common medium of exchange, and as pricing of goods is facilitated due to a common unit of account. The value of the money increases as the number of participants increases as more opportunities of trade emerge. The resulting increase of the network size might only cease once an entire economic system has adopted this form of money as their money, at which point the system has converged to a single form of money. This is the main argument made in the article "Bitcoin Obsoletes All Other Money" by Parker Lewis.

- Monetary goods satisfy different monetary properties (such as scarcity, fungibility, divisibility etc.) to a different degree. The monetary properties inform the appropriateness of a good to satisfy the main monetary functions. Since the vast majority of the monetary properties are not context or location dependent, but objective, it would be rational for individuals across the entire economic system to come to the same conclusion as of which monetary good is most rational to adopt. As a result, the entire economic system might converge to use the same form of money. This line of thinking is behind the argument of the articles in the series "The Bullish Case for Bitcoin" by Vijay Boyapati, but also the gist of the argument made in the article "Bitcoin Obsoletes All Other Money" by Parker Lewis as of why Bitcoin is the single form of money that societies will converge to.

- In the 19th century, most major powers and countries gradually adopted the gold standard as the underlying principle of their monetary system. Coincidentally, or as a result, global trade flourished. This can be seen as historical evidence for the fact that different economies benefit if a common monetary system is used.

- The fact that governments have the ability to set regulations (such as legal tender laws and taxation laws) that strongly favor a certain forms of money over others is a socioeconomic reality. Typically, these regulations are set to favor only one type of money. As a result, entire economies often use only one form of money for most of their use cases (such as the US dollar in the United States).

- Friedrich Hayek's "Denationalisation of Money: The Argument Refined" introduces the idea that allowing competitive, privately issued monies can lead to market-driven efficiency. According to Hayek, when multiple currencies compete, the best-performing currency,Äîby virtue of its superior properties such as stability, low transaction costs, and broad acceptability,Äîwill eventually prevail. While Hayek did not explicitly claim that this process would result in a single form of money, his theory implies that economic rationality and market competition naturally favor convergence on the currency that best meets the needs of the majority. In a dynamic global market, even minor advantages can lead to significant long-term shifts, steering the system towards a dominant monetary form.

Possible arguments against the claim:

- There are different functions of money that different forms of money might fulfill to a different degree. For example, it could be that a certain form of money (e.g., gold or Bitcoin) excels as being a store of value, whereas another form of money is more efficient as medium of exchange (US dollar). This quite accurately describes the current socioeconomic reality in the United States economy.

- The system of competitive, privately issued monies in Friedrich Hayek's "Denationalisation of Money: The Argument Refined" could be also interpreted as a viable setup that does not lead to the convergence of usage of one form of money, as the competition between the money issuers will always allow currently less favored forms of money to re-emerge by innovation. As none of the money issuers can be completely trusted to manage their money

type perfectly, it might be rational risk management to diversify across forms of money from an individual point of view.

- The modern world economy can be considered as a common economic system. We observe that different countries use different forms of money (e.g., China uses the Yuan, the U.S. uses the US dollar). This might not change in the future as each country's government benefits from the right to issue their own money through central banking.