

# Zero-Knowledge Protocols

Abhabongse Janthong  
สถาพงศ์ จันทรทอง  
Associate Visionary Architect, KBTG

# Zero-Knowledge Protocols

**HOW TO ACHIEVE A  
COMMUNICATION  
GOAL WITHOUT  
LEAKING JUST  
ANYTHING?**

Abhabongse Janthong

สถาพงศ์ จันทรทอง

Associate Visionary Architect, KBTG

# Zero-Knowledge Protocols

ต้องการสื่อสารเพื่อบรรลุ  
เป้าหมายบางอย่างโดยไม่  
เปิดเผยอะไรนอก  
เหนือจากที่จำเป็น

Abhabongse Janthong  
อาภาพงศ์ จันทรทอง  
Associate Visionary Architect, KBTG

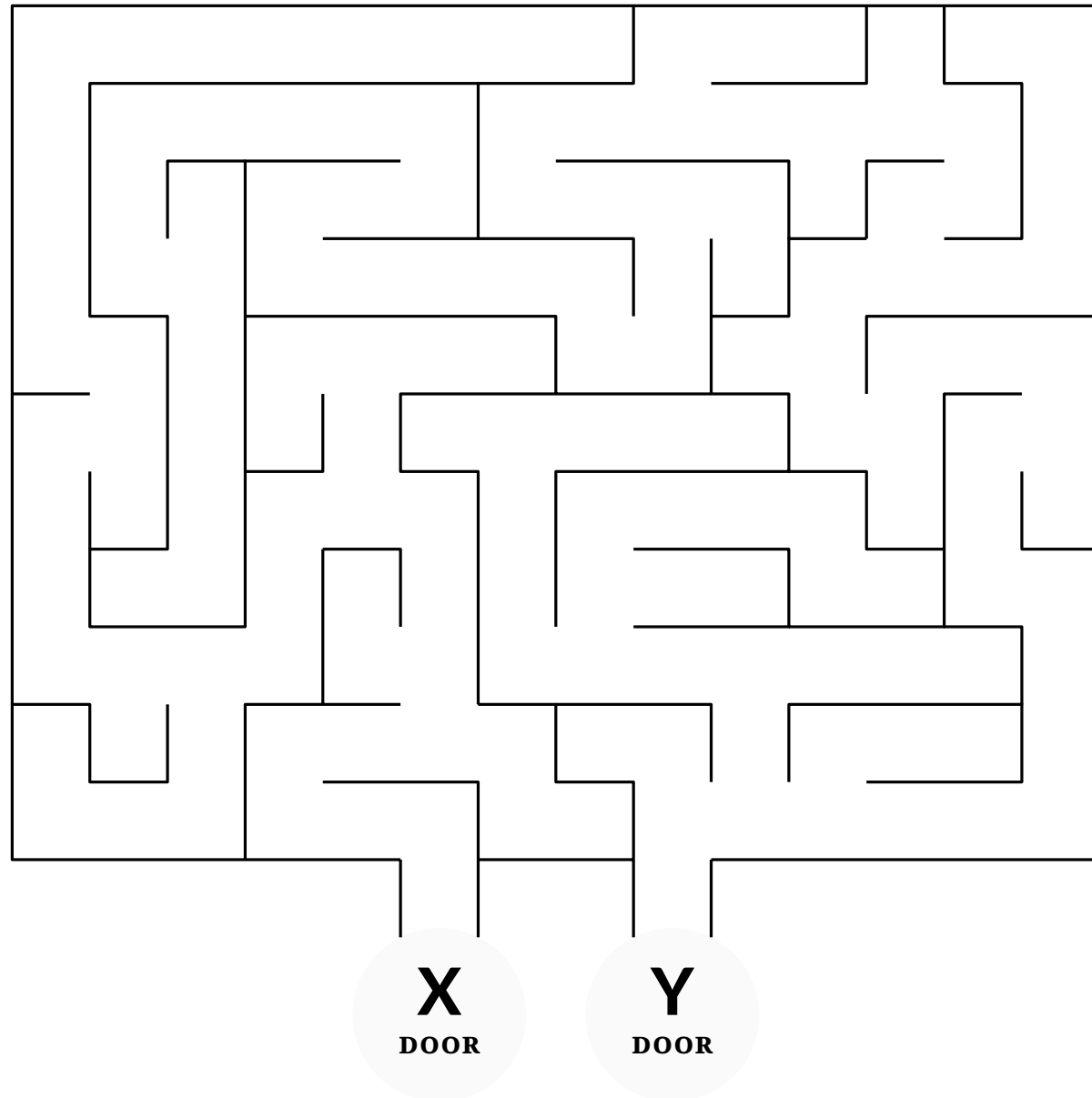


**Act I**

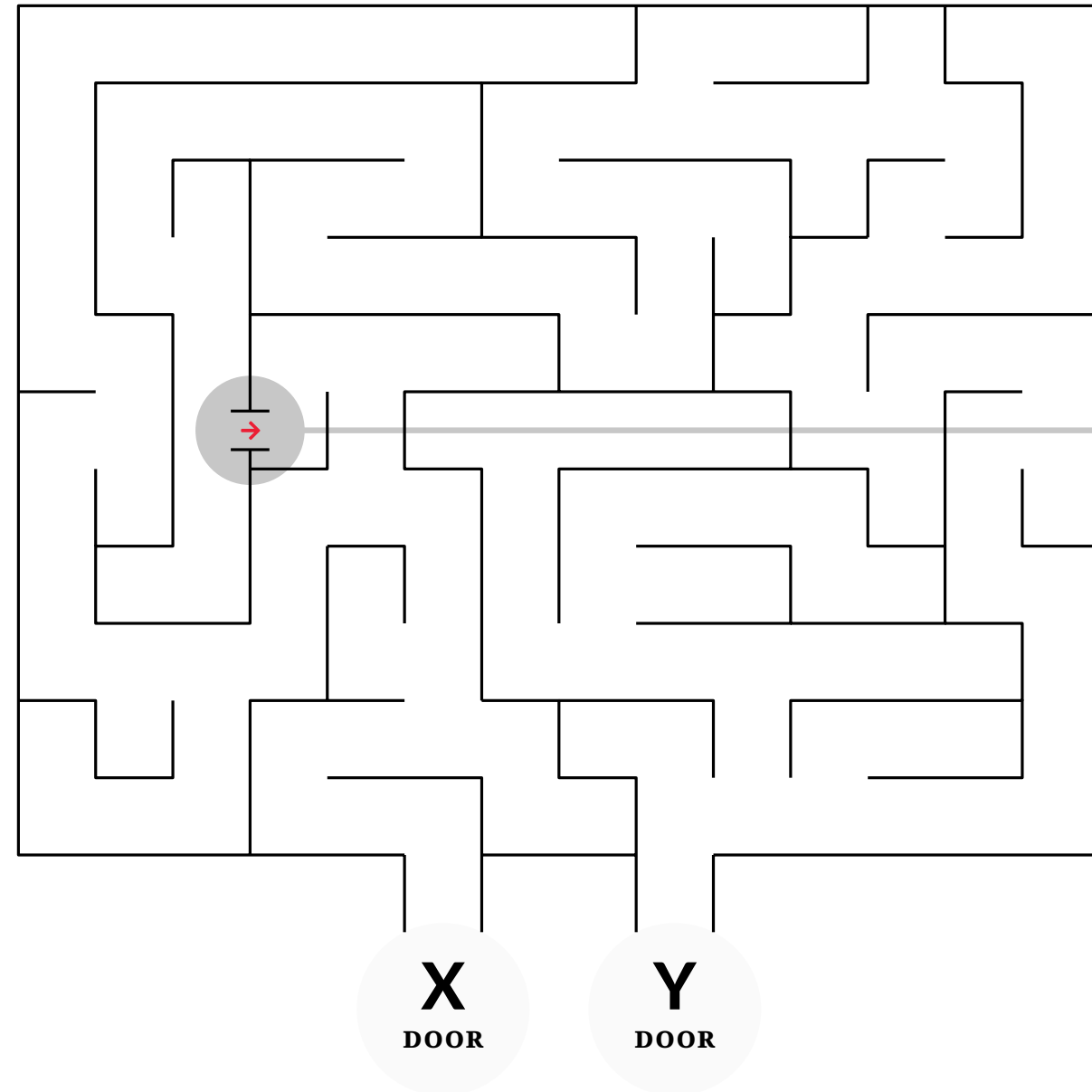
# **IN – DEPTH TECHNICAL DEMO**

# เขาวงกต ► โจทย์

เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง



# เขาวงกต ► โจทย์



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

# เขาวงกต ► โจทย์



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

**Alice** ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

# เขาวงกต ► โจทย์



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

**Alice** ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!



# เขาวงกต ► โจทย์



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

**Alice** ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

# เขาวงกต ► โจทย์



**Alice** ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

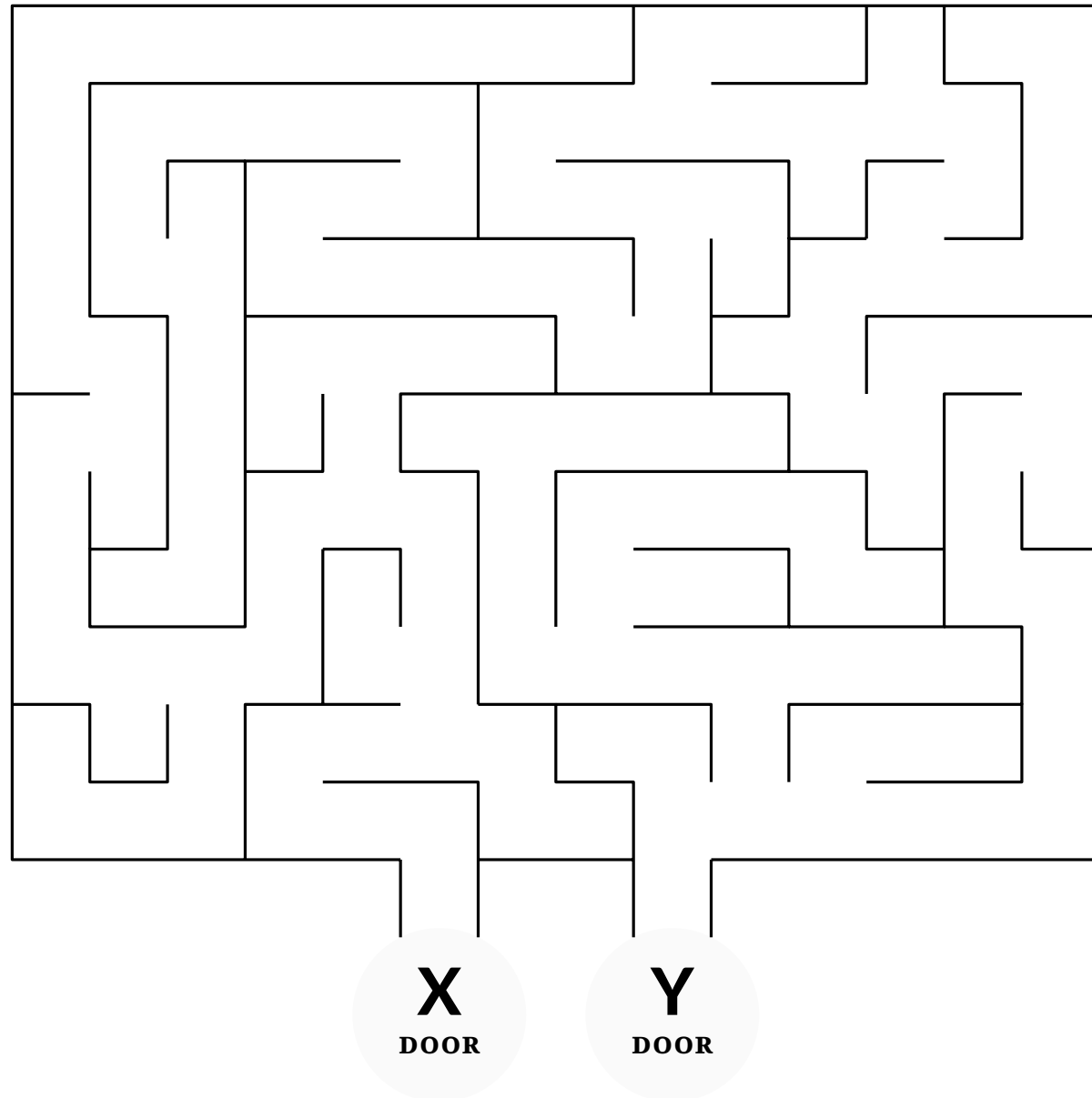
ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

# เขาวงกต ► โจทย์



**Alice** ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

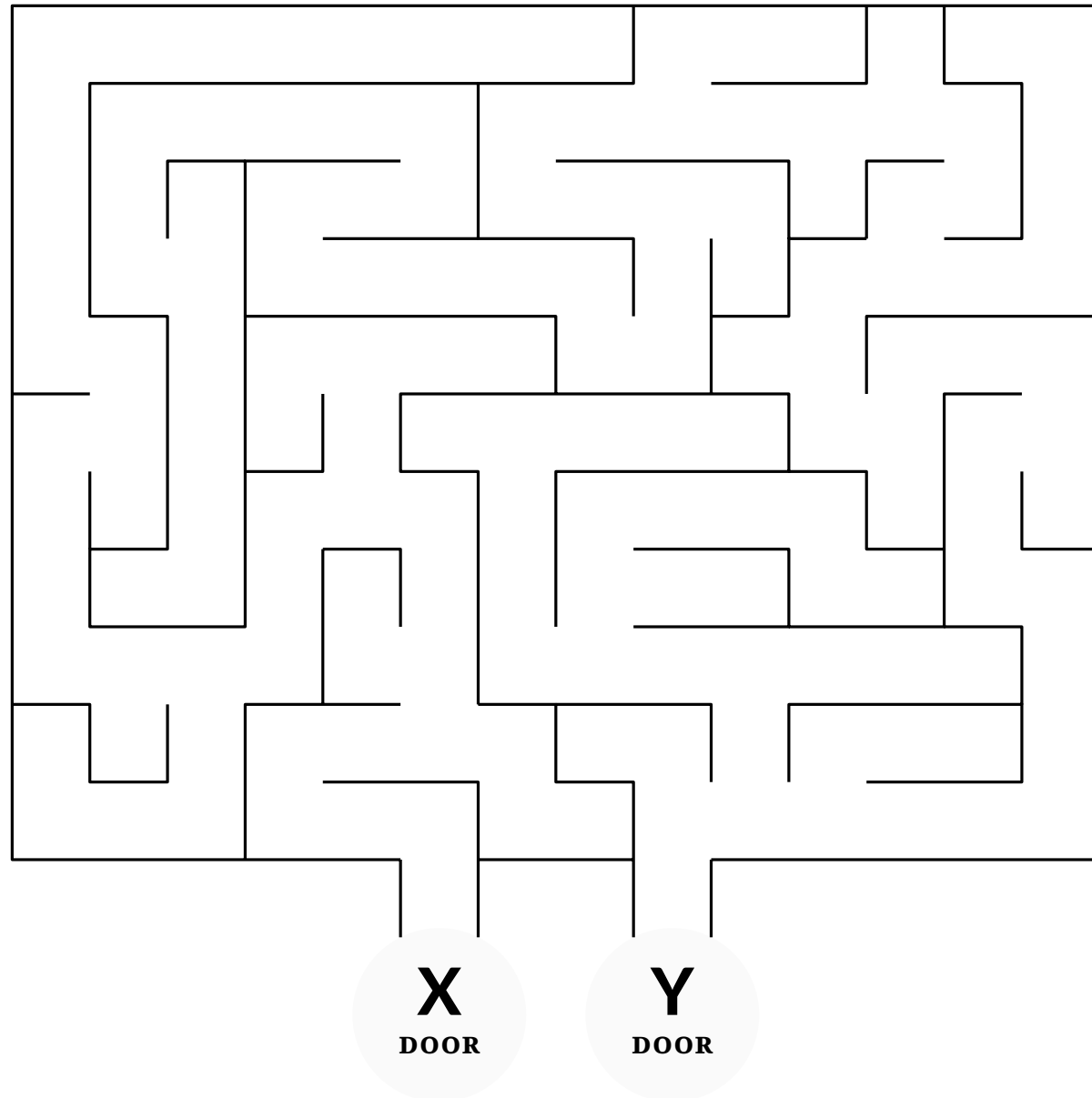
เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :( จะเอาไง

# เขาวงกต ► โจทย์



**Alice** ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

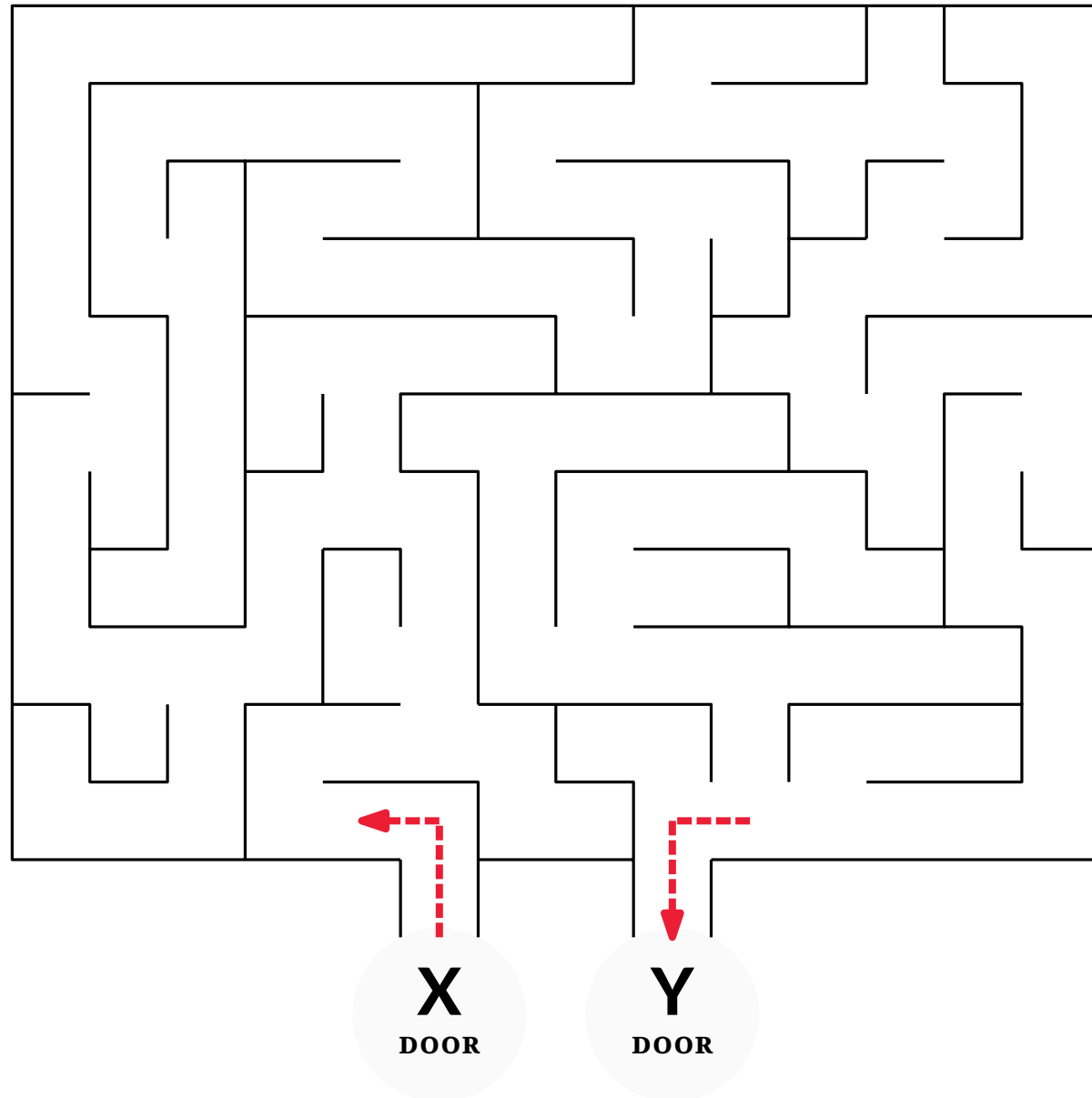
มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :( จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

# เขาวงกต ► โจทย์



ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

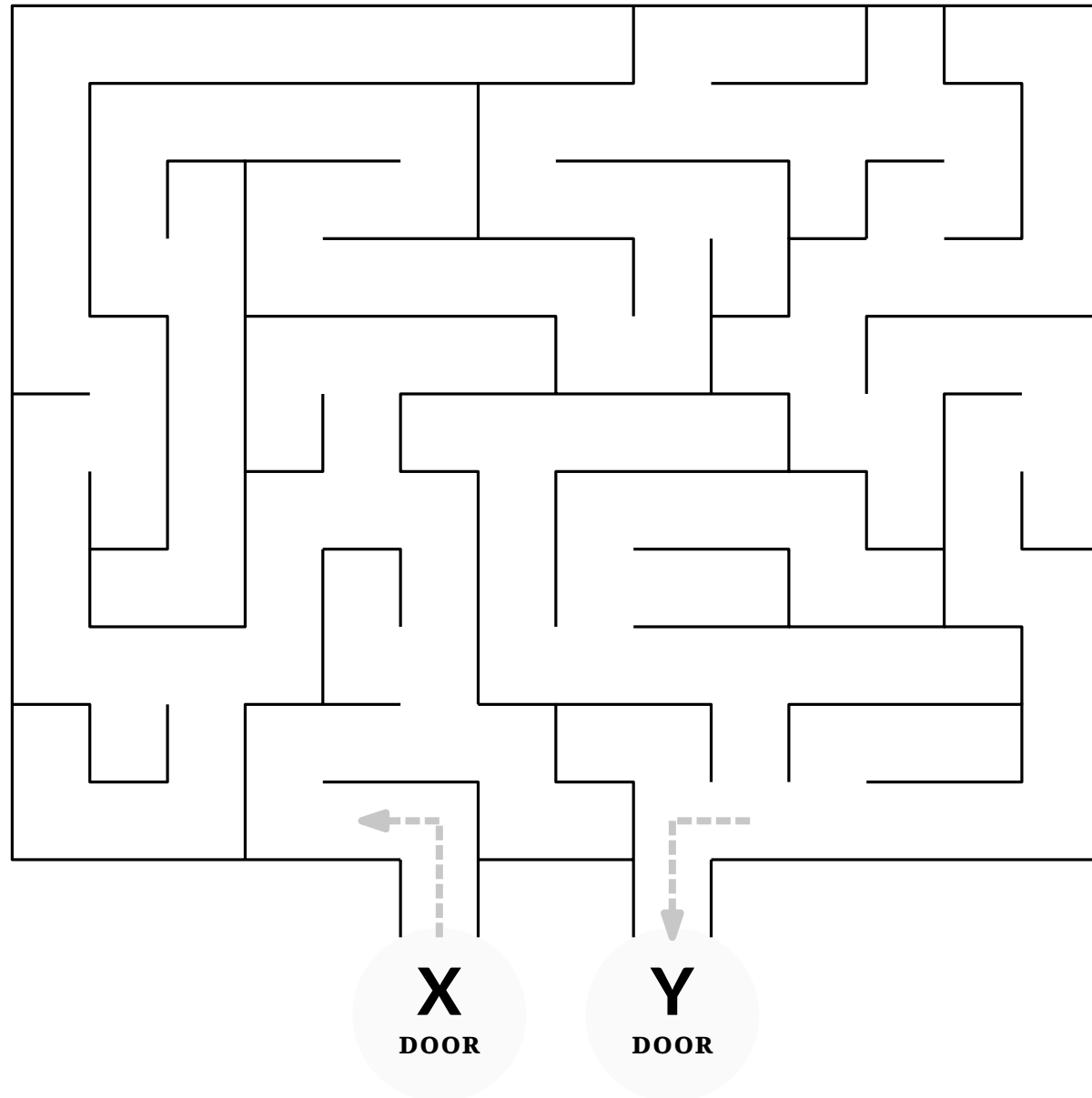
ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :( จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น  
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

# เขาวงกต ► โจทย์



เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

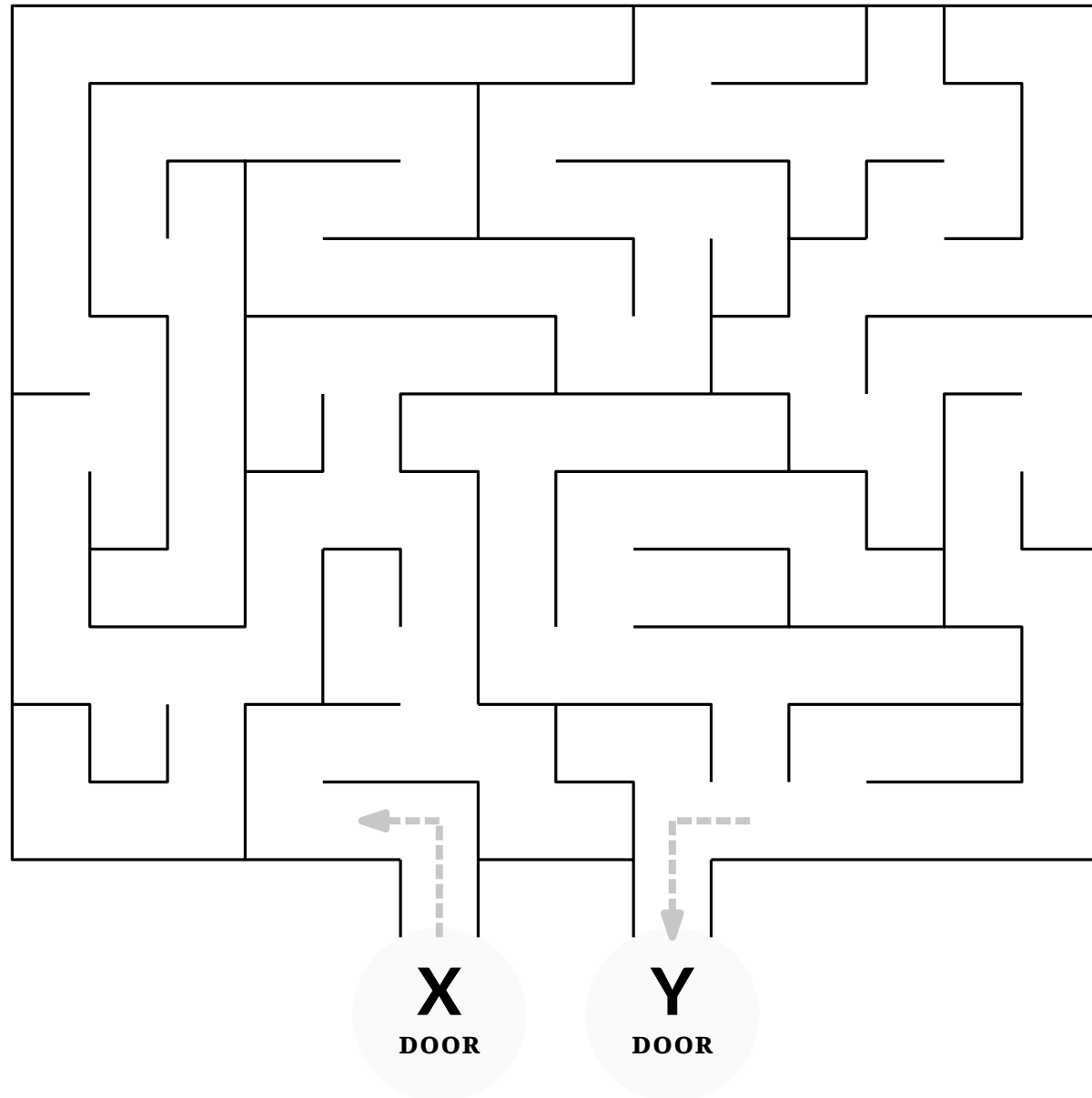
เธอนี้เรื่องมากจังนะ :( จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น  
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

# เขาวงกต ► โจทย์



มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :( จะเอาไง

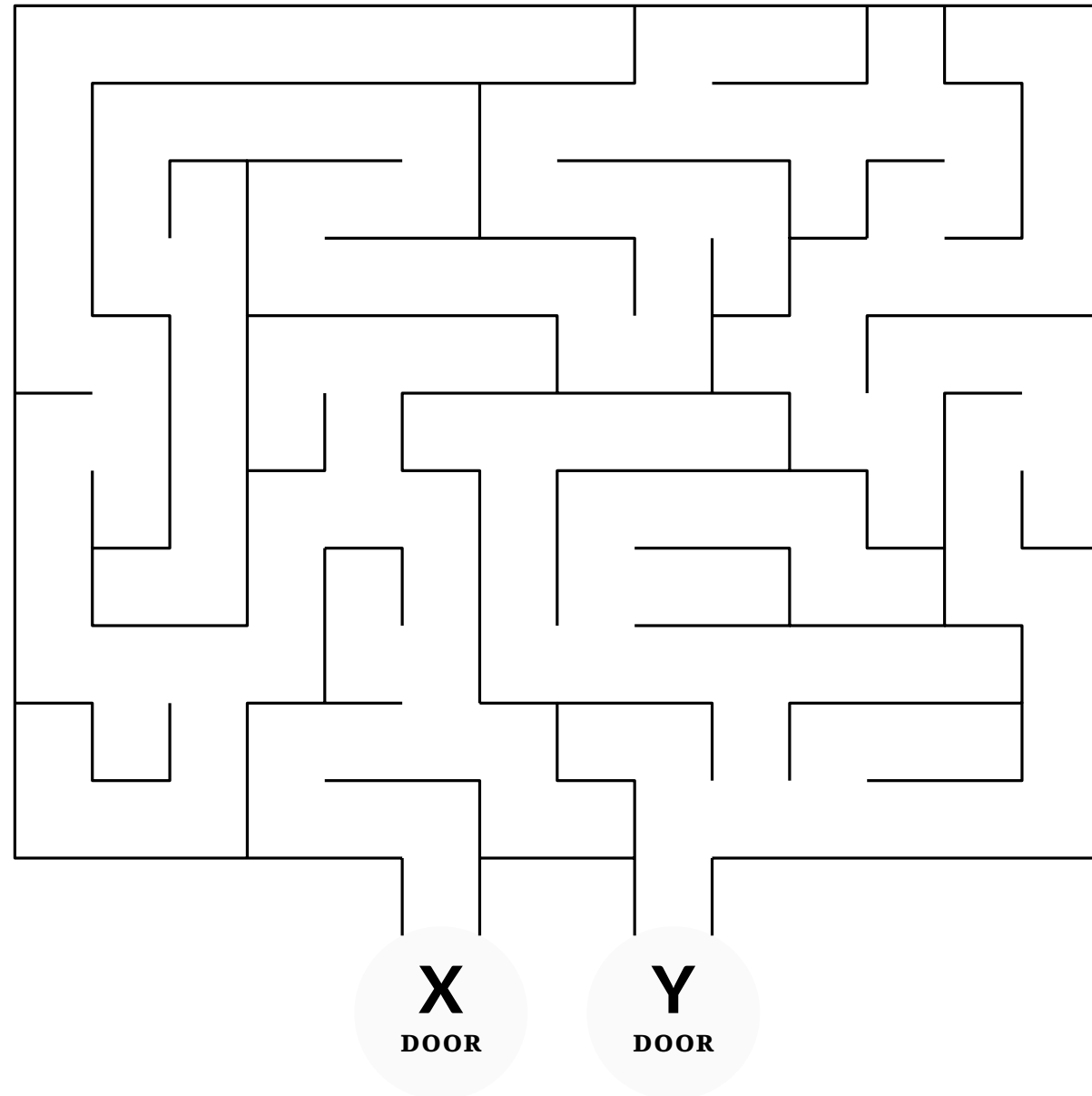
จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น  
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้นะสิ

... ว่ามีทางเข้า-ออกเขาวงกต ที่ต้องเข้าจาก  
ประตู **X** แล้วออกทางประตู **Y**

# เขาวงกต ► โจทย์



ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :( จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น  
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หะสิ

... ว่ามีทางเข้า-ออกเขาวงกต ที่ต้องเข้าจาก  
ประตู **X** แล้วออกทางประตู **Y**



เธอไม่ควรรู้ด้วยซ้ำว่ามีเส้นทางแบบนั้น  
มันก็คือสปอยล์รูปแบบหนึ่งนะ



# Zero-Knowledge Proof

# Zero-Knowledge Proof

เป้าหมายการสื่อสาร    พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

# Zero – Knowledge Proof

เป้าหมายการสื่อสาร

พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข

ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดนอกเหนือจากข้อเท็จจริงถูกต้อง

# Zero – Knowledge Proof

เป้าหมายการสื่อสาร      พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข      ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดนอกเหนือจากข้อเท็จจริงถูกต้อง

เช่น      พิสูจน์ว่า บางปัญหามีคำตอบ แต่ ไม่บอกคำตอบ ✓

# Zero – Knowledge Proof

เป้าหมายการสื่อสาร      พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข      ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดนอกเหนือจากข้อเท็จจริงถูกต้อง

เช่น      พิสูจน์ว่า บางปัญหามีคำตอบ แต่ ไม่บอกคำตอบ ✓

            พิสูจน์ว่า ฉันอายุ 18 ปีขึ้นไป แต่ ไม่บอกวันเดือนปีเกิด 📅

# Zero – Knowledge Proof

เป้าหมายการสื่อสาร      พิสูจน์ข้อเท็จจริงบางอย่างให้อีกฝ่ายทราบ

เงื่อนไข      ผู้ฟังต้องไม่เรียนรู้สิ่งอื่นใดนอกเหนือจากข้อเท็จจริงถูกต้อง

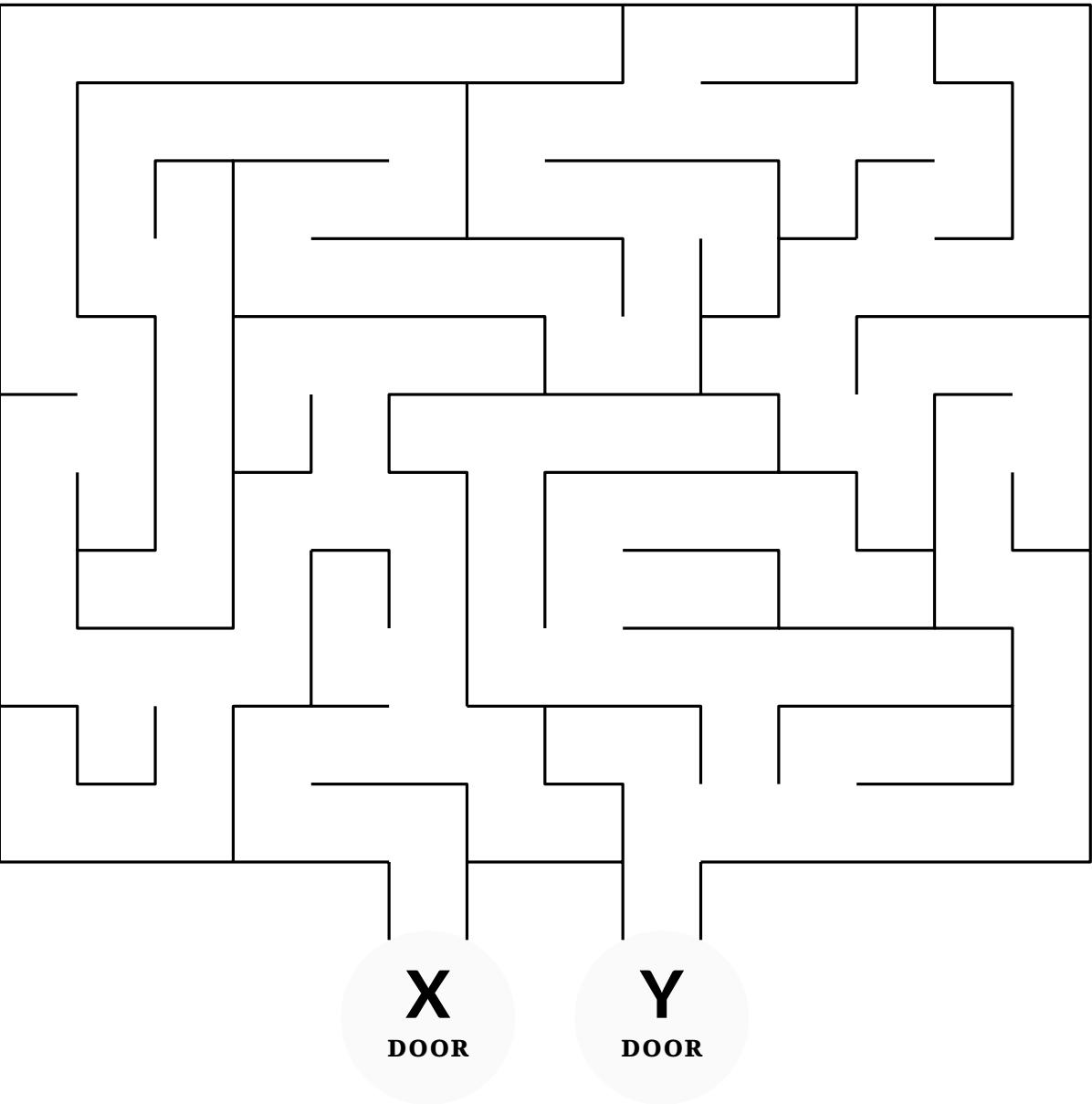
เช่น      พิสูจน์ว่า บางปัญหามีคำตอบ แต่ ไม่บอกคำตอบ ✓

พิสูจน์ว่า ฉันอายุ 18 ปีขึ้นไป แต่ ไม่บอกวันเดือนปีเกิด 📅

พิสูจน์ว่า ฉันมีสิทธิเข้าถึงข้อมูล แต่ ไม่บอก credentials / secret key 🔑

~~พิสูจน์ว่า บางปัญหาแก้ไขได้ แต่ ไม่บอกวิธีแก้ไข~~ 😞

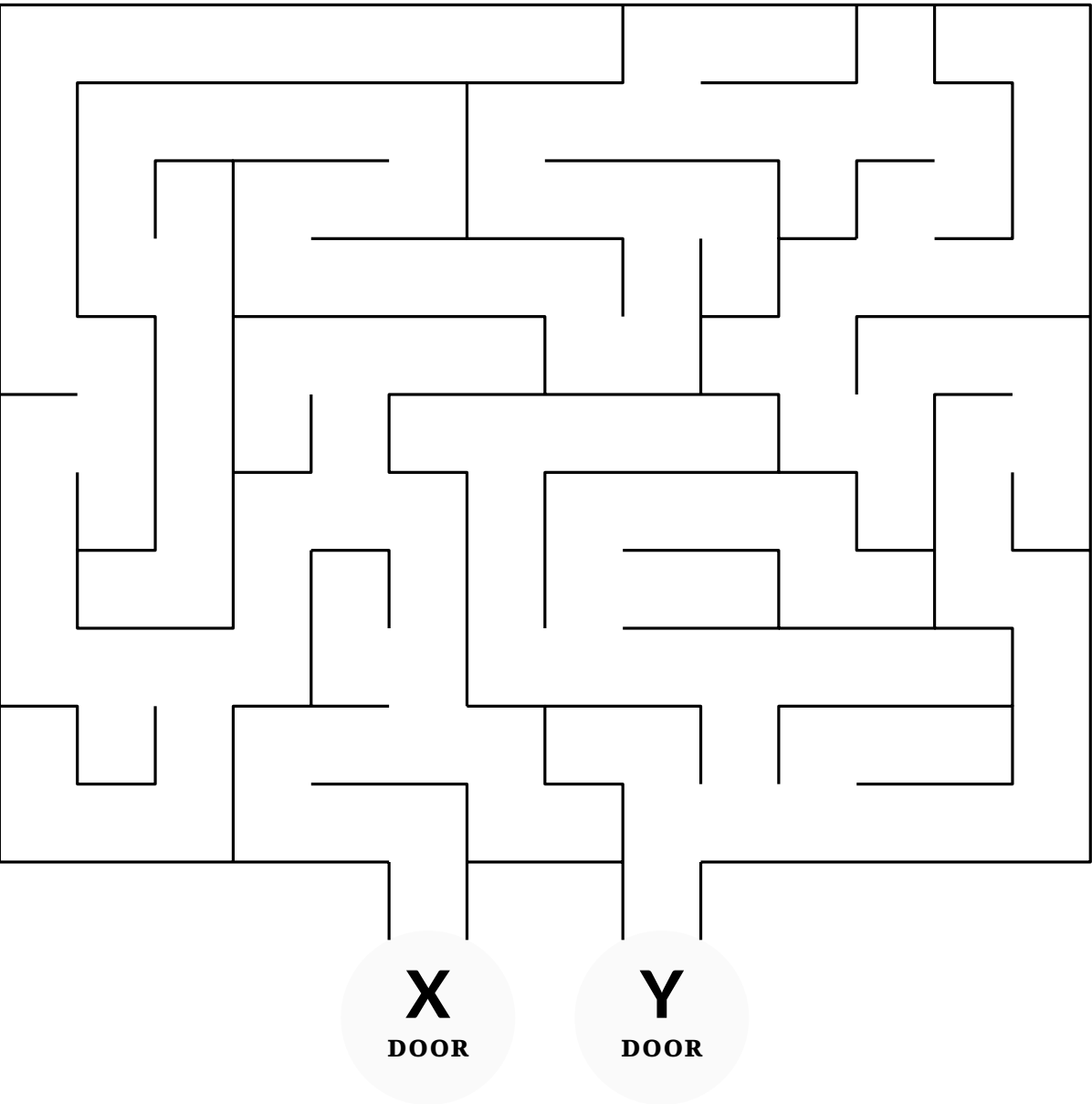
เขาวงกต ► วิธีแก้ปัญห



Alice ผู้พิสูจน์

ผู้ตรวจสอบ Bob

# เขาวงกต ► วิธีแก้ปัญห



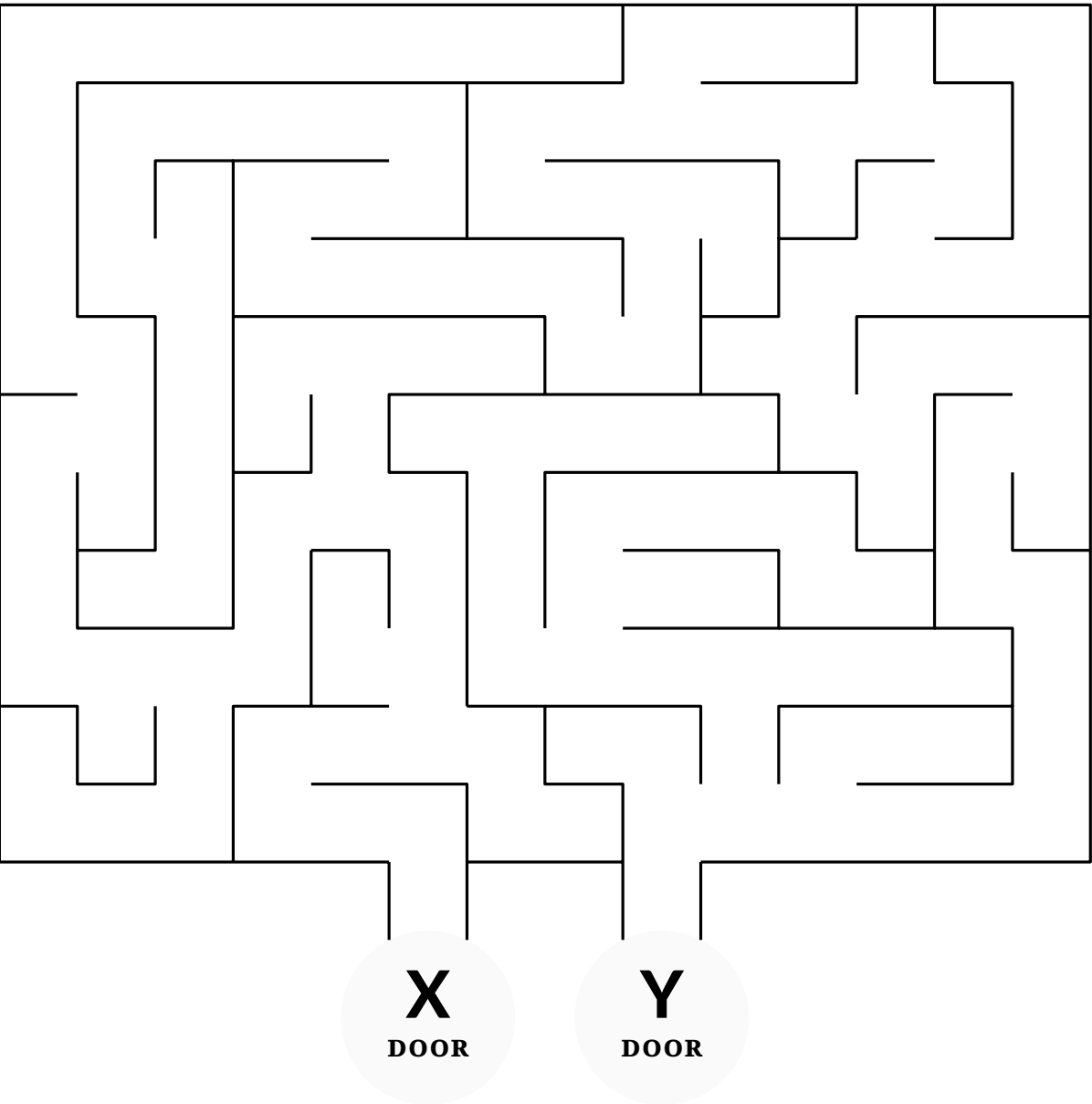
Alice ผู้พิสูจน์

ผู้ตรวจสอบ Bob

เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน  
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น  
(2) เดินฉันจะเดินออกมาให้เธอดู



# เขาวงกต ► วิธีแก้ปัญห



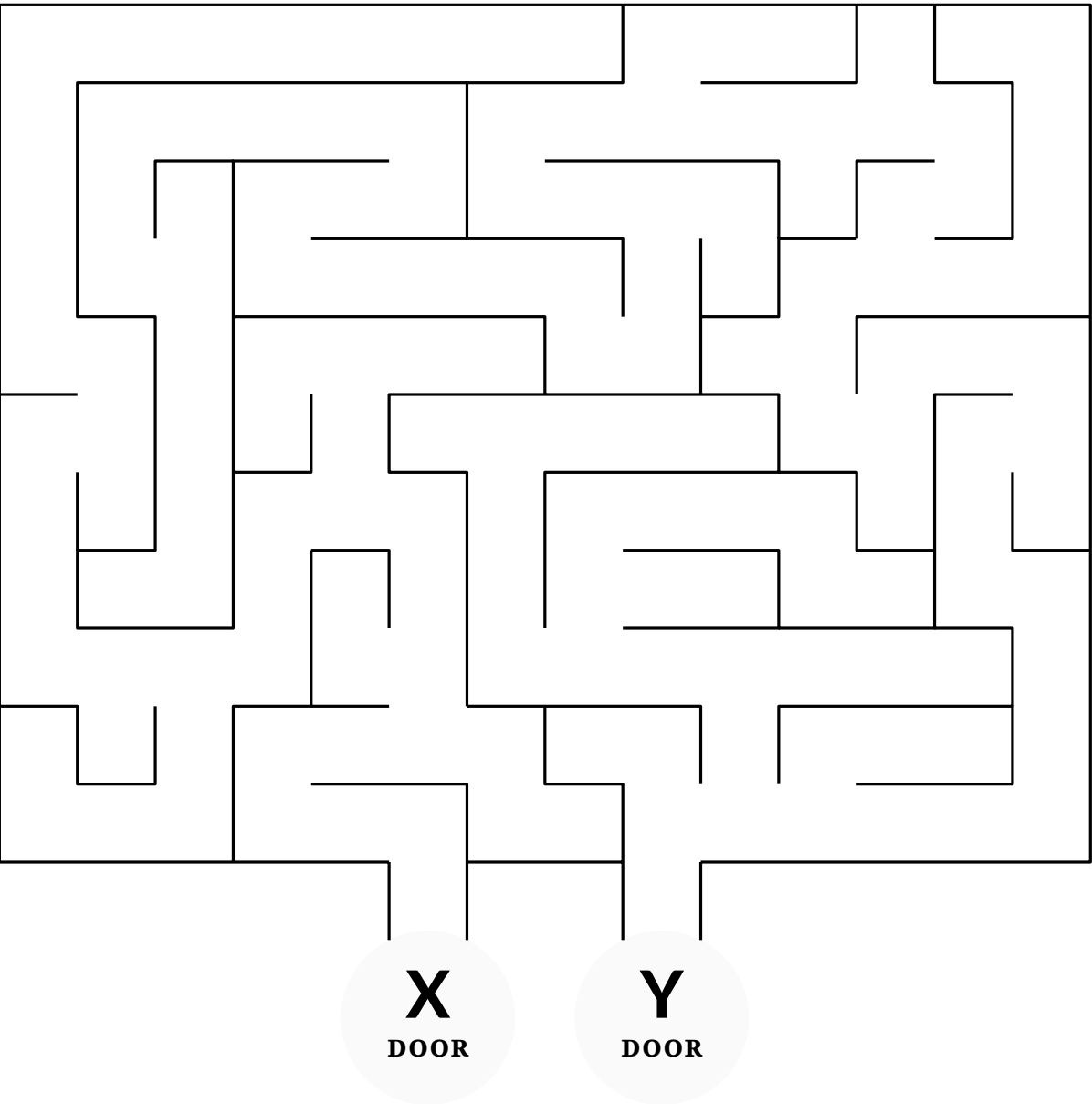
**Alice** ผู้พิสูจน์

ผู้ตรวจสอบ **Bob**

เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน  
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น  
(2) เดินฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

# เขาวงกต ► วิธีแก้ปัญห



Alice ผู้พิสูจน์

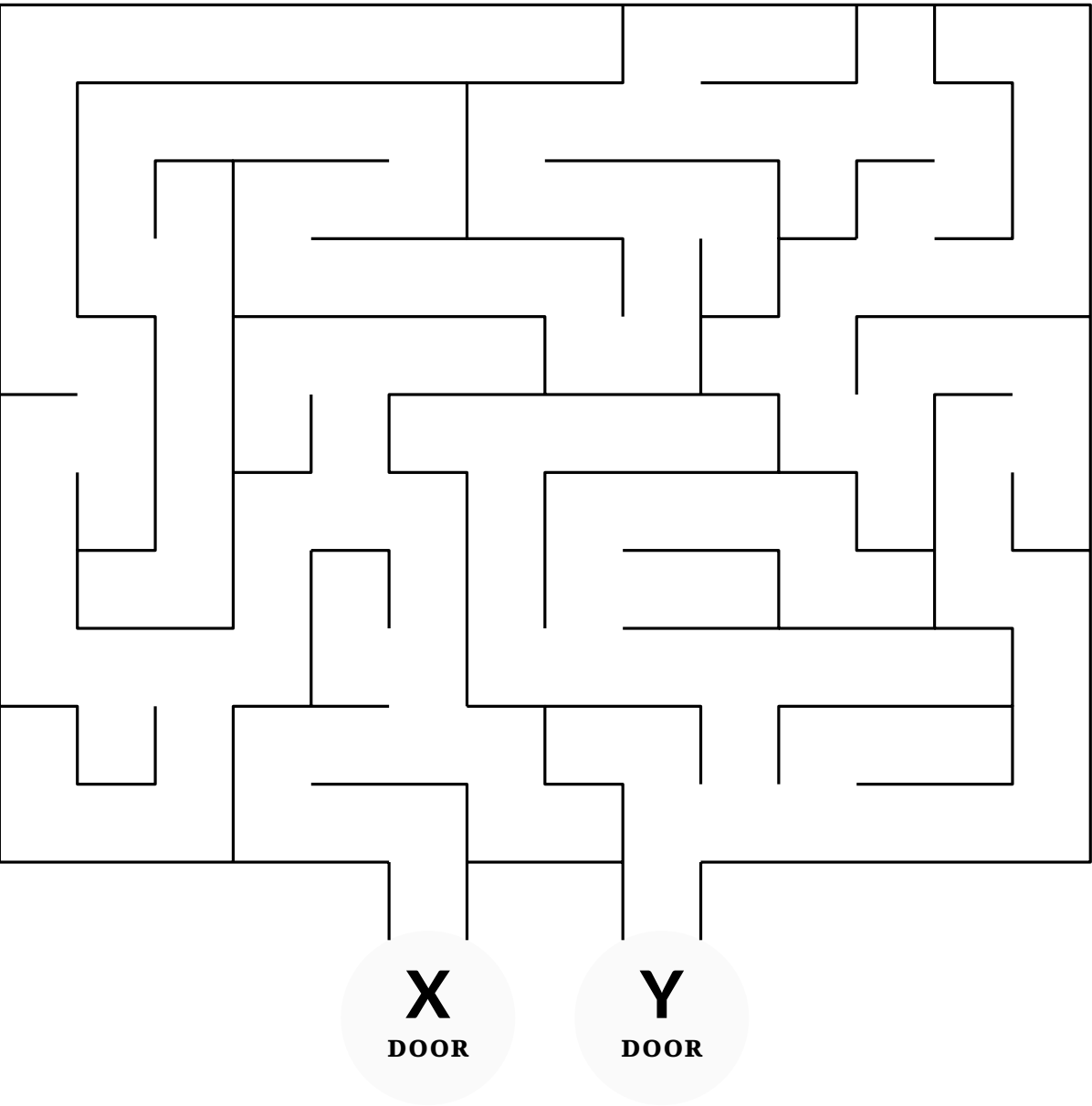
ผู้ตรวจสอบ Bob

เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน  
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น  
(2) เดินฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

อ้าว! แล้วแบบนี้จะรู้ได้ไงว่าแกไม่ได้กลับ  
ออกมาทางเดิมที่แกเดินเข้าไป

# เขาวงกต ► วิธีแก้ปัญห



Alice ผู้พิสูจน์

ผู้ตรวจสอบ Bob

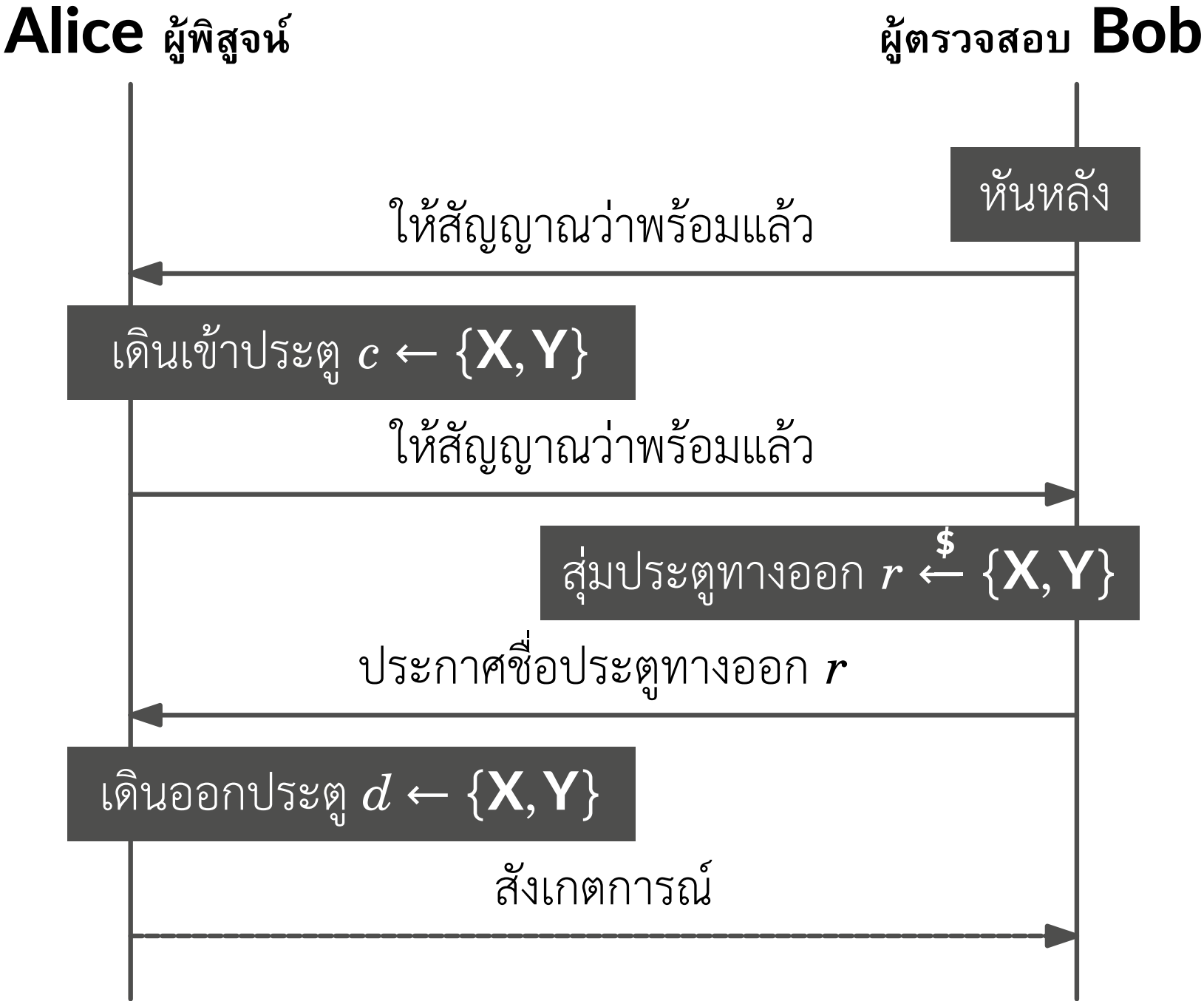
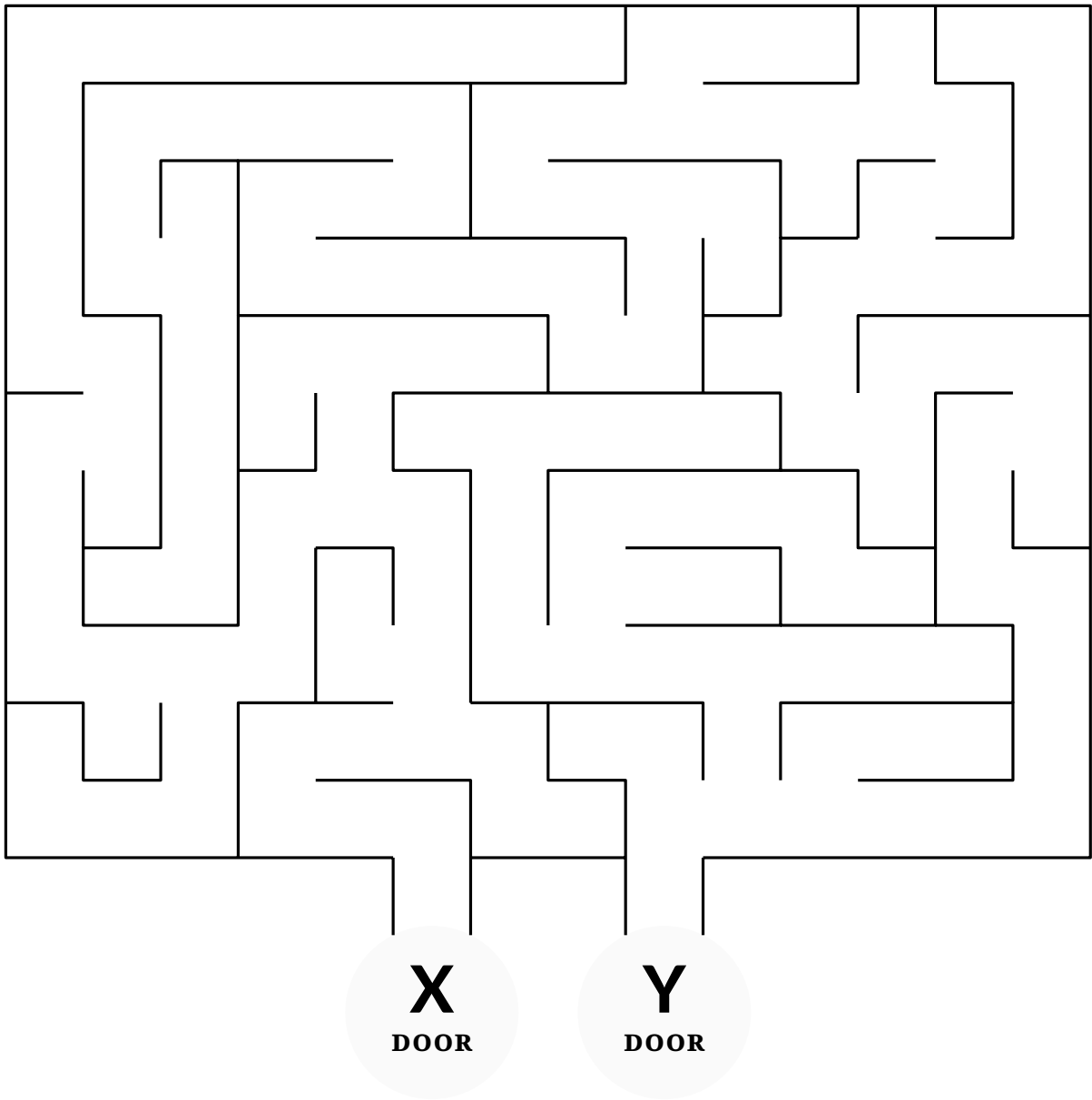
เอาอย่างนี้แล้วกัน (1) เดินเธอหันหลังก่อน  
แล้วฉันจะเดินเข้าไปเตรียมตัวข้างใน จากนั้น  
(2) เดินฉันจะเดินออกมาให้เธอดู

ทำแบบนี้แล้วเธอก็ไม่รู้ว่าฉันเดินเข้าประตูไหน

อ้าว! แล้วแบบนี้จะรู้ได้ไงว่าแกไม่ได้กลับ  
ออกมาทางเดิมที่แกเดินเข้าไป

เธอก็สุ่มสิว่าจะให้ฉันเดินออกทางประตูไหน  
ถ้าฉันรู้วิธีแก้เขาวงกต ฉันจะเดินออกประตู  
ไหนก็ได้ / แต่ถ้าฉันไม่รู้ ฉันต้องเดาใจเธอไง

# เขาวงกต ► วิธีแก้ปัญห



# **THE HEART OF Zero-Knowledge Proof**

# THE HEART OF Zero-Knowledge Proof

## COMPLETENESS

---

ถ้า **Alice** ทราบคำตอบจริง

แล้ว **Alice** สามารถพิสูจน์ว่า  
ตนรู้จริงให้ **Bob** กระจ่างได้

# THE HEART OF Zero-Knowledge Proof

## COMPLETENESS

---

ถ้า **Alice** ทราบคำตอบจริง  
แล้ว **Alice** สามารถพิสูจน์ว่า  
ตนรู้จริงให้ **Bob** กระจ่างได้

## SOUNDNESS

---

ถ้า **Alice** ไม่ทราบคำตอบ  
แล้ว **Alice** ไม่สามารถหลอก  
ให้ **Bob** เชื่อคล้อยตามได้

# THE HEART OF Zero-Knowledge Proof

## COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง  
แล้ว **Alice** สามารถพิสูจน์ว่า  
ตนรู้จริงให้ **Bob** กระจ่างได้

## SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ  
แล้ว **Alice** ไม่สามารถหลอก  
ให้ **Bob** เชื่อคล้อยตามได้

## ZERO-KNOWLEDGE

ถ้า **Alice** ทราบคำตอบจริง  
แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใด  
จาก **Alice** เว้นเฉพาะสิ่งที่  
**Bob** คาดเดาได้ด้วยตัวเอง



# THE HEART OF Zero-Knowledge Proof

## COMPLETENESS

ถ้า **Alice** ทราบคำตอบจริง  
แล้ว **Alice** สามารถพิสูจน์ว่า  
ตนรู้จริงให้ **Bob** กระจ่างได้

*\*ด้วยความน่าจะเป็นที่สูงมาก ๆ*

CORRECTNESS PROPERTY

## SOUNDNESS

ถ้า **Alice** ไม่ทราบคำตอบ  
แล้ว **Alice** ไม่สามารถหลอก  
ให้ **Bob** เชื่อคล้อยตามได้

*\*ด้วยความน่าจะเป็นที่สูงมาก ๆ*

## ZERO-KNOWLEDGE

ถ้า **Alice** ทราบคำตอบจริง  
แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใด  
จาก **Alice** เว้นเฉพาะสิ่งที่  
**Bob** คาดเดาได้ด้วยตัวเอง

*\*ด้วยความน่าจะเป็นที่สูงมาก ๆ*

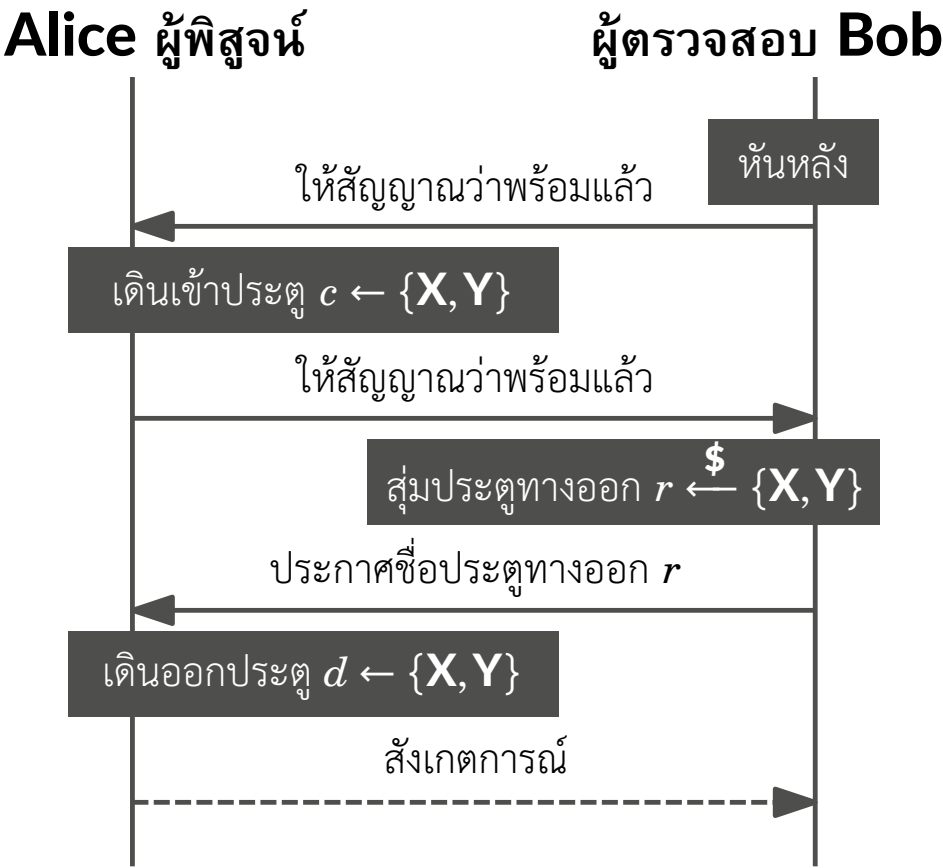
SECURITY PROPERTY

# เขาวงกต ► ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE

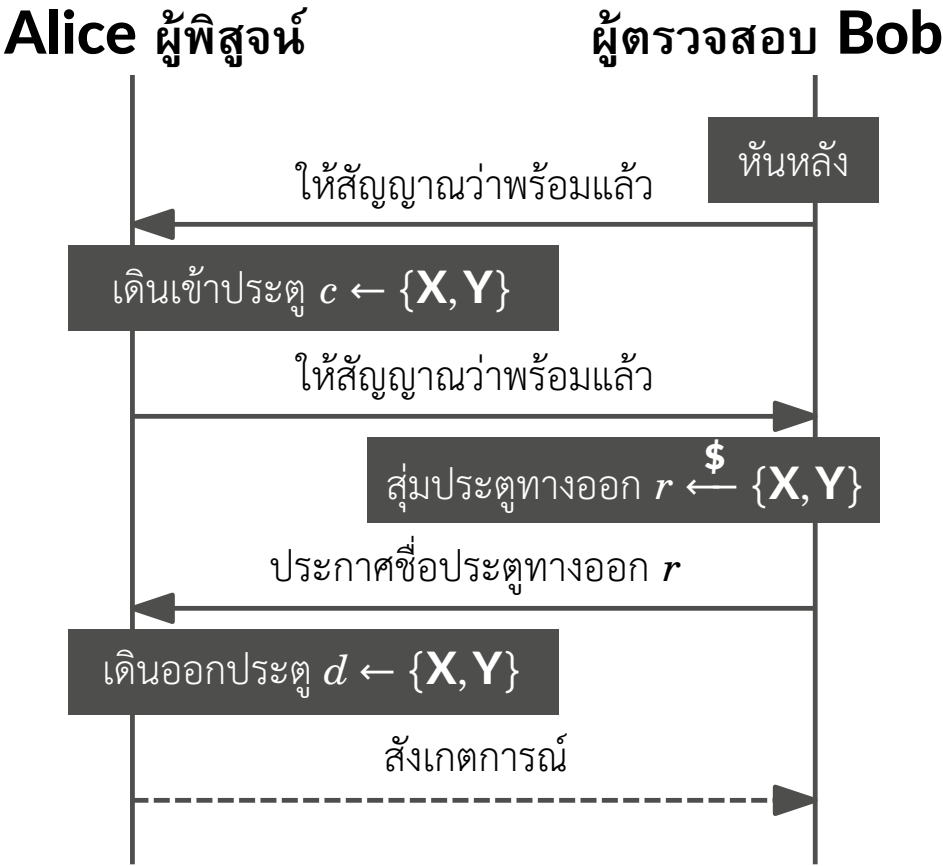


# เขาวงกต ► ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE



ถ้า **Alice** ทราบคำตอบจริง

(**Alice** รู้เส้นทางระหว่างประตูทั้งสอง)



**Alice** สามารถเลือกออกประตูไหนก็ได้



**Alice** สามารถเลือกออกประตูที่ **Bob** กำหนดให้ได้เสมอ

เพียงแค่เลือก  $d = r$



**Bob** เชื่อว่า **Alice** ทราบคำตอบจริง

(ด้วยความน่าจะเป็น เท่ากับ 100%)



แล้ว **Alice** สามารถพิสูจน์ว่าตนรู้จริงให้ **Bob** กระจ่างได้

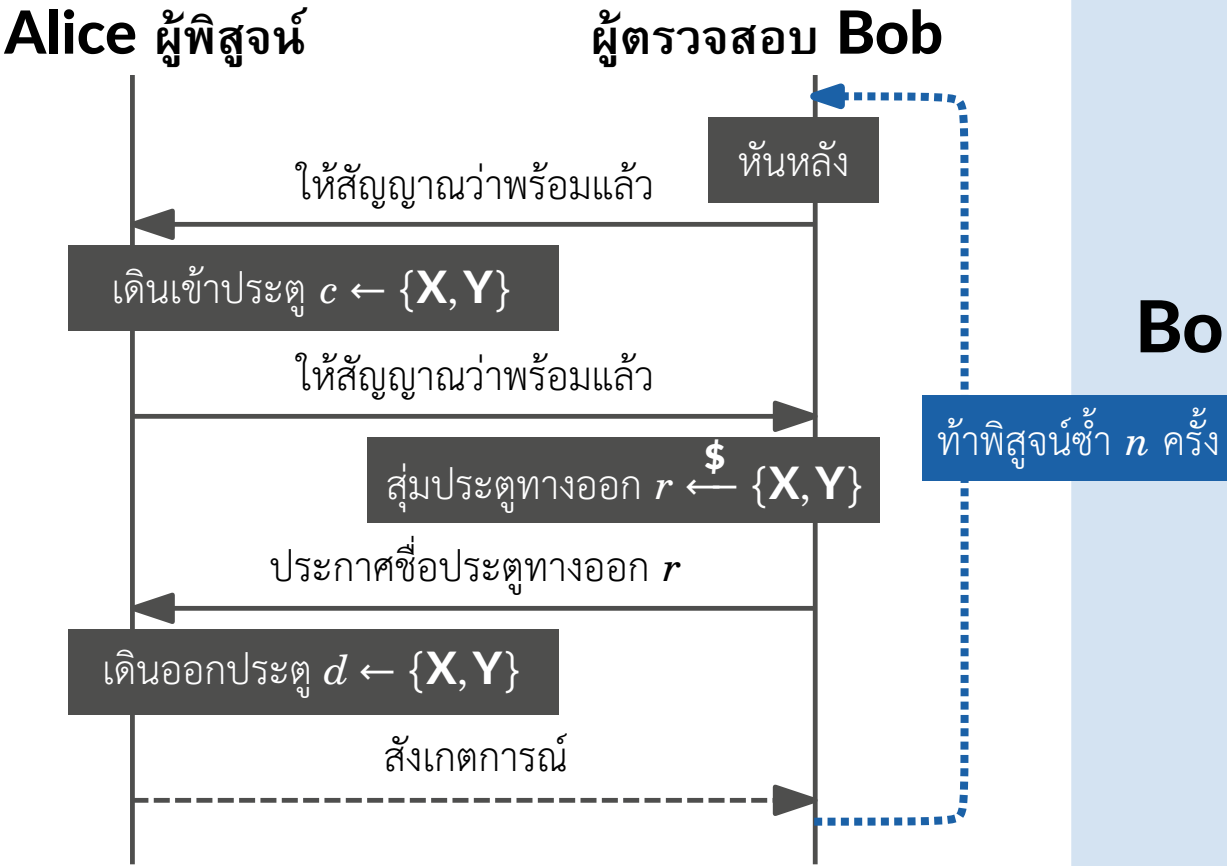
(ด้วยความน่าจะเป็น เท่ากับ 100%)

# เขาวงกต ► ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE



ถ้า Alice ไม่ทราบคำตอบ



Alice จำเป็นต้องออกทางประตูที่เข้ามา

นั่นคือบังคับเลือก  $d = c$



Alice ต้องเดาว่า Bob จะให้ออกประตูใด

โอกาสเดา  $c = r$  ถูกต้องเพียง 50% เปอร์เซนต์



Bob สามารถทำ Alice พิสูจน์ซ้ำได้หลายครั้ง เพื่อ(บางครั้ง)ถูกหลอก

โอกาสที่ Bob ถูกหลอกสำเร็จติดกันจะลดลง และความเชื่อมั่นก็จะมากขึ้น  
(เช่น ถ้าทดสอบ  $n = 20$  ครั้ง ความมั่นใจจะเพิ่มเป็น  $1 - 0.5^n \approx 99.999905\%$ )



แล้ว Alice ไม่สามารถหลอกให้ Bob เชื่อคล้อยตามได้

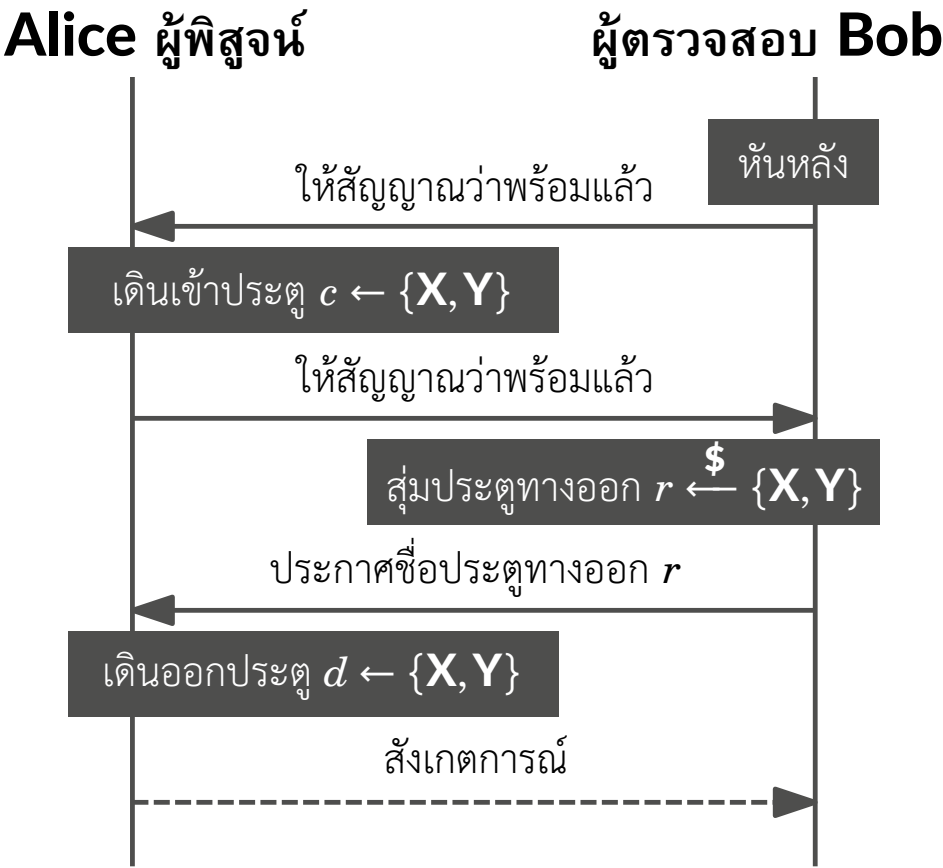
(ด้วยความน่าจะเป็น มากกว่า 99.99%)

# เขาวงกต ► ประเมินวิธีแก้ปัญหา

COMPLETENESS

SOUNDNESS

ZERO-KNOWLEDGE



ถ้า **Alice** ทราบคำตอบจริง  
(**Alice** รู้เส้นทางระหว่างประตูทั้งสอง)

**Alice** สามารถเลือกออกประตู  
ที่ **Bob** กำหนดให้ได้เสมอ

ถึงแม้สมมติ **Alice** ไม่อยู่  
**Bob** สามารถลองจินตนาการได้

**Bob** จะเห็นภาพ **Alice** เดินออกทางประตูที่ตนเรียกเสมอ

แล้ว **Bob** ไม่ได้เรียนรู้สิ่งใดจาก **Alice**  
เว้นเฉพาะสิ่งที่ **Bob** คาดเดาได้ด้วยตัวเอง

# ลายเซ็นดิจิทัล ► วิเคราะห์

## ข้อมูลเบื้องต้น

FIDO Alliance นำเสนอวิธีใช้ Digital Signature เพื่อพิสูจน์ตัวตน (Authentication) ผ่านเว็บไซต์



<https://fidoalliance.org/>

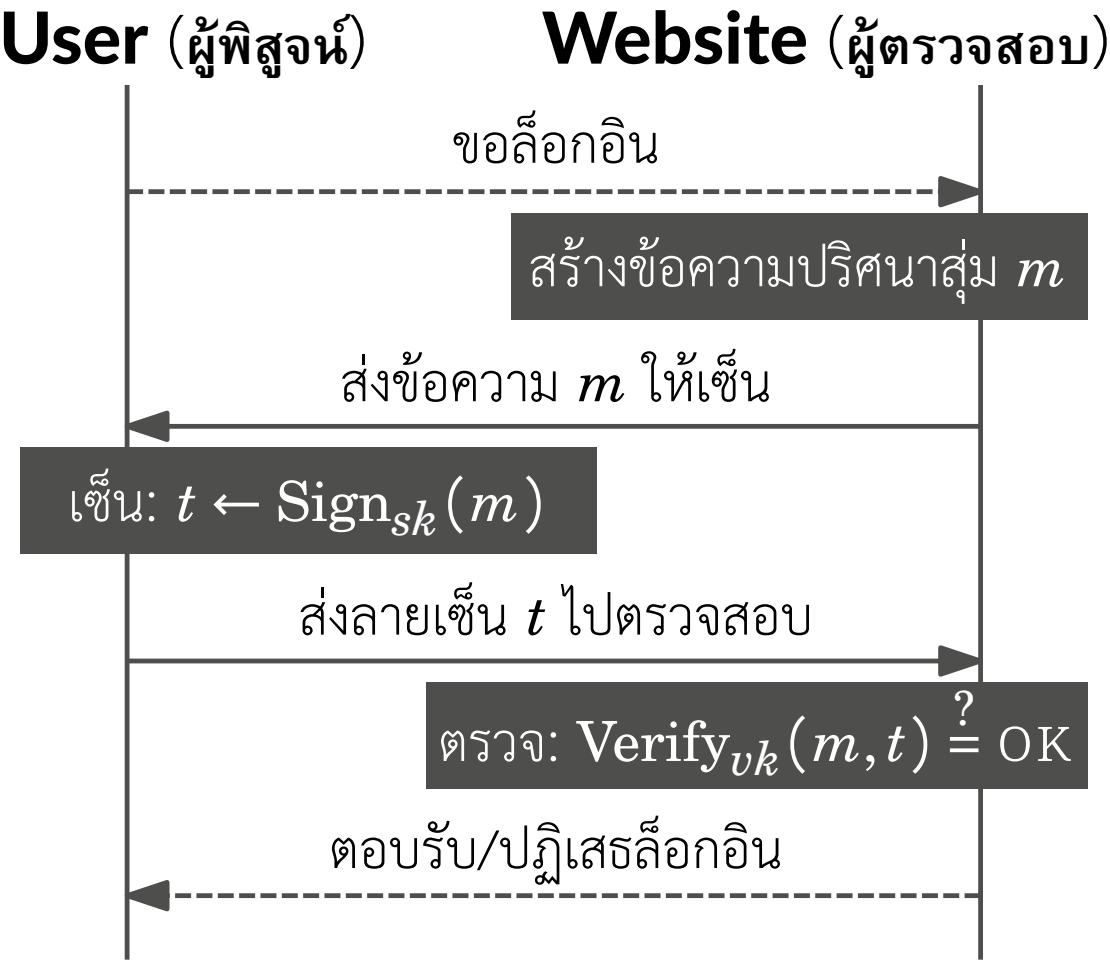
# ลายเซ็นดิจิทัล ► วิเคราะห์

ข้อมูลเบื้องต้น FIDO Alliance นำเสนอวิธีใช้ Digital Signature เพื่อพิสูจน์ตัวตน (Authentication) ผ่านเว็บไซต์



<https://fidoalliance.org/>

จงพิสูจน์ความเป็นเจ้าของกุญแจสาธารณะ (verification key,  $vk$ ) โดยใช้กุญแจส่วนตัว (signing key,  $sk$ ) เซ็นข้อความปริศนาที่กำหนดให้



# ลายเซ็นดิจิทัล ► วิเคราะห์

## ข้อมูลเบื้องต้น

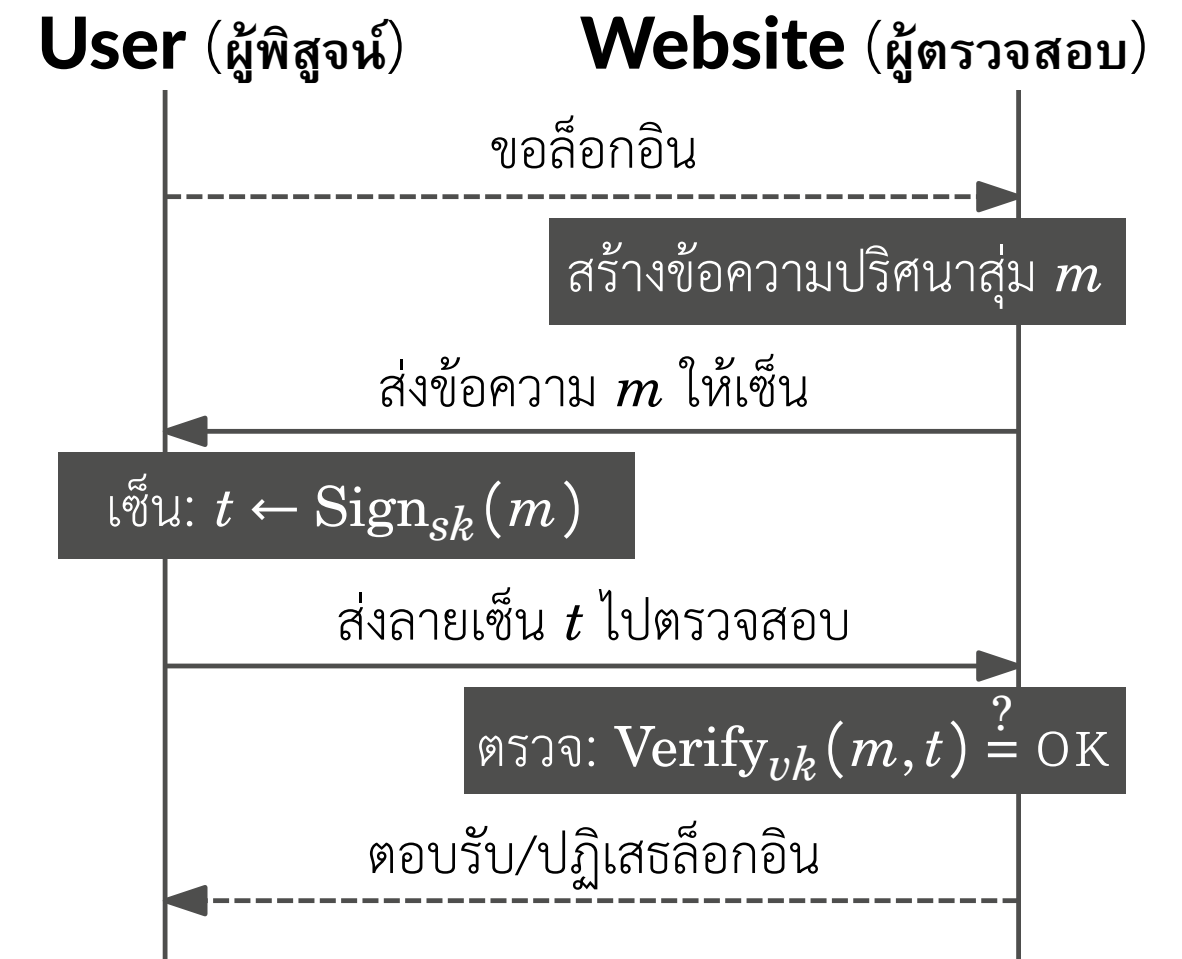
FIDO Alliance นำเสนอวิธีใช้ Digital Signature เพื่อพิสูจน์ตัวตน (Authentication) ผ่านเว็บไซต์



<https://fidoalliance.org/>

จงพิสูจน์ความเป็นเจ้าของของกุญแจสาธารณะ (verification key,  $vk$ ) โดยใช้กุญแจส่วนตัว (signing key,  $sk$ ) เซ็นข้อความปริศนาที่กำหนดให้

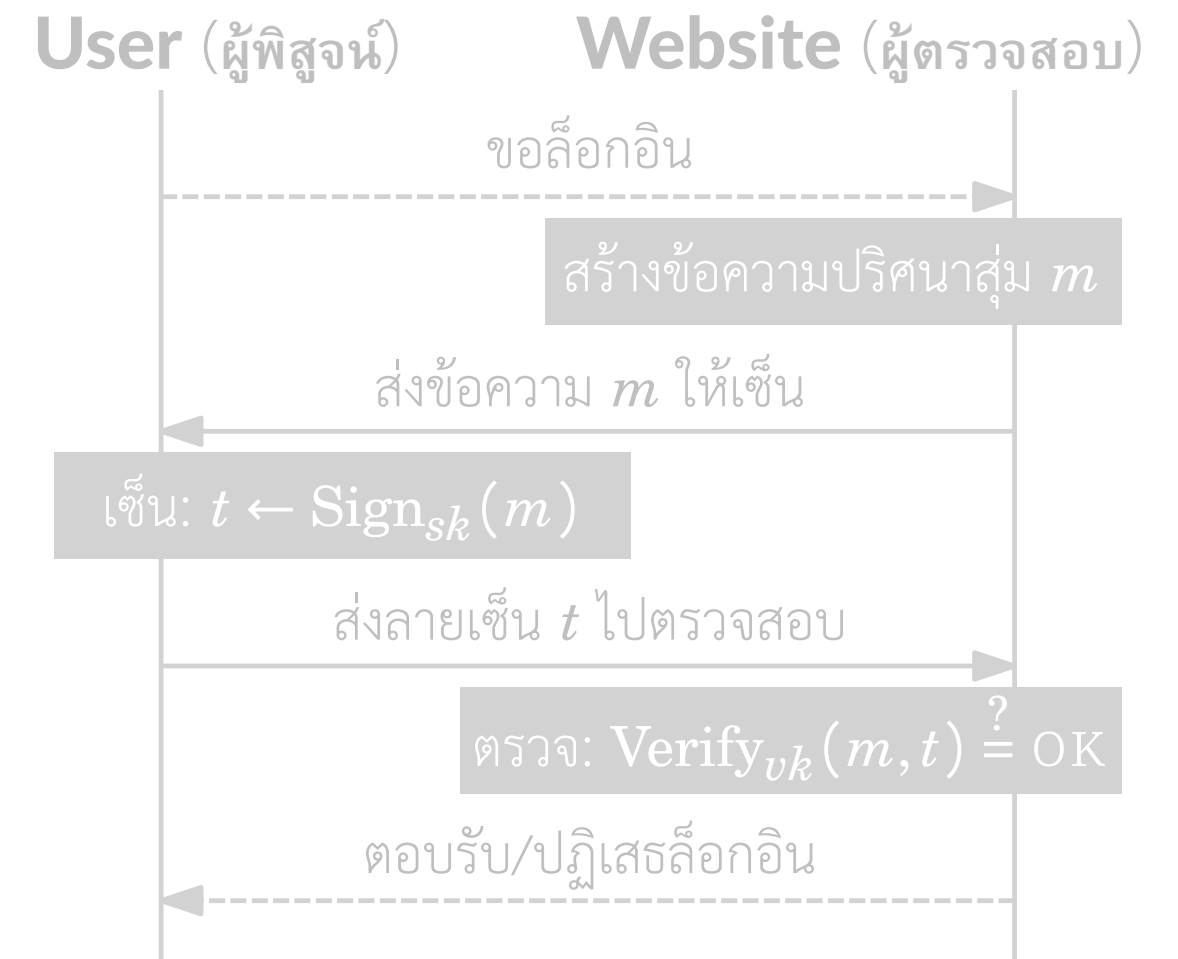
# IS THIS PROTOCOL ZERO - KNOWLEDGE?





# NO

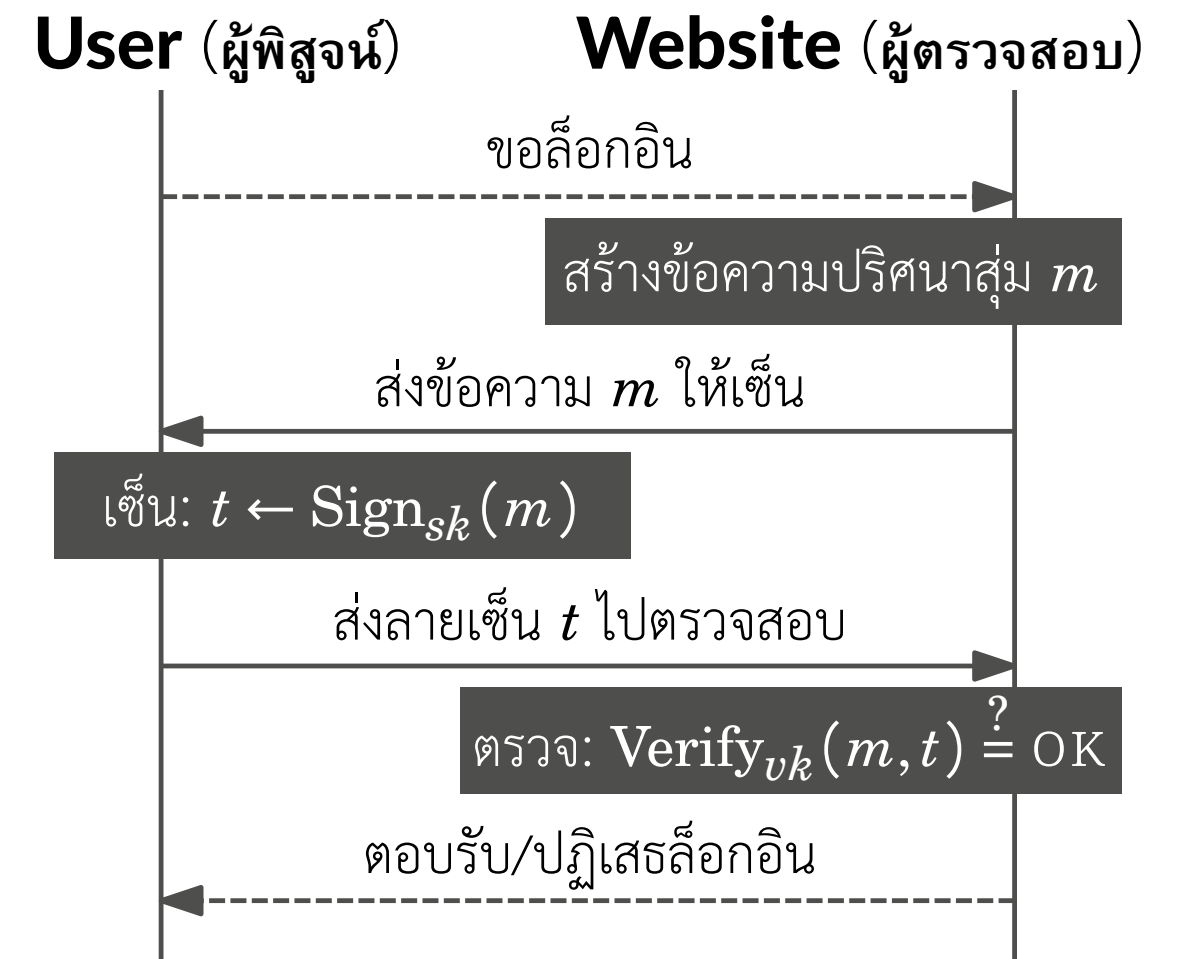
## IS THIS PROTOCOL ZERO-KNOWLEDGE?



**NO**

**IS THIS PROTOCOL  
ZERO - KNOWLEDGE?**

เหตุผล **Website** ไม่สามารถคาดเดา  
ลายเซ็น  $t$  ได้ด้วยตัวเอง  
(แต่เรียนรู้ได้จาก **User**)



 **Act II**

# **OUT IN THE FIELDS**

# ZKP on Cryptocurrency

$$send_1 + send_2 + \dots + send_m = recv_1 + recv_2 + \dots + recv_n$$

# ZKP on Cryptocurrency

$$send_1 + send_2 + \dots + send_m = recv_1 + recv_2 + \dots + recv_n$$

ซึ่งต้องพิสูจน์



สมการโอน-รับเงิน เป็นจริง



เงินแต่ละก้อน มีค่าเป็นบวก

เงื่อนไข



ซ่อนมูลค่าเงินแต่ละก้อน



ซ่อนเจ้าของบัญชี

# ZKP on Cryptocurrency

$$send_1 + send_2 + \dots + send_m = recv_1 + recv_2 + \dots + recv_n$$

ซึ่งต้องพิสูจน์



สมการโอน-รับเงิน เป็นจริง



เงินแต่ละก้อน มีค่าเป็นบวก

เงื่อนไข



ซ่อนมูลค่าเงินแต่ละก้อน



ซ่อนเจ้าของบัญชี

## zk-SNARKs Protocol

### Definition Provided

Bitansky, Nir, Ran Canetti, Alessandro Chiesa and Eran Tromer. “From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again.” *ITCS* (2011).

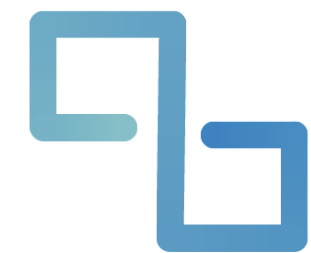
### Recent Improvements on Computational Complexity

Bünz, Benedikt, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille and Greg Maxwell. “Bulletproofs: Short Proofs for Confidential Transactions and More.” *IACR Cryptology ePrint Archive 2017* (2017): 1066.



CASH

J.P.Morgan



Quorum